





Data Protection and Information Governance

Incorporating the Records Management Plan

Information governance, or IG, is the set of multi-disciplinary structures, policies, procedures, processes and controls implemented to manage information at an enterprise level, supporting an organisation's immediate and future regulatory, legal, risk, environmental and operational requirements. IG encompasses more than traditional records management. It incorporates privacy attributes, electronic discovery requirements, storage optimisation, and metadata management.

Version	Description	Date	Approved
0.1	Approved by Senior Management Team	2014 Jun	Senior Personal Assistant
0.2	[Draft RMP submitted informally to The Keeper's Assessment Team for initial guidance]	2014 Dec	Senior Personal Assistant
1.0	Published on SPSO website. [RMP formally submitted to The Keeper]	2015 Apr	Senior Personal Assistant
1.1	RMP updated with NRS MoU, CIGO and Keeper's approval	2016 Apr	Senior Personal Assistant
1.2	Updated records management and security guidance policy	2018 May	Corporate Services Manager
2.0	RMP self-assessment completed, DP policy included, handbook reviewed	2018 Aug	Corporate Services Manager
3.0	RMP, BCS, Retention, breach protocol updated, FM, info sharing added, handbook reviewed	2020 Dec	Corporate Information Governance Officer
4.0	RMP, Complying with Info Leg, DP policy and procedure, Covert recording policy	2021 Oct	Corporate Information Governance Officer
5.0	RMP	2022 May	Corporate Information Governance Officer
6.0	Information about access & restrictions in business classification scheme added	2022 Aug	Corporate Services Manager
7.0	Full review of handbook	2023 Mar	Corporate Information Governance Officer
8.0	Ful review of handbook	2024	Corporate Information Governance Officer

Contents: Information Governance Handbook

-  **Records management plan**
-  **Records management policy**
-  **Business classification scheme**
-  **Case file management guidance**
-  **Retention and disposal policy**
-  **Information sharing policy**
-  **Electronic information sharing – eRDM Connect**
-  **Records management and security guidance: processing information off-network and out-of-office**
-  **Clear desk and screen policy**
-  **Protective marking system**
-  **Access to information legislation**
-  **Data Protection Legislation**
-  **Data Protection policy and procedure**
-  **Subject Access Requests**
-  **Data Protection Impact assessments: process and supplementary guidance**
-  **Protocol for data security incidents**
-  **SPSO Covert recording policy**
-  **Digital recording policy**

Records management plan

Prepared in accordance with The Public Records (Scotland) Act 2011

Submitted to The Keeper April 2015

Agreed by The Keeper February 2016

Contents

Introduction	2
The Public Records (Scotland) Act 2011	2
Records Management Plan	2
Element 1: Senior management responsibility	4
Element 2: Records manager responsibility	5
Element 3: Records management policy statement	6
Element 4: Business classification	7
Element 5: Retention schedules	9
Element 6: Destruction arrangements	11
Element 7: Archiving and transfer arrangements	12
Element 8: Information security	13
Element 9: Data protection	16
Element 10: Business continuity and vital records	18
Element 11: Audit trail	19
Element 12: Competency framework for records management staff	20
Element 13: Assessment and review	21
Element 14: Shared Information	22

Back to the main [Contents Page](#)

Introduction

1. Under The Public Records (Scotland) Act 2011 (the Act) Scottish public authorities are required to produce and submit a records management plan (RMP) setting out proper arrangements for the management of an authority's public records to the Keeper of the Records of Scotland (the Keeper) for his agreement under section 1 of the Act. The scope of the Records Management Plan applies to all records irrespective of the technology used to create and store them or the type of information they contain.

The Public Records (Scotland) Act 2011

2. Section 1 of the Act says,
 - (1) Every authority to which this Part applies must—
 - (a) prepare a plan (a 'records management plan') setting out proper arrangements for the management of the authority's public records,
 - (b) submit the plan to the Keeper for agreement, and
 - (c) ensure that its public records are managed in accordance with the plan as agreed with the Keeper.
3. The Act specifically requires a public authority to include certain elements in its records management plan and it is unlikely the Keeper would agree a RMP that does not include these elements.

Records Management Plan

4. The Plan has 14 elements, which are:
 - 4.1. Senior management responsibility
 - 4.2. Records manager responsibility
 - 4.3. Records management policy statement
 - 4.4. Business classification
 - 4.5. Retention schedules
 - 4.6. Destruction arrangements
 - 4.7. Archiving and transfer arrangements
 - 4.8. Information security
 - 4.9. Data protection
 - 4.10. Business continuity and vital records
 - 4.11. Audit trail
 - 4.12. Competency framework for records management staff
 - 4.13. Assessment and review

4.14. Shared information

5. The compulsory elements to ensure the records management plan will be agreed by the Keeper are 4.1, 4.2, 4.3, 4.6, 4.7 and 4.8.

RMP Element Description	SPSO Statement	Evidence
<p>Element 1: Senior management responsibility</p> <p>Identify an individual at senior level who has overall strategic accountability for records management.</p> <p>Section 1(2)(a)(i) of the Act specifically requires a RMP to identify the individual responsible for the management of the authority's public records. An authority's RMP must name and provide the job title of the senior manager who accepts overall responsibility for the RMP that has been submitted.</p> <p>It is vital that the RMP submitted by an authority has the approval and support of that authority's senior management team. Where an authority has already appointed a Senior Information Risk Owner, or similar person, they should consider making that person responsible for the records management programme. It is essential that the authority identifies and seeks the agreement of a senior post-holder to take overall responsibility for records management. That person is unlikely to have a day-to-day role in implementing the RMP, although they are not prohibited from doing so.</p> <p>As evidence, the RMP could include, for example, a covering letter signed by the senior post-holder. In this letter the responsible person named should indicate that they endorse the authority's record management policy (See Element 3).</p> <p>Read further explanation and guidance about element 1: http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement1.asp</p>	<p>The Senior Responsible Officer for Records Management within the SPSO is the Head of Corporate and Shared Services: Stuart Crickmar.</p> <p>The HoCSS has overall strategic accountability for records management and accepts overall responsibility for the RMP that has been submitted. This is listed as one of the duties of the HoCSS post and is evidenced by the job description. This plan is supported by the Leadership Team headed by the Ombudsman.</p> <p>Any staff changes will not invalidate this plan as all records management responsibilities will be transferred to the incoming post holder and relevant training will be undertaken</p>	<p>HoCss's job description</p>

RMP Element Description	SPSO Statement	Evidence
<p>Element 2: Records manager responsibility</p> <p>Identify individual within the authority, answerable to senior management, to have day-to-day operational responsibility for records management within the authority.</p> <p>Section 1(2)(a)(ii) of the Act specifically requires a RMP to identify the individual responsible for ensuring the authority complies with its plan. An authority's RMP must name and provide the job title of the person responsible for the day-to-day operation of activities described in the elements in the authority's RMP. This person should be the Keeper's initial point of contact for records management issues. It is essential that an individual has overall day-to-day responsibility for the implementation of an authority's RMP. There may already be a designated person who carries out this role. If not, the authority will need to make an appointment. As with element 1 above, the RMP must name an individual rather than simply a job title. It should be noted that staff changes will not invalidate any submitted plan provided that the all records management responsibilities are transferred to the incoming post holder and relevant training is undertaken. This individual might not work directly for the scheduled authority. It is possible that an authority may contract out their records management service. If this is the case an authority may not be in a position to provide the name of those responsible for the day-to-day operation of this element. The authority must give details of the arrangements in place and name the body appointed to carry out the records management function on its behalf. It may be the case that an authority's records management programme has been developed by a third party. It is the person operating the programme on a day-to-day basis whose name should be submitted.</p> <p>Read further explanation and guidance about element 2: http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement2.asp</p>	<p>The officer with operational responsibility for records management within the SPSO is the Corporate Information Governance Officer.</p> <p>The Corporate Information Governance Officer is responsible for the day-to-day operation of activities described in the elements and is the Keeper's initial point of contact for records management issues. This is listed as one of the duties of the Corporate Information Governance Officer post and is evidenced by the job description.</p> <p>Any staff changes will not invalidate this plan as all records management responsibilities will be transferred to the incoming post holder and relevant training will be undertaken</p>	<p>Corporate Information Governance Officer's Job Description</p>

Element 3: Records management policy statement

A records management policy statement underpins effective management of an authority's records and information. It demonstrates to employees and stakeholders that managing records is important to the authority and serves as a mandate for the activities of the records manager.

The Keeper expects each authority's plan to include a records management policy statement. The policy statement should describe how the authority creates and manages authentic, reliable and useable records, capable of supporting business functions and activities for as long as they are required. The policy statement should be made available to all staff, at all levels in the authority. The statement will properly reflect the business functions of the public authority. The Keeper will expect authorities with a wide range of functions operating in a complex legislative environment to develop a fuller statement than a smaller authority. The records management statement should define the legislative, regulatory and best practice framework, within which the authority operates and give an overview of the records management processes and systems within the authority and describe how these support the authority in carrying out its business effectively. For electronic records the statement should describe how metadata is created and maintained. It should be clear that the authority understands what is required to operate an effective records management system which embraces records in all formats. The statement should demonstrate how the authority aims to ensure that its records remain accessible, authentic, reliable and useable through any organisational or system change. This would include guidelines for converting or migrating electronic records from one system to another.

The records management statement should include a description of the mechanism for records management issues being disseminated through the authority and confirmation that regular reporting on these issues is made to the main governance bodies. The statement should have senior management approval and evidence, such as a minute of the management board recording its approval, submitted to the Keeper. The other elements in the RMP, listed below, will help provide the Keeper with evidence that the authority is fulfilling its policy.

Read further explanation and guidance about element 3:
<http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement3.asp>

The SPSO Records Management Policy is contained in one of the suite of policies in the SPSO Handbook - Information Governance (this document).

The SPSO Handbooks are easily accessed by all staff on the internal file management system eRDM. This particular handbook is also published on our website here: [SPSO Policies | SPSO](#)

[SPSO Records Management Policy](#)

Internal Audit of SPSO's public records management in March 2014

SMT Minute 09/10/14 noting approval of Record Management Plan and Policy - published:
https://www.spsso.org.uk/sites/spso/files/communications_material/minutes/2014/SMT2MeetingNote9Oct2014.pdf

AAC Minute 21/10/14 noting endorsement of the Record Management Plan and Policy – published:
https://www.spsso.org.uk/sites/spso/files/communications_material/minutes/2014/AACMeetingNote141021.pdf

Element 4: Business classification

A business classification scheme describes what business activities the authority undertakes – whether alone or in partnership.

The Keeper expects an authority to have properly considered business classification mechanisms and its RMP should therefore reflect the functions of the authority by means of a business classification scheme or similar.

A business classification scheme usually takes the form of a hierarchical model or structure diagram. It records, at a given point in time, the informational assets the business creates and maintains, and in which function or service area they are held. As authorities change the scheme should be regularly reviewed and updated.

A business classification scheme allows an authority to map its functions and provides a structure for operating a disposal schedule effectively.

Some authorities will have completed this exercise already, but others may not. Creating the first business classification scheme can be a time-consuming process, particularly if an authority is complex, as it involves an information audit to be undertaken. It will necessarily involve the cooperation and collaboration of several colleagues and management within the authority, but without it the authority cannot show that it has a full understanding or effective control of the information it keeps.

Although each authority is managed uniquely there is an opportunity for colleagues, particularly within the same sector, to share knowledge and experience to prevent duplication of effort.

All of the records an authority creates should be managed within a single business classification scheme, even if it is using more than one record system to manage its records.

An authority will need to demonstrate that its business classification scheme can be applied to the record systems which it operates.

Read further explanation and guidance about element 4:
<http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement4.asp>

The SPSO has a clear and discrete remit outlined in the Scottish Public Services Ombudsman Act. The electronic records for the core functions of the SPSO are stored on a bespoke casework management system - WorkPro. This application provides an electronic records management system for all casework, including PCSs, INWO complaints, SWF reviews, decision reviews, CSCs, FOI / EIR / DP, and most complaint standards authority, outreach and media work. Individual records are created and stored electronically by reference number, with supporting paperwork also retained by reference number when required.

All other SPSO records are mostly administrative in function, easily defined and highly structured; and whose access are clearly determined. Therefore, the SPSO business classification system is modelled on the functions of the organisation, and directly reflects the hierarchical relationship of functions, activities, transactions and records.

The SPSO business classification scheme (BCS) for the non-casework business records is implemented through an electronic records management system on the Scottish Government eDRM (Objective) system. The SPSO strives to be a paper-less office for these functions; therefore, there is no central storage or archiving of paper files.

Some personnel functions, such as payroll, are contracted out to MoorePay, who manage and retain personnel details to provide this service.

The BCS is described in Section 3 of the SPSO Handbook - Information Governance (this document). The BCS will be

CAS WorkPro ICT System Documentation]

[SPSO Business Classification Scheme](#)

[220112 Workpro and eRDM Document Naming Convention:](#)

<https://erdm.scotland.gov.uk:8443/documents/A36078650/details>

[220117 eRDM Document Naming Convention Video:](#)

<https://erdm.scotland.gov.uk:8443/documents/A36154606/details>

[IMSO guidance and training](#)

[eRDM etraining](#)

RMP Element Description	SPSO Statement	Evidence
	reviewed every two years by the Leadership Team, with the HoCSS providing oversight of the review	

Element 5: Retention schedules

A retention schedule is a list of records for which pre-determined disposal dates have been established.

Section 1(2)(b)(iii) of the Act specifically requires a RMP to include provision about the archiving and destruction or other disposal of the authority's public records.

An authority's RMP must demonstrate the existence of and adherence to corporate records retention procedures. The procedures should incorporate retention schedules and should detail the procedures that the authority follows to ensure records are routinely assigned disposal dates, that they are subsequently destroyed by a secure mechanism (see element 6) at the appropriate time, or preserved permanently by transfer to an approved repository or digital preservation programme (See element 7).

The principal reasons for creating retention schedules are to:

ensure records are kept for as long as they are needed and then disposed of appropriately;

ensure all legitimate considerations and future uses are considered in reaching the final decision; and

provide clarity as to which records are still held by an authority and which have been deliberately destroyed.

'Disposal' in this context does not necessarily mean destruction. It includes any action taken at the agreed disposal or review date including migration to another format and transfer to a permanent archive.

A retention schedule is an important tool for proper records management. Authorities who do not yet have a full retention schedule in place should show evidence that the importance of such a schedule is acknowledged by the senior person responsible for records management in an authority (see element 1). This might be done as part of the policy document (element 3). It should also be made clear that the authority has a retention schedule in development.

The SPSO Retention and Disposal Policy is included in the SPSO Handbook - Information Governance (this document). This document describes the list of records for which pre-determined disposal dates have been established and the archiving and destruction arrangements that are in place. It also includes an MoU with National Records Scotland for the long-term archiving of particular records of national interest

[SPSO Retention and Disposal Policy](#)

[MoU](#)

RMP Element Description	SPSO Statement	Evidence
<p>An authority's RMP must demonstrate the principle that retention rules are consistently applied across all of an authority's record systems.</p> <p>Read further explanation and guidance about element 5: http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement5.asp</p>		

RMP Element Description	SPSO Statement	Evidence
<p>Element 6: Destruction arrangements</p> <p>It is not always cost-effective or practical for an authority to securely destroy records in-house. Many authorities engage a contractor to destroy records and ensure the process is supervised and documented.</p> <p>Section 1(2)(b)(iii) of the Act specifically requires a RMP to include provision about the archiving and destruction, or other disposal, of an authority's public records.</p> <p>An authority's RMP must demonstrate that proper destruction arrangements are in place.</p> <p>A retention schedule, on its own, will not be considered adequate proof of disposal for the Keeper to agree a RMP. It must be linked with details of an authority's destruction arrangements. These should demonstrate security precautions appropriate to the sensitivity of the records. Disposal arrangements must also ensure that all copies of a record – wherever stored – are identified and destroyed.</p> <p>Read further explanation and guidance about element 6: http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement6.asp</p>	<p>The SPSO Retention and Disposal Policy is included in the SPSO Handbook - Information Governance (this document). This document describes the list of records for which pre-determined disposal dates have been established and the archiving and destruction arrangements that are in place.</p> <p>Disposal of SPSO records according to the policy is managed by the Corporate Information Governance Officer, and implemented by the Team Assistant – Information Governance.</p> <p>Disposal arrangements for paper records are contracted to Paper Shredding Services (PSS) who dispose of our paper securely. They comply with Code of Practice BS EN 15713:2009.</p> <p>Disposal arrangements for electronic records contained in the filing system are managed in-house using the electronic file management arrangements contained within Workpro and eRDM (Objective). Email records are archived and destroyed in line with SCOTS Connect arrangements using MS Exchange Online. Records kept within the call recording system hosted by GAMMA are destroyed in line with the policy after 90 working days unless they have been transferred to an in-house system when the above arrangements apply.</p> <p>IT hardware must be returned to iTECS for disposal in line with the Scottish Government Security Policy standards, in particular, 6.6.3 Equipment Disposal and 7.5.4 Secure erasure and disposal of computer media</p>	<p>SPSO Retention and Disposal Policy</p> <p>WorkPro case file destruction logs</p> <p>Paper Shredding Services</p> <p>PSS Shredding Procedures</p> <p>PSS Certificate of physical destruction by onsite shredding</p> <p>SG Intranet page outlining Physical and Environmental Security</p> <p>SG Intranet page outlining Administrative and Procedural Security Policy</p>

RMP Element Description	SPSO Statement	Evidence
<p>Element 7: Archiving and transfer arrangements</p> <p>This is the mechanism by which an authority transfers records of enduring value to an appropriate archive repository, specifying the timing of transfers and other terms and conditions.</p> <p>Section 1(2)(b)(iii) of the Act specifically requires a RMP to make provision about the archiving and destruction, or other disposal, of an authority's public records.</p> <p>An authority's RMP must detail its archiving and transfer arrangements and ensure that records of enduring value are deposited in an appropriate archive repository. The RMP will detail how custody of the records will transfer from the operational side of the authority to either an in-house archive, if that facility exists, or another suitable repository, which must be named. The person responsible for the archive should also be cited.</p> <p>Some records continue to have value beyond their active business use and may be selected for permanent preservation. The authority's RMP must show that it has a mechanism in place for dealing with records identified as being suitable for permanent preservation. This mechanism will be informed by the authority's retention schedule which should identify records of enduring corporate and legal value. An authority should also consider how records of historical, cultural and research value will be identified if this has not already been done in the retention schedule. The format/media in which they are to be permanently maintained should be noted as this will determine the appropriate management regime.</p> <p>Read further explanation and guidance about element 7: http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement7.asp</p>	<p>The SPSO Retention and Disposal Policy is included in the SPSO Handbook - Information Governance (this document).</p> <p>This document describes the list of records for which pre-determined disposal dates have been established and the archiving and destruction arrangements that are in place</p>	<p>SPSO Retention and Disposal Policy</p> <p>Memorandum of Understanding with The Keeper of the Records</p>

Element 8: Information security

Information security is the process by which an authority protects its records and ensures they remain available. It is the means by which an authority guards against unauthorised access and provides for the integrity of the records. Robust information security measures are an acknowledgement that records represent a risk as well as an asset. A public authority should have procedures in place to assess and contain that risk.

Section 1(2)(b)(ii) of the Act specifically requires a RMP to make provision about the archiving and destruction or other disposal of the authority's public records.

An authority's RMP must make provision for the proper level of security for its public records.

All public authorities produce records that are sensitive. An authority's RMP must therefore include evidence that the authority has procedures in place to adequately protect its records. Information security procedures would normally acknowledge data protection and freedom of information obligations as well as any specific legislation or regulatory framework that may apply to the retention and security of records.

The security procedures must put in place adequate controls to prevent unauthorised access, destruction, alteration or removal of records. The procedures will allocate information security responsibilities within the authority to ensure organisational accountability and will also outline the mechanism by which appropriate security classifications are linked to its business classification scheme.

Information security refers to records in all or any format as all are equally vulnerable. It refers to damage from among other things: computer viruses, flood, fire, vermin or mould.

Current or semi-current records do not normally require archival standard storage. Physical records will however survive far better in a controlled environment. In broad terms the environment for current records should not allow large changes in temperature or excess humidity (as increased high temperatures and humidity are more likely to cause mould). If records are not adequately protected then the risk that the records could be damaged and destroyed is potentially higher and could lead to significant reputational and financial cost to the business.

The SPSO has in place security policies and procedures that ensure there are adequate controls to prevent unauthorised access, destruction, alteration or removal of records. In the event of a breach, the Corporate Information Governance Officer is informed immediately who will coordinate and ensure all the appropriate investigation and reporting processes are undertaken.

To ensure the proper level of security for all the SPSO records:

1. the SPSO utilises the secure SCOTS Connect service provided by the Scottish Government to host our network services under an agreed Memorandum of Understanding (MOU). The network is assured to the standards and principles of the PSN as well as accreditation to NCSC's Cyber Essentials +. Users of the network must be formally registered with an agreed level of access. Access rights of system users who have left are removed immediately and permissions for staff changing role are reviewed and adjusted accordingly
2. the SPSO has enabled multi-factor authentication (MFA) for staff accounts on its payroll system, finance systems and learning hub, and for administrators (working towards switching on for all staff) on its casework management system.
3. Objective Connect application implemented for use by all staff in September 2020 as a secure way to share electronic information. Alongside the training and guidance provided, a new Electronic [Information Sharing – eRDM Connect](#) policy has been added to the Information Governance handbook (this document). Disc usb drives were closed in 2023-24.

Internal Audit of IS Installation and Network Services is undertaken every three years

SCOTS ITECS MoU

SG Intranet page outlining [Administrative and Procedural Security Policy](#)

SG Disclosure Scotland Guidance

SCOTS Connect Security Standards

ISIS Security Survey of Bridgeside House 08/2018

[Scottish Government IT security policy](#)

[SPSO Clear Desk and Screen policy](#)

[SPSO Complying with Information Legislation User Guide](#)

[SPSO Protective Marking System](#)

Staff Confidentiality Statement

[SPSO Records Management and Security Guidance: sharing information off-network and out-of-office](#)

RMP Element Description	SPSO Statement	Evidence
<p>Read further explanation and guidance about element 8: http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement8.asp</p>	<p>Mail out/in from SCOTS uses opportunistic TLS. Transport of paperwork is provided by an approved courier contractor.</p> <ol style="list-style-type: none"> 4. all employees are vetted appropriate to their job role which would include either a basic or enhanced disclosure; 5. the building Bridgeside House, 99 MacDonald Road (2018-19) is adapted to meet the Scottish Government security requirements for the SCOTS network; 6. the SPSO Clear Desk and Screen policy is described in the SPSO Handbook - Information Governance (this document) and details the procedures to reduce the risk of unauthorised access, loss of, and damage to information during and outside normal working hours; 7. a check of office is undertaken annually; 8. the SPSO Data Protection policy and procedures are described in the SPSO Handbook - Information Governance (this document) and details statutory obligations, guidance for protecting personal data and the emergency protocol for security and data breaches; 9. Staff confidentiality statement is included in annual declarations. 10. the SPSO policy 'Working from home' describes confidentiality and security rules for business conducted on behalf of the SPSO; 11. the SPSO Records Management and Security Guidance: sharing information off-network and out-of-office is described in the SPSO Handbook - Information Governance (this document) and details issues that must be considered to ensure that any SPSO information worked on out of the office is kept confidential and protected from loss of unauthorised 	<p>Annual staff training e-learning package on GDPR, policies and procedures, cyber security</p> <p>ICT Strategy and IT Security Policy</p> <p>2019 Cyber Essentials Accreditation: Certificate Number IASME-CE-009821</p> <p>2020 Cyber Essentials Accreditation: Certificate Number: IASME-A-014166</p> <p>2021 Cyber Essentials Accreditation: Certificate Number IASME-CE-032832</p> <p>2022 Cyber Essentials Accreditation: Certificate Number ed362dad-f1d7-44b6-8947-0d191258afcb</p> <p>2023 Cyber Essentials Accreditation: Certificate Number: 2281d201 – 2bb1-49a0-bd62-11fff561e3aa</p> <p>Cyber Resilience Internal audit Sept 2020</p> <p>Exercise in a box</p> <p>WorkPro cyber security</p>

RMP Element Description	SPSO Statement	Evidence
	<p>access and exploitation; and a WFH security checklist is provided to staff.</p> <p>12.the Corporate Information Governance Officer provides training to all staff regarding the Data Protection requirements. Induction and regular data protection, records management and information and cyber security updates, training and bulletins provided for staff</p> <p>13.Cyber Essentials Accreditation achieved November 19 and maintained annually</p> <p>14.ICT Strategy and IT Security Policy</p> <p>15.Internal Audit of Cyber Resilience was undertaken in September 2020</p> <p>16.The Gamma call recording facility meets industry standards and has appropriate ISO accreditation. Access is limited to SPSO staff and only some staff can download. The system is auditable.</p>	

Element 9: Data protection

An authority that handles personal information about individuals has a number of legal obligations to protect that information under the Data Protection Act 1998.

The Keeper will expect an authority's RMP to indicate compliance with its data protection obligations. This might be a high-level statement of public responsibility and fair processing.

If an authority holds and processes information about stakeholders, clients, employees or suppliers, it is legally obliged to protect that information. Under the Data Protection Act, an authority must only collect information needed for a specific business purpose, it must keep it secure and ensure it remains relevant and up to date. The authority must also only hold as much information as is needed for business purposes and only for as long as it is needed. The person who is the subject of the information must be afforded access to it on request.

Read further explanation and guidance about element 9:
<http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement9.asp>

The SPSO is legally obliged to protect any personal information that we hold, and we are required to notify the Information Commissioner's Office (ICO). SPSO data protection and information governance policies, procedures and guidance are described in the SPSO Handbook - Information Governance (this document) and detail statutory obligations, guidance for protecting personal data and the emergency protocol for security and data breaches. The SPSO outlines its duty to employees in the policy 'Managing Personal Data'. A privacy notice is also available for staff and advisers.

The SPSO publishes a privacy notice and information on its website and summarises its duties in leaflets for complainants and applicants, organisations, and others. It also provides privacy information in templates and footers.

The SPSO is a registered data controller with the Information Commissioner's Office (ICO).

We have produced the SPSO Data Protection Policy Statement included in the SPSO Handbook - Information Governance (this document). We have an Appropriate Policy Document for special category data.

Data protection activity is incorporated into our regular business planning and risk management, with regular reporting to LT, We keep records of our processing activities (RoPA), and carry out DPIAs where required. Inductions and regular staff training is in place.

Internal Audit of Data Management (GDPR) was undertaken in November 2020.

Registered data controller with ICO. Registration Number: Z7336887 - Date Registered: 29 Nov 2002 - Registration is renewed annually every November

[SPSO Data Protection Policy and Procedure](#)

[SPSO Managing Personal Data](#)

[SPSO Website Disclaimer and Privacy Policy](#)

Privacy notices

[Notice in Complainant leaflet containing Anonymity statement](#)

Internal Audit of Data Management (GDPR), November 2020.

Personal data breach staff training

Rist Register

Business Plan

Assurance papers

DPIAs

APD

RoPA

RMP Element Description	SPSO Statement	Evidence
		Induction and training material

RMP Element Description	SPSO Statement	Evidence
<p>Element 10: Business continuity and vital records</p> <p>A business continuity and vital records plan serves as the main resource for the preparation for, response to, and recovery from, an emergency that might affect any number of crucial functions in an authority.</p> <p>The Keeper will expect an authority's RMP to indicate arrangements in support of records vital to business continuity. Certain records held by authorities are vital to their function. These might include insurance details, current contract information, master personnel files, case files, etc. The RMP will support reasonable procedures for these records to be accessible in the event of an emergency affecting their premises or systems.</p> <p>Authorities should therefore have appropriate business continuity plans ensuring that the critical business activities referred to in their vital records will be able to continue in the event of a disaster. How each authority does this is for them to determine in light of their business needs, but the plan should point to it.</p> <p>Read further explanation and guidance about element 10: http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement10.asp</p>	<p>The SPSO keeps all vital records in electronic form, which are stored on servers hosted off-site by the Scottish Government, with an agreed back-up schedule as outlined in the MoU. The BCP confirms that the Scottish Government iTECS BCP Team would be responsible for reinstating normal (lost) IT Services in the event of the activation of the plan. The BCP is published on our website</p> <p>Vital records are clearly identified in the eRDM file plan with their own Corporate, Legal or Historic file type to ensure correct retention periods are maintained</p> <p>Internal Audit of Business Continuity (C-19) was undertaken in February 2021</p>	<p>Link to SPSO Business Continuity Plan which is published on SPSO website</p> <p>ISIS MoU</p> <p>Internal audit of Business Continuity (C-19), February 2021</p>

RMP Element Description	SPSO Statement	Evidence
<p>Element 11: Audit trail</p> <p>An audit trail is a sequence of steps documenting the movement and / or editing of a record resulting from activities by individuals, systems or other entities.</p> <p>The Keeper will expect an authority's RMP to provide evidence that the authority maintains a complete and accurate representation of all changes that occur in relation to a particular record. For the purpose of this plan, 'changes' can be taken to include movement of a record even if the information content is unaffected. Audit trail information must be kept for at least as long as the record to which it relates.</p> <p>This audit trail can be held separately from or as an integral part of the record. It may be generated automatically, or it may be created manually.</p> <p>Read further explanation and guidance about element 11: http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement11.asp</p>	<p>The ERMS systems for casework records (WorkPro) and non-casework records (eRDM (Objective)) provide concise audit trails documenting the editing of all records resulting from activities by individuals, systems or other entities; and recording the movement and location of associated paper files</p> <p>The location of casework paper files is also audited each year to ensure the electronic case file on WorkPro accurately records the location of the associated paper documents. The results of the audit are reported to the Leadership Team and circulated to all staff</p> <p>The SPSO strives to be a paper-less office for the non-casework functions; therefore, there is no central storage or archiving of paper files for these functions apart from finance documents and personnel records, and those that will be agreed for long-term archiving by NRS</p>	<p>CAS WorkPro ICT System Documentation</p> <p>Objective ICT System Documentation</p> <p>Annual File Location Audit</p>

Element 12: Competency framework for records management staff

A competency framework lists the core competencies and the key knowledge and skills required by a records manager. It can be used as a basis for developing job specifications, identifying training needs, and assessing performance.

The Keeper will expect an authority's RMP to detail a competency framework for person(s) designated as responsible for the day-to-day operation of activities described in the elements in the authority's RMP. It is important that authorities understand that records management is best implemented by a person or persons possessing the relevant skills.

A competency framework outlining what the authority considers are the vital skills and experiences needed to carry out the task is an important part of any records management system. If the authority appoints an existing non-records professional member of staff to undertake this task, the framework will provide the beginnings of a training programme for that person.

The individual carrying out day-to-day records management for an authority might not work for that authority directly. It is possible that the records management function is undertaken by a separate legal entity set up to provide functions on behalf of the authority, for example an arm's length body or a contractor. Under these circumstances, the authority must satisfy itself that the supplier supports and continues to provide a robust records management service to the authority. The authority's RMP must confirm that it is satisfied by the standard of the records management provided by the supplier and name the organisation that has been appointed to carry out records management on the authority's behalf.

Where an authority's records management system has been put in place by a third party, but is operated on a day-to-day basis by a member of staff in the authority, it is the competencies of that member of staff that should be confirmed, not those of the third party supplier of the system.

Read further explanation and guidance about element 12:
<http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement12.asp>

A competency framework outlining what the authority considers are the vital skills and experiences needed to carry out the task is an important part of any records management system. If the authority appoints an existing non-records professional member of staff to undertake this task, the framework will provide the beginnings of a training programme for that person

Mandatory training is undertaken by all staff before being granted access to the eRDM system. Additional training and guidance for eRDM Connect workspace admins and IMSOs.

HoCSS's Job Description

Corporate Information
Governance Officer's Job
Description

Workspace admins/IMSOs
training and guidance

RMP Element Description	SPSO Statement	Evidence
<p>Element 13: Assessment and review</p> <p>Regular self-assessment and review of records management systems will give an authority a clear statement of the extent that its records management practices conform to the Records Management Plan as submitted and agreed by the Keeper.</p> <p>Section 1(5)(i)(a) of the Act says that an authority must keep its RMP under review.</p> <p>An authority's RMP must describe the procedures in place to regularly review it in the future.</p> <p>It is important that an authority's RMP be regularly reviewed to ensure that it remains fit for purpose. It is therefore vital that a mechanism exists for this to happen automatically as part of an authority's internal records management processes.</p> <p>A statement to support the authority's commitment to keep its RMP under review must appear in the RMP detailing how it will accomplish this task.</p> <p>Read further explanation and guidance about element 13: http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement13.asp</p>	<p>The SPSO will review SPSO Handbook - Information Governance (this document), which includes the Records Management Plan and all its elements, every two years to ensure that it remains fit for purpose as part of the internal records management processes. The review will be led by the Corporate Information Governance Officer with relevant staff providing input and updates to the sections under their responsibility.</p> <p>Any significant changes to any part of the SPSO Handbook - Information Governance (this document) will be reported to the Leadership Team for approval and the Advisory Audit Board for information. The Keeper will be informed of the outcome from this review</p>	<p>First review reported July 2018</p> <p>PURs</p>

Element 14: Shared Information

Under certain conditions, information given in confidence may be shared. Most commonly, this relates to personal information, but it can also happen with confidential corporate records.

The Keeper will expect an authority's RMP to reflect its procedures for sharing information. Authorities who share, or are planning to share, information must provide evidence that they have considered the implications of information sharing on good records management.

Information sharing protocols act as high-level statements of principles on sharing and associated issues, and provide general guidance to staff on sharing information or disclosing it to another party. It may therefore be necessary for an authority's RMP to include reference to information sharing protocols that govern how the authority will exchange information with others and make provision for appropriate governance procedures.

Specifically the Keeper will expect assurances that an authority's information sharing procedures are clear about the purpose of record sharing which will normally be based on professional obligations. The Keeper will also expect to see a statement regarding the security of transfer of information, or records, between authorities whatever the format.

Issues critical to the good governance of shared information should be clearly set out among parties at the earliest practical stage of the information sharing process. This governance should address accuracy, retention and ownership. The data-sharing element of an authority's RMP should explain review procedures, particularly as a response to new legislation.

Read further explanation and guidance about element 14:
<http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement14.asp>

The SPSO does not routinely share information with other bodies as we conduct our investigations in private. However, we do request bodies under our jurisdiction to provide their complaint file and suitable evidence during the course of an investigation. At these times, the SPSO operate in accordance with GDPR and the Information Commissioner's Data Sharing Code of Practice. Information we hold relating to casework is processed in line with the statutory obligations listed in the SPSO Act 2002. The SPSO Sharing Information User Guide is described in the SPSO Handbook - Information Governance (this document)

The Scottish Government SCOTS network is assured to the standards and principles of the UK Public Services Network (PSN), which was formerly known as the GSI network, as well as accreditation to NSCS's Cyber Essentials +, and is subject to rigorous security controls; and provides a secure network infrastructure protected from intrusion or attack (the SCOTS network is managed to the information security standard ISO 27001)

Mail out/in from SCOTS uses opportunistic Transport Layer Security (TLS) to encrypt and protect email traffic.

SPSO moved onto the SCOTS network (an Impact Level 3 (IL3) (restricted) network under the HMG Security Policy Framework) in 2011 to access the secure GSI email network for the safe sharing of electronic documents. As such, all users have security clearances appropriate to handling IL3 data. The SPSO started using Objective Connect for secure file sharing in 2020.

SPSO Handbook - Complaints Handling Guidance Section C Step 9a SPSO Sharing Information User Guide]

Eagle Couriers Tender for Contract November 2013 outlining security clearance of drivers and security checks

SCOTS Connect Security Standards

Moved to Objective/Connect in 2020

[ICT Strategy and IT Security Policy](#)

RMP Element Description	SPSO Statement	Evidence
	<p>Transport of hard-copy case files and other sensitive documents to approved locations out of the office is provided by an approved courier contractor only. The current contractor is Eagle Couriers.</p> <p>The SPSO's information sharing powers have been extended. SPSO are also part of the Sharing Intelligence for Health and Care group which has an emerging concerns protocol. A new information sharing policy has been created</p>	

Back to the main [Contents Page](#)

Records management policy

Issued: April 2015

Contents

Introduction	2
Purpose and scope	2
What is records management?	3
Why is records management important?	4
Policy statement and commitment	4
Roles and responsibilities	5
The Head of Corporate and Shared Services (HoCSS)	6
The Leadership Team	6
Line Mangers	6
Corporate Information Governance Officer	6
Information Management support officers	6
Legislative framework	6
Relationship to other SPSO policies	7
Training	7
Monitoring and review	7

Back to the main [Contents Page](#)

Introduction

1. Records management (RM) is the professional practice or discipline of controlling and governing what are considered to be the most important records of an organisation throughout the records life cycle, which includes from the time such records are conceived through to their eventual disposal. This work includes identifying, classifying, prioritising, storing, securing, archiving, preserving, retrieving, tracking and destroying of records.
2. Records management is part of an organisation's broader activities that are associated with the discipline known as governance, risk, and compliance and is primarily concerned with the evidence of an organisation's activities as well as the reduction or mitigation of risk that may be associated with such evidence.
3. The SPSO recognises that the effective management of its records is essential in order to support our core functions, to comply with legal, statutory and regulatory obligations, and to demonstrate transparency and accountability to all its stakeholders. Records are a vital information asset and a valuable resource for the organisation's decision-making processes, policy creation and operations, and must be managed effectively from the point of their creation until their ultimate disposal.

Purpose and scope

4. The purpose of this policy is to demonstrate the importance of managing records effectively within the organisation, to outline key aims and objectives for SPSO in relation to its record-keeping, and to act as a mandate for the support and delivery of records management policies, procedures and initiatives across the organisation.
5. This policy relates to all staff of the SPSO and all records created or acquired in the course of its business. It relates to the management of records as an internal, facilitative function of the organisation.
6. The policy is to be read in conjunction with the [Records management plan](#) for the SPSO, which details the current record-keeping practices in place within the organisation.
7. The aims of this policy include:
 - 7.1. the improvement of business efficiency through less time spent searching for information;
 - 7.2. increased joined up working and improved communications across the organisation as a whole;

- 7.3. the demonstration of compliance with statutory and regulatory record-keeping obligations including the Public Records (Scotland) Act 2011, the Freedom of Information (Scotland) Act 2002, Environmental Information Regulations 2004 and the Data Protection Act 2018; and
 - 7.4. the promotion of openness, transparency, accountability and improved corporate governance, commensurate with the organisation's role.
8. The Public Records (Scotland) Act 2011 places an obligation on named authorities in Scotland to produce a records management plan which sets out their arrangements for the effective management of all records. The SPSO is a named authority as defined in the Act. The creation of a records management policy statement is a mandatory element of the plan, and is necessary in order to identify the procedures to be followed in managing the organisation's public records.

What is records management?

- 9. Records management can be defined as the process an organisation manages its records, whether created internally or externally and in any format or media type, from their creation or receipt, through to their destruction or permanent preservation.
- 10. Records management is about placing controls around each stage of a record's lifecycle, at the point of creation (through the application of metadata, version control and naming conventions), during maintenance and use (through the management of security and access classifications, facilities for access and tracking of records), at regular review intervals (through the application of retention and disposal criteria), and ultimate disposal (whether this be recycling, archiving, or confidential destruction). By placing controls around the lifecycle of a record, we can ensure they demonstrate the key attributes of authenticity, reliability, integrity and accessibility, both now and in the future.
- 11. Through the effective management of the organisation's records, the SPSO can provide a comprehensive and accurate account of its activities and transactions. This may be achieved through the management of effective metadata¹ as well as the maintenance of comprehensive audit trail data.
- 12. We retain records that provide evidence of our functions, activities and transactions, for:

¹ Metadata can be defined in very general terms as 'data about data' and is necessary in order to understand the context, purpose, extent and location of a record. Examples of metadata can include information relating to a record's creator, creation date, receipt date, editor, access history and disposal.

- 12.1. Operational Use – to serve the purpose for which they were originally created, to support our decision-making processes, to allow us to look back at decisions made previously and learn from previous successes and failure, and to protect the organisation's assets and rights.
- 12.2. Internal and External Accountability – to demonstrate transparency and accountability for all actions, to provide evidence of legislative, regulatory and statutory compliance and to demonstrate that all business is conducted in line with best practice.
- 12.3. Historical and Cultural Value – to protect and make available the corporate memory of the organisation to all stakeholders and for future generations.

Why is records management important?

- 13. Information and records are a valuable corporate asset without which we would be unable to carry out our functions, activities and transactions, meet the needs of our stakeholders, and ensure legislative compliance.
- 14. The benefits of implementing records management systems and processes include:
 - 14.1. improved information sharing and the provision of quick and easy access to the right information at the right time;
 - 14.2. the support and facilitation of more efficient service delivery;
 - 14.3. improved business efficiency through reduced time spent searching for information;
 - 14.4. demonstration of transparency and accountability for all actions;
 - 14.5. the maintenance of the corporate memory;
 - 14.6. the creation of better working environments and identification of opportunities for office rationalisation and increased mobile working;
 - 14.7. risk management in terms of ensuring and demonstrating compliance with all legal, regulatory and statutory obligations; and
 - 14.8. the meeting of stakeholder expectations through the provision of good quality services.

Policy statement and commitment

- 15. It is the policy of the SPSO to maintain authentic, reliable and useable records, which are capable of supporting business functions and activities for as long as they are required. This will be achieved through the consolidation and establishment of effective records management policies and procedures, including:

- 15.1. The maintenance of a business classification scheme (BCS) to reflect the functions, activities and transactions of SPSO.
- 15.2. The review of the retention and disposal policy to provide clear guidance regarding the management of SPSO records and the correct procedures to follow when disposing of business information.
- 15.3. The review of information security policies and procedures in order to protect records and systems from unauthorised access, use, disclosure, disruption, modification, or destruction.
- 15.4. The review of data protection policies in order to demonstrate the SPSO's commitment to compliance with the data protection legislation and the safeguarding and fair processing of all personal data held.
- 15.5. The review of the business continuity plan, encompassing strategies to ensure vital records held by the SPSO remain accessible over time and there are processes in place to monitor the integrity and usability of records.
- 15.6. The regular review of audit trail mechanisms in WorkPro and the development of audit trail mechanisms for non-casework business records, in order to produce a clear strategy for improving the capture and management of key events in a record's lifecycle (for example, creation, access, editing, destruction or preservation).
- 15.7. The identification of records management as a distinct stream within the organisation's training portfolio, with dedicated training provided to all staff.
- 15.8. The completion of a self-assessment review, following the implementation of the records management plan in order to ensure that the records management practices remain fit for purpose and continue to act as exemplars within the profession in Scotland.

Roles and responsibilities

16. All staff have a responsibility to manage records effectively, through the documentation of all decisions and actions made by the SPSO; the effective maintenance of records throughout their lifecycle, including access, tracking and storage of records; the timely review of records and their ultimate disposal. All staff are responsible for suitably maintaining all records so that they can be easily retrieved, retaining all records in line with the retention and disposal schedule, ensuring that all actions and decisions are properly recorded and adhered to this policy.

The Head of Corporate and Shared Services (HoCSS)

17. The lead responsible officer for records management in the SPSO is the HoCSS. With the support of the Corporate Information Governance Officer, they have responsibility for ensuring compliance with this records management policy.

The Leadership Team

18. The Leadership Team, led by the Ombudsman, are responsible for approving a corporate approach to the management of records as defined within this policy, promoting a culture of excellent record-keeping principles and practices in order to improve business efficiency, supporting records management through commitment and the provision of resources and recognising the importance of preserving the SPSO's corporate memory.

Line Managers

19. All Line Managers are responsible for offering advice and guidance regarding records management to all staff within their responsibility and highlighting any records management issues or concerns to the Corporate Information Governance Officer or HoCSS as appropriate.

Corporate Information Governance Officer

20. The Corporate Information Governance Officer is responsible for ensuring that records management practices and procedures are established in line with all legal obligations and professional standards, issuing advice and guidance to all staff, and meeting the aims and objectives as outlined in the records management strategy.

Information Management support officers

21. IMSOs will provide advice on information management to colleagues. They have additional administrative rights and permissions in the eRDM. An IMSO should have a good understanding of business processes and the information needs of colleagues in their area, alongside a strong knowledge of the eRDM system so they can support users.

Legislative framework

22. The management of the SPSO's records is done so in line with the legislative, statutory and regulatory frameworks. Compliance with this policy will facilitate compliance with these acts, regulations and standards.

Relationship to other SPSO policies

23. This policy forms part of SPSO's overall framework but specifically relates to the policies contained within the SPSO Handbook - Information Governance (this document).

Training

24. A comprehensive training programme is provided to all staff in order to highlight and increase awareness of their responsibilities in line with data protection, freedom of information and records management. Furthermore, core competencies and key knowledge and skills required by staff with operational responsibility for records management will be clearly defined to ensure that they understand their roles and responsibilities, can offer expert advice and guidance, and can remain proactive in their management of record-keeping issues and procedures within SPSO.

Monitoring and review

25. The Corporate Information Governance Officer in consultation with the Leadership Team will monitor compliance with this Policy and related standards and guidance.
26. This policy will be reviewed in line with the SPSO Records Management Plan, in order to take account of any new or changed legislation, regulations or business practices.

Back to the main [Contents Page](#)

Business classification scheme

Issued: April 2015

Contents

Introduction	2
Casework documentation	2
Other documentation	2
SPSO business classification scheme and file plan.....	2
Electronic records access and restrictions.....	3
Electronic record and document management system (eRDM) for non-casework	4
Structure.....	4
eRDM management rules	5
Retention and disposal guidelines	6
Naming conventions	6
eRDM administration	7
SPSO IMSO - the role	7

Back to the main [Contents Page](#)

Introduction

1. The SPSO has a clear and discrete remit outlined in the Scottish Public Services Ombudsman Act. This is described in more detail on our website:
<https://www.spsso.org.uk/about-us>
2. The SPSO recognises that managing documents, and in particular electronic documents, presents a significant challenge for an organisation of any size or sector. Electronic record and document management needs to be very carefully considered and structured to ensure the integrity of the documents is not compromised upon capture and they remain retrievable for as long as they are required.

Casework documentation

3. Electronic documents for the casework functions of the SPSO are stored on a bespoke casework management system (CMS). Call recordings are held for a limited period on a safe, secure external server and subject to automatic destruction. If required for casework or information requests they are transferred to this system. This application provides an electronic document management system for the management of individual cases, and the documents created in our improvement, standards and engagement work with individual organisations within our jurisdiction. Documents are created and then stored electronically by a casework reference number. For complaints casework there may also be a corresponding paper file retained by the same reference number.

Other documentation

4. All other documentation, including corporate records, held by SPSO is mostly administrative or supports the casework functions¹, they are easily defined, highly structured; and whose access and retention is clearly determined. Electronic documents for non-casework functions of the SPSO are stored on a different electronic record and document management system (eRDM). The SPSO strives to be a paper-less office for these functions; therefore, the only central storage or archiving of paper files associated with these documents are for HR and financial legal requirements only.

SPSO business classification scheme and file plan

5. The business classification scheme (BCS) is modelled on the functions of the SPSO, and directly reflects the hierarchical relationship of functions, activities, transactions

¹ Casework strictly covers the documents needed to deal with individual cases. eRDM will hold documents which support that work such as policies, procedures, knowledge management, statistics, performance information etc.

and documents. This is supported by a detailed file plan to provide a logical structure to locate all documents to mitigate the risk of business critical information being lost.

6. The SPSO Business Classification Scheme and file plan is designed to underpin effective electronic documents management by ensuring:
 - 6.1. improved business efficiency through access to documents to enable informed and effective decision making;
 - 6.2. structured management of documents retained for legal and regulatory purposes;
 - 6.3. accurate capture and management of electronic documents;
 - 6.4. retention of a corporate memory of transactions, decisions and actions taken by, or on behalf of, the organisation;
 - 6.5. protection of the rights and interests of the organisation (and others) who the organisation retains documents about;
 - 6.6. protection of the characteristics of documents, particularly their reliability, integrity and usability; and
 - 6.7. identification of documents required for permanent preservation and archive.

Electronic records access and restrictions

7. SPSO operates the document management system under the values of open and transparent governance; therefore, all files are accessible by default to all colleagues and will only be restricted by exception:
 - 7.1. to protect personal data;
 - 7.2. to ensure safe and secure financial governance; and
 - 7.3. to enforce statutory disclosure restrictions.
8. Where required, restricted access is applied at the file level of the plan and to specifically named individuals. The list staff members in each of the restriction groups is contained in the detailed file plan for each year. The current plan is located at this link: [220105 SPSO eRDM File Plan - IMSO WORKING DOC \(A35559217\)](#)
9. SPSO casework requires additional protection for sensitive information. To limit the damage that may be caused by a cyber-incident and ensure protection of the personal data held within case files, staff access to cases within the case management application is aligned by role and team. Within the casework management application access restrictions are managed through the Okta Group Membership as part of the user access to the SCOTS network. The lists of group memberships is located at this link: [220818 WorkPro Okta group membership \(A40249083\)](#)

10. In addition, a small number of staff have the ability to lock specific cases to only be accessible to specific named users, when authorised by the leadership team. Cases that meet identified criteria on receipt will be restricted on receipt, and these restrictions may be reviewed and changed during the progress of the case.

Electronic record and document management system (eRDM) for non-casework

11. SPSO has adopted the electronic record and document management system (eRDM), as offered on the SCOTS network, to manage the business classification scheme and file plan. eRDM provides a variety of functions including access controls, auditing and disposal using a combination of system and user generated metadata.
12. The benefits of the eRDM to manage the business classification scheme and file plan include:
 - 12.1. determining where a document should be placed in a larger aggregation of documents;
 - 12.2. assisting users in retrieving documents;
 - 12.3. assisting the responding to requests for information by ensuring only one copy of a document, or location for document exists;
 - 12.4. assigning and controlling retention periods; and
 - 12.5. assigning and controlling access rights and security markings.

Structure

13. The structure of the file system is determined by the eRDM. This structure conforms to a typical 'functional' filing structure, with three levels of folders that act as segregations for information, representing the functions, activities and transactions. The fourth file level sits beneath these to contain the individual documents. This model is to prevent users from creating idiosyncratic, sub-folder structures below the file level which do not conform to the management rules.
14. The file level is most critical. It is a type of aggregation or container within the eRDM used to store documents and pictures. It is the principal building block of a file plan and the level at which documents are managed through their lifecycle (for example, for disposal or retention).
15. There are eight functions at level one of the Business Classification Scheme:

Function	Description
Admin Groups – non-casework	Includes administration documents for long-term groups and communities of practice; and team administration. Products of these groups are stored in the appropriate function below
Communications	Includes all presentations, templates, contact / mailing lists, and website publications
Corporate governance	Includes facilities; finance; planning, incident and risk management; organisation history; information governance; official statistics; policies; and service standards
Human resources	Includes learning and development; pay and reward; health and wellbeing; organisational development; and reporting
Information and Communications Technology	Includes applications; hardware; and systems
Stakeholder Engagement non-casework	Includes all non-casework interaction with external organisations and individuals
Standards External	Complaints Standards Authority, external training unit
Supporting casework	Includes Connect sharing space for casework; IPA; guidance; support and intervention policy; and legal advice.

16. The detailed file plan based on this structure is in [this document](#).

eRDM management rules

17. Management rules are explicit instructions to users on the preferred means of managing documents within the eRDM. These include direction on appropriate capture, access management and disposal of all documents irrespective of format or media.
18. All documents contained within a single file will have the same access and retention rules applied, regardless of the date they were created.

Retention and disposal guidelines

19. Open, retention and disposal workflows for the lifespan of each file are controlled by the file type the file was created with. There are four specific SPSO file types and one existing Scottish Government file type we will access:

File Type name	Open file (Jan - Jan)	Retention File closure +	Actions
SPSO Administration	2 years	+ 2 years	open-close-destroy
SPSO Corporate	2 years	+ 6 years	open-close-destroy
SPSO Legal	5 years	+ 10 years	open-close-review-destroy
SPSO Historic	1 year	+ 99 years	open-close-review-destroy
Employee Personnel Records Casework (existing SG file type)	Close on exit from employment	+ 100 years after date of birth	open-close-destroy

20. The retention and disposal rules for different activities are outlined in the [Retention and Disposal policy](#).

Naming conventions

21. A disciplined approach to naming files and documents is very important, as it greatly assists users with searching and retrieval of the required documentation. Documents are stored in the eRDM database by an identification number. This number is used for linking and sharing purposes. The search and browsing feature works best with a maximum of 1000 documents stored within a file.
22. General guidelines for naming items in the eRDM are:

Folders and files:

- 22.1. files must be titled as specifically and simply as possible, identifying the logical element of the filing structure. This can be achieved by using the following structure: Topic – Type – Time. Time refers how long the file is open for according to its file type, usually two years. For example: 'Customer Service Complaints – 2022-23 Reports: 2022-2024'; and
- 22.2. acronyms should not be used for naming folders or files. However, they can be bracketed after the text is spelled out in full, for ease.

Documents:

- 22.3. name documents consistently and clearly, using a structure that supports the easy location of each document;

- 22.4. each document's name should include a date reference;
- 22.5. use the shortest name possible, using sentence case; with spaces between words to enable the document to be found in the search function;
- 22.6. use the date convention: YYMMDD. This can be used at the beginning, middle or the end of the document name, depending on grouping requirements, and should be consistent within the file. The order of the date and name will dictate the order in which the documents are listed, therefore, for some groups of documents it may be appropriate to group by common name differentiated by date, for others to list them by date order with more descriptive names; and
- 22.7. use document naming to group documents together by type or in date order, for example, 'LT Q1 191129 – 01. Agenda', '2019 Declaration AAB JC'.

eRDM administration

- 23. Administration for the eRDM is provided by iTECS, including initial set-up of the SPSO file plan, application of the retention and disposal rules to each file, and the application of access restrictions to each file.
- 24. SPSO Information Management Support Officers (IMSO) are named members of staff with additional administrative rights in the eRDM. All IMSOs will be trained to use the eRDM system.
- 25. Document owners have more administration rights over their own documents, such as changing location, than over other documents. Document owners can be changed over the life of the document where required.

SPSO IMSO - the role

- 26. SPSO Information Management Support Officer (IMSO)s will provide advice on information management to colleagues. They have additional administrative rights and permissions in the eRDM.
- 27. An IMSO should have a good understanding of business processes and the information needs of colleagues in their area, alongside a strong knowledge of the eRDM system so they can support users.
- 28. IMSO tasks will include:
 - 28.1. helping colleagues with their use of My Home and Handy folders;

- 28.2. support file management by creating groups and creating and approving file requests;
- 28.3. managing documents with corporate value or restrictions and checking naming conventions; and
- 28.4. the IMSO also supports new staff in completing their eRDM - introduction for new staff e-learning and completing processes for staff who are leaving.

29. They would be responsible for:

- 29.1. liaising with iTECS with all administration requests, including new files, and changes workflow rules and access requirements;
- 29.2. ensuring SPSO eRDM guidelines are implemented correctly;
- 29.3. reviewing iTECS reports for retention and disposal of documents; and
- 29.4. providing advice on information management to colleagues.

[https://scotsconnect.sharepoint.com/sites/MyWork/SitePages/information-management-support-officers-\(imsos\).aspx](https://scotsconnect.sharepoint.com/sites/MyWork/SitePages/information-management-support-officers-(imsos).aspx)

Back to the main [Contents Page](#)

Case file management guidance

Issued: December 2010

Contents

WorkPro case file management.....2

 Additional supporting paperwork4

 Post closure activity (PCA) and landmarks.....5

Retention and disposal of case files6

 Retention and disposal of scanned paperwork.....6


 Retention and disposal of casework notes7

Additional Resources7

Back to the main [Contents Page](#)

WorkPro case file management

1. The primary records for all case types are kept on WorkPro, with any paperwork scanned and uploaded (then securely disposed of for destruction). A hard copy file should only be created when necessary, if there is additional supporting paperwork which cannot be scanned or stored electronically (see [Additional Supporting Paperwork](#)).
2. The case owner (or other person working on the case if post-closure, such as an Executive Casework Officer) is responsible for ensuring the record is in order and is properly maintained.
3. Documents on the record should be named to make it clear what they contain (see [Workpro Document Naming Convention guidance](#)).
 - 3.1. Documents should be contained in the correct folders and labelled with accurate activity dates.
4. Apart from specific fields where personal data is required (such as contact details) information should be pseudonymised (data that cannot be linked to an individual without additional information, for example, by replacing names or other identifiers that are easily attributed to an individual with a reference number).
 - 4.1. This is especially important for information added to fields where content is retained after [file disposal](#)). See [Annex 1 of the Retention and disposal policy](#) for the full table of retained fields.
 - 4.2. Where it is possible to do so, file notes and emails should also be pseudonymised.
5. If a hard copy file is created, the file location on WorkPro must be updated to reflect this, and kept up-to-date.
6. A record should be kept of any information that is taken out of the office and when it is returned.
7. When requested, original documents should be scanned and returned at the earliest opportunity (see [Retention and disposal of scanned paperwork](#)).
 - 7.1. Where documents are particularly large, contain sensitive information, or are originals, they should be returned by the secure courier (see separate courier guidance).

8. Where scanning is not possible, the additional hard copy supporting documentation should be clearly signposted within the WorkPro case file, in line with [additional supporting paperwork guidance](#).
9. We should not usually accept information on removable electronic storage devices. Information should instead be provided via Connect if email is not appropriate. If it is necessary to retain a device it should be appropriately secured in the supporting paperwork file and signposted on the WorkPro case file.
 - 9.1. Any electronic storage devices we hold must be encrypted.
 - 9.2. We should only retain electronic storage devices where it is not possible to hold the information on WorkPro (as in the case of radiology images, which require special software to view).
 - 9.3. We should only accept electronic storage devices from Boards where it is not possible to provide the information  via Connect (or the Sectra Image Exchange Portal (IEP)).
10. Absolutely no electronic case documents should be stored in email folders, OneDrive, or other locations. Case documents must not be stored anywhere other than WorkPro, with the exception of using Connect (or the Sectra IEP) to securely share documents on a temporary basis.
11. When requesting information from authorities / complainants / applicants / advisers, ask that this be provided electronically where possible, and proactively offer the use of Connect if email is not appropriate.
12. Documents which are shared using Connect should not be renamed when saving to the record. This is to ensure that it is clear exactly what information has been shared even after the workspace has been deleted.
 - 12.1. Where documents are created or amended specifically for sharing using Connect, these documents should be saved to the record even if they contain information already on the record.
 - 12.1.1. For example: if a BUJ sends several separate files, but these files are merged into a single file before sending to an adviser using Connect, both the separate files and merged file should be saved to the record.
 - 12.2. Where documents are not amended before sharing with Connect, only one copy of the document needs to be saved to the record (see [16] below).

13. Documents should be deleted from Connect as soon as they no longer need to be shared.
14. Only relevant information should be retained on the case record. If we have been sent information that isn't relevant, it should be deleted or redacted.
15. In line with our call recording policy, only save and / or retain a telephone recording to the case record if it is necessary to do so (that is, when a telephone note is not sufficient).
16. As far as possible, remove and destroy all duplicate copies of documents held on the WorkPro case file.
 - 16.1. Generally, drafts of letters and reports should not be retained on file once the final version of the document has been agreed.
 - 16.2. The only exception to this is the draft version of a public report which is issued to all parties for comment. A copy of this should be kept to assist in the event that details are questioned or disputed at a later date.
17. Intelligence reports provided by the Scottish Prisons Service in the course of an investigation should be destroyed once a decision on the complaint has been issued.
18. When a case contains particularly sensitive data, access should be restricted to only those for whom it is essential.
 - 18.1. All INWO cases are set to restricted access by default.
 - 18.2. Information request and CSC cases which contain any identifiable information related to restricted cases should also be set to restricted access.
19. The electronic record must be kept up-to-date to the point of disposal, including the period after the case is closed.

Additional supporting paperwork

20. Where hard copy documentation is provided that cannot be scanned (such as CDs containing radiology images) or are prohibitively difficult to scan (such as very large volumes of medical records) this should be stored in a supporting paperwork file.
21. Care should be taken that information from different cases is not accidentally filed together.
22. Supporting paperwork files should be clearly labelled with the complaint reference number and complainant surname on the front and side of the file. They should also

be labelled as confidential and with the SPSO contact details, in case of loss outside the office.

23. Where there are multiple supporting paperwork files for the same case (for example, medical records) each file should be numbered and indicate the total number of files, such as 'volume 2 of 3'.
24. All documents within the supporting paperwork file must be numbered or otherwise labelled (using dividers, for example), with these details noted on the WorkPro file. It should be clear on the WorkPro file exactly what is contained in the supporting paperwork file.
 - 24.1. For example, 'documents received from BUJ' is not by itself sufficient. Additional details such as 'medical records (files 1-2), complaint file (file 3)', should also be included.
25. If it is necessary for a paper file to be removed from the office (for example, so it can be worked on from home, or shared with an adviser), this must be done securely. If being transferred by courier, the [courier process](#) should be followed.
 - 25.1. Information should be shared electronically using Connect wherever possible.
 - 25.2. It is important to ensure the file location on the WorkPro record is kept up-to-date.
26. When the complaint is closed, supporting paperwork files should be passed to the team assistant for filing in the office archive.
 - 26.1. Only paperwork which cannot be held electronically should be filed in the archive. Any printed paperwork or hard copies of information are considered casework notes and should be disposed of [as described below](#).

Post closure activity (PCA) and landmarks

22. If significant work needs to be done on a case but it does not meet the criteria for being reopened, or it is unclear whether or not it should be reopened, the activity should be logged as 'post closure activity'.
23. Adding post closure activity to a record will delay the case going through the file disposal process for an additional 14 months from the date the PCA is closed.
24. For cases which need to be retained in full or in part for longer than the standard period (for example, if they are of national historic interest, are relevant to ongoing public inquiries, or are significant for our office) a landmark can be added.

- 24.1. The file will be exempt from the file disposal process for as long as the landmark is active.
 - 24.2. A clear reason for adding the landmark must be included in the appropriate field.
 - 24.3. A date to review the landmark must be set for no more than five years from the creation of the landmark (or the last review).
25. The responsibility for adding a PCA or landmark lies with the person who is working on the case post-closure, which may not necessarily be the case owner.

Retention and disposal of case files

26. Cases go through the file disposal process at 14 and 26 months after the last significant activity on the case. Significant activity is considered to be:
- 26.1. Case closed date
 - 26.2. Last review closed date
 - 26.3. Last CSC closed date
 - 26.4. Last PCA closed date
27. At 14 months paper case files and any hardcopies of additional supporting paperwork will be destroyed.
28. At 26 months the documents on the WorkPro electronic casefile will be destroyed, specific fields containing personal data will be anonymised, and all information held in other fields will be deleted except for those specified in [Annex 1 of the Retention and Disposal Policy](#).
29. No documents are to be added to a case which has gone through the file disposal process. If documents or actions need to be recorded after a case has been destroyed, a new case file should be created.

Retention and disposal of scanned paperwork

30. Scanned paperwork should be reviewed on WorkPro by the case owner at the earliest opportunity and within one month of scanning, or in the case of complaints which have not yet been allocated, within one month of allocation. This is to ensure the scanned version has been checked before hard copy of the paperwork is destroyed.
- 30.1. Hard copy documents for new complaints which have been scanned will be stored in batches by the calendar month in which they were scanned. Each

batch will be destroyed one month after the last case in the batch has been allocated.

- 30.2. Hard copy documents for allocated complaints which have been scanned will be stored in batches by the calendar month in which they were scanned. Each batch will be destroyed on or as close as possible to the last day of the following month.
- 31. If asked to return any hard copy documents, the case owner must make a team assistant aware at the earliest opportunity so that the hard copy can be located quickly and returned before its batch is destroyed.
- 32. The team assistant will maintain a record of paperwork destroyed, noting the batch month and date of disposal.
 - 32.1. The team assistant will confirm to Information Governance on a monthly and quarterly basis that all appropriate batches have been destroyed and all existing paperwork is held in the designated place.

Retention and disposal of casework notes

- 33. Where possible any additional notes made regarding casework should be held electronically on the WorkPro record.
- 34. Where notes are held in hard copy, these must be stored securely, whether at home or in the office.
- 35. Use pseudonymisation wherever possible.
- 36. Only transport notes between locations if absolutely necessary, for example when returning them to the office for destruction, and ensure they are transported securely.
- 37. Notes should be destroyed when they are no longer required, at the earliest opportunity. Any notes held at home should be securely returned to the office to be destroyed as confidential waste.

Additional Resources

[INWO Casework Guidance](#)
[Process for sending items by courier](#)
[Courier instructions for CRs and advisers](#)
[Workpro Document Naming Convention guidance](#)
[Working from home checklist](#)

Back to the main [Contents Page](#)

Retention and disposal policy

Issued: December 2010

Contents

Introduction	2
Statutory Obligations	2
Legislative considerations and models of best practice.....	2
SPSO casework (including Information Requests) retention and disposal periods....	3
Casework retention period.....	4
Casework reports	5
Casework disposal plan	5
Other documents	6
Non-casework disposal.....	8
Memorandum of Understanding with National Records of Scotland (NRS).....	8
Roles and responsibilities	8
Monitoring and review.....	9
Annex 1: SPSO casework – open fields retained.....	10
Annex 2: SPSO other documents retention periods.....	13
Annex 3: British Library Web Archive Licence	18
Annex 4: National Records of Scotland.....	20

Back to the main [Contents Page](#)

Introduction

1. The SPSO recognises that its administrative documents are a unique and irreplaceable resource. The effective management of our documents, regardless of format, is essential in order to support our core functions, to comply with legal, statutory and regulatory obligations, and to demonstrate transparency and accountability to all its stakeholders. The SPSO Records Management Policy sets out a commitment to the implementation of an efficient and effective documents management system. Crucial to the success of the policy is the development and implementation of a retention and disposal schedule.
2. This retention and disposal policy aims to identify documents which should be retained because of their legal, statutory and regulatory obligations, or long-term historical/research value, and enable the SPSO to dispose of documents promptly when they cease to be of any continuing administrative/legal value.
3. The policy is to be read in conjunction with the [Records Management Policy](#) for the SPSO, which details the importance of managing documents effectively within the organisation, outlines key aims and objectives for SPSO in relation to its record-keeping, and acts as a mandate for the support and delivery of documents management policies, procedures and initiatives across the organisation.

Statutory Obligations

4. The management of the SPSO's documents is done so in line with legislative, statutory and regulatory framework. Compliance with this policy will facilitate compliance with these acts, regulations and standards.

Legislative considerations and models of best practice

5. Freedom of Information (Scotland) Act 2002 (FOISA), Environmental Information Regulations 2004 and Data Protection Legislation have provisions entitling individuals to request information that is held by SPSO, but do not oblige the SPSO to keep information longer than is required for its purposes.
6. These Acts, therefore, do not determine standard retention periods, although where possible information that has been requested under FOISA, EISR or Data Protection Legislation but withheld by SPSO should not be destroyed until the time allowed for the requestor to request a review and / or appeal has lapsed.
7. The SPSO holds both casework and non-casework related information. Case work covers information held for the purpose of responding to public enquiries, complaints, welfare fund reviews and information requests.

8. The Scottish Public Services Ombudsman Act 2002, Welfare Funds (Scotland) Act 2015, and Public Services Reform (SPSO) (Healthcare Whistleblowing) Order 2020 do not determine specific periods for retaining case-related information. The 2002 Act does state that¹

'The Ombudsman must not consider a complaint more than 12 months after the day on which the person aggrieved first had notice of the matter complained of, unless the Ombudsman is satisfied that there are special circumstances which make it appropriate to consider a complaint made outwith that period'

9. The Section 61 Code of Practice on Records Management² describes good practice for Scottish public authorities to follow. In Part 1: Records Management it states:

'3. Keeping records to meet corporate requirements: Authorities should ensure they keep records they will need for business, regulatory, legal and accountability purposes.'

'7. Disposal of records: As a general principle, records should be kept for as long as they are needed by the authority: for reference or accountability purposes, to comply with regulatory requirements or to protect legal and other rights and interests. Destruction at the end of this period ensures that office and server space are not used and costs are not incurred in maintaining records that are no longer required. For records containing personal information it also ensures compliance with the fifth data protection principle³.'

10. In the absence of prescriptive legislation and regulations, the overriding determinant is what suits the business requirements of the organisation.

SPSO casework (including Information Requests) retention and disposal periods

11. Casework information is stored in electronic format. We also hold paper copies of some files. These paper files will include information submitted to SPSO but not scanned into the electronic record.
12. Following consideration of the existing legislation and business requirements of SPSO the retention times for SPSO casework is approved as follows:

¹ Scottish Public Services Ombudsman Act 2002, section 10 (1)

² <https://www.gov.scot/publications/code-of-practice-on-records-management/>

³ "Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed"

Casework retention period

13. SPSO have identified they should retain most casework data, including personal information, on individual case files for 26 months after the last activity date to meet business purposes. This will include calls downloaded on to the case file. The call recording policy sets the limit for call recordings not downloaded to 90 working days. Calls may be deleted earlier if there is reason to do so under that policy. The last activity date relates to direct casework actions:
 - 13.1. case closed actual date (different field names for different case types);
 - 13.2. last review actual date;
 - 13.3. last PCA actual date;
 - 13.4. last CSC actual date;
 - 13.5. last enquiry tracker actual date; and
 - 13.6. last Recommendations actual date.
14. Data is required to be retained for different purposes: for example to allow for quality assurance activities, dealing with customer concerns, tracking multiple complaints/reviews on the same issue or from the same person, using our casework for our own learning and development, and protecting staff from difficult behaviour⁴.
15. When we hold a paper file as well as the electronic record, we have identified that we do not need to keep the full paper file to achieve our purposes for more than 14 months. Retaining paper files raises the risk of storage problems including files becoming misplaced, damaged or lost.

Exceptions:

16. Some individual cases need to be retained in full or in part for longer for specific business, legal or other reasons. This may be because the case is of national historic interest, there are ongoing public inquiries, or the case is a significant one for our office. When retaining cases for longer than the standard 14 or 26 months, we must identify a clear reason for doing so and set a review date which should be no longer than five years (Note: cases can be kept for longer but reviews should be conducted at least every five years).
17. We will also keep evidence/documentation necessary for any information request or to deal with a customer service complaint. This may mean we extend the retention period for an individual case file or files beyond 14 or 26 months.

⁴Full detail of all purposes for which we process data is held in our [data processing register](#)

18. Intelligence reports provided to us by the Scottish Prisons Service in the course of an investigation are destroyed on the issue of the decision on the case.

Personal data

19. While most personal data does not need to be retained for more than 26 months, we have identified that we should retain some casework data on an anonymised or pseudonymised basis indefinitely. This primarily comprises information which is useful for statistical and tracking complaints trends purposes such as reasons closed, subjects, organisation complained about.
20. Some information is kept to monitor information requests. Summary, decision and recommendation information is also retained because of the record they provide of our own work and approach. Names of SPSO staff associated with cases are retained in the database until they cease employment. The only details that are retained apart from their name are their business contact details. Names of authority staff are pulled through from a live section of the database and are retained as part of an administrative record and not pseudonymised / anonymised with the individual record.
21. In terms of file management, we retain most drop down or selected data for these purposes. Annex 1 sets out the open texts fields we retain and the specific reason for retaining them.

Casework reports

22. SPSO produces individual reports of casework which are laid before Parliament. These pseudonymised reports laid before the Scottish Parliament are published and kept by the SPSO and the Scottish Parliament indefinitely in electronic form.

Casework disposal plan

23. Once cases have met the minimum retention period, SPSO need to ensure we have in place an appropriate disposal plan to ensure safe, secure disposal of information we no longer need to retain.
24. Reports are run on our database regularly to identify cases which have met the 14 month and 26 month period.
25. Physical files only exist for certain cases. For those cases which do have a physical file and have met the 14 month period, the physical file is securely disposed of, and the date of file management is noted on the individual case record.
26. For cases which have met the 26 month period, and where we have not identified an individual reason to keep the cases for a longer period, we run a file management

programme which deletes all electronic documents attached to the file, and the electronic database is stripped of information we no longer have a purpose to keep. The date of file management is noted on the individual case record. See Annex 1 for details of open fields retained.

27. Link to WorkPro FM guidance: [Workpro FM – Archiving process details](#)
28. The Ombudsman and leadership team have the authority to pause the disposal program and will note any reason for doing so.

Other documents

29. For some non-casework administrative functions of the organisation there is legislation which dictates the minimum retention period specific types of record are required to be retained. This section and [Annex 2](#) describe the areas where we have identified legislation which directly impacts on the retention of information we hold. These statutes set minimum timeframes and these have been taken into account when setting our retention timescales.
30. The SPSO creates and receives a variety of documents which are necessary for carrying out the business of SPSO which are subject to more specific controls and regulations than is the case with casework documents. Organisations do not have any discretion over the retention period for many types of documents as the legislation dictates the required period.
31. The table at [Annex 2](#) identifies the retention periods for documents which are not discretionary. For those documents where there is discretion, the SPSO policy is to retain documents for only as long as there is a business requirement for the record, unless of legal value or historical interest.
32. Published documents are contained on the SPSO websites. The SPSO websites are listed with the [UK Web Archive](#), whose purpose is to give permanent online access to key UK websites for future generations and this provides for permanent retention of those documents. The current licences are attached at [Annex 3](#).
33. SPSO use five file types to manage the retention and disposal of different documents held within the electronic record and document management system (EDMS eRDM). Only some human resources and financial documents are held in hard copy, if legally required.
34. The file types applied in EDMS eRDM are:

- 34.1. SPSO Administration file type is used for most general operation and administration documents, which are only retained for two years after the file is closed.
- 34.2. SPSO Corporate file type covers most corporate administration and governance functions, such as audit and finance, and by retaining documents for six years after closure meets the majority of the legal requirements for these types of documents. This is also the file type used for key stakeholder engagement. By retaining documents in this file type for six years after closure, the majority of the legal retention requirements for these types of documents is met.
- 34.3. SPSO Legal file type is for legal advice received and documents relating to changes to our legislation, which we require to hold for a longer period given the impact to the organisation and need to reference these documents over a long period of time. This file type is subject to review at closure.
- 34.4. SPSO Historic file type is for documents that need to be kept for significant periods. There is a long retention of 99 years which reflects this may contain documents which could be kept permanently but are not suitable for normal publication. However, documents within this file type may be disposed of before that time frame if appropriate and not all will need to be kept permanently. This file type may be used for:
- 34.4.1. documents of national historic interest, subject to the NRS MOU, but may also be used to document;
 - 34.4.2. key changes to SPSO procedure, governance, legislation that may be of use to SPSO in the longer term and act as our archive;
 - 34.4.3. documents we need to keep for longer than the legal file type but that do not sit within the HR file type. (This allows us to retain this data appropriately without the need to create individual file types for limited data); and
 - 34.4.4. this file type is subject to review at closure.
- 34.5. Employee Personnel Records Casework file type is self-explanatory.

35. In summary:

File Type name	Open file	Retention File closure +	Actions
SPSO Administration	2 years	+ 2 years	open-close-destroy
SPSO Corporate	2 years	+ 6 years	open-close-destroy

SPSO Legal	5 years	+ 10 years	open-close-review-destroy
SPSO Historic	1 year	+ 99 years	open-close-review-destroy
Employee Personnel Records Casework (existing SG file type)	Close on exit from employment	+ 100 years after date of birth	open-close-destroy

Non-casework disposal

36. Secure arrangements for the disposal of materials are in place using the following processes:
- 36.1. identification of eligible documents for disposal as outlined in this policy, ensuring precedents and other material for longer term retention are located in the historical file type for secure storage;
 - 36.2. secure disposal of material in accordance with agreement with contractor; who will comply with the British Standard: Secure Destruction of Confidential Material – Code of Practice BS EN 15713:2009, and
 - 36.3. updating and secure storage of disposal audit file.

Memorandum of Understanding with National Records of Scotland (NRS)

37. The MoU sets out the understanding between the Keeper and the SPSO on how the process of depositing, storing and accessing documents of enduring historical, cultural and research value which have been transferred from the SPSO to NRS will operate. Deposit of these archival documents in NRS is pursuant to section 5 of the PR(S) Act 1937 and in fulfilment of the SPSO's record management obligations under the PR(S) Act 2011 as also stated in the SPSO's published records management policy statement. For further details, please refer to our [Memorandum of Understanding with The Keeper of the Records of Scotland](#).

Roles and responsibilities

38. The Ombudsman has overall responsibility for ensuring that the SPSO complies with the requirements of legislation affecting the management of documents, and with any supporting regulations and codes.
39. The HoCSS is responsible for:
- 39.1. ensuring that the Records Management Policy is implemented effectively;
 - 39.2. the provision of record management guidance to staff;

- 39.3. producing procedures documenting all necessary record management arrangements;
 - 39.4. regularly reviewing and where necessary amending record management policies and procedure statements; and
 - 39.5. making recommendations to the Leadership Team in relation to changes or improvements.
40. Line managers are responsible for:
- 40.1. ensuring that the agreed records management policy and procedures are fully observed and implemented within their area of responsibility; and
 - 40.2. ensuring that all staff within their area of responsibility receive the appropriate training.
41. All members of staff are responsible for documenting their actions and decisions, and for maintaining the documents in accordance with the SPSO's agreed policies and practices.

Monitoring and review

42. The policy will be reviewed every two years or as legislation or policy change dictates.

Annex 1: SPSO casework – open fields retained

Case type	Fields retained	Reasons for retention
Complaint	Summary	Keeps a record of issues brought and our decision to allow us to monitor trends over a longer period but also to keep a history of our office's approach. This will also help us by providing information for development purposes/review of policies/standards.
	Heads of complaint	Keeps a record of subjects investigated us to monitor trends over a longer period but also to keep a history of our office's approach. This will also help us by providing information for development purposes/review of policies/standards.
	Recommendations	Keeps a record of actions we have asked organisations to commit to us to monitor trends over a longer period but also to keep a history of our office's approach. This will also help us by providing information for development purposes/review of policies/standards.
	Knowledge capture comments	This is the section we use to highlight information we want to keep but which might not be captured above. Importantly it includes if equalities issues have been relevant. Again this to monitor trends over a longer period but also to keep a history of our office's approach. This will also help us by providing information for development purposes/review of policies / standards.
	Complaints handling comments	This is where we retain details of complaints handling issues This to monitor trends over a longer period but also to keep a history of our office's approach. This will also help us by providing

Case type	Fields retained	Reasons for retention
		information for development purposes / review of policies / standards.
Welfare fund reviews	Summary	Keeps a record of issues brought and our decision to allow us to monitor trends over a longer period but also to keep a history of our office's approach. This will also help us by providing information for development purposes / review of policies / standards.
	Findings details	Keeps a record of decisions made (similar to heads of complaint etc above) allowing us to monitor trends over a longer period but also to keep a history of our office's approach. This will also help us by providing information for development purposes/review of policies/standards.
	Recommendations	Keeps a record of actions we've asked organisations to commit to us to monitor trends over a longer period but also to keep a history of our office's approach. This will also help us by providing information for development purposes/review of policies / standards.
	Knowledge capture comments	This is the section we use to highlight information we want to keep but which might not be captured above. Importantly it includes if equalities issues have been relevant. Again this to monitor trends over a longer period but also to keep a history of our office's approach. This will also help us by providing information for development purposes/review of policies / standards.
	Complaints handling comments	This is where we retain details of complaints handling issues This to monitor trends over a longer period but also to keep a history of

Case type	Fields retained	Reasons for retention
		our office's approach. This will also help us by providing information for development purposes / review of policies / standards.
Information requests	<p>Appeal > Appeal Details Appeal > Appeal Outcome Details Appeal > Appeal source Appeal > Notes Information Request > Request Details Information Request > Response Details Information Request > Notes / Missed Target Reason Information Request > Incident or breach > Incident Source Information Request > Incident or breach > Incident Reported to Information Request > Time taken (mins) Review > Review Request Details Review > Review Response Details Review > Notes</p>	We are retaining more open text fields in the information request case type. These reflect that the open fields are used to track our decision-making and key aspects of our approach to individual rights requests, complaints, and incidents. Fields are retained to allow us to monitor our trends and our decision-making. They also help us to comply with information legislation.

Annex 2: SPSO other documents retention periods

The table below identifies retention periods which are not discretionary.

Category	Type	Retention Period	Legislation/Guidance
Finance and Audit	Annual accounts	Permanent	The Local Authority Accounts (Scotland) Regulations 1985. SI 1985 No. 267 (S. 24)
	Records documenting the preparation of the consolidated annual accounts and financial statements	six years from end of financial year	Taxes Management Act 1970, c9
	Asset registers, depreciation and disposal registers	six years from end of financial year	Taxes Management Act 1970 c9; Prescription and Limitation (Scotland) Act 1973 c.52 and 1984 c.45; VAT Act 1994; Audit Commission Act 1998
	Long term strategy and planning -major records (3 year financial plan; financial strategic forecast)	Permanent	Retain for business and historical value
	Financial transactions management records: authorisation, bank account documents, payment instructions, processing of payment; petty cash, fraud investigation, funding application, associated records, refunds.	six years from end of financial year	Taxes Management Act 1970 c9; Prescription and Limitation (Scotland) Act 1973 c.52 and 1984 c.45;
	Register of gifts and hospitality received by individual members of staff	ten years	Business Requirement - Standards Commission
	Payroll records (including P45, P60, Statutory Sick Pay, Statutory Maternity Pay)	six years from end of financial year	Income Tax (Employments Regulations) S.I. 1993 / 744; National Minimum Wage Regulations S.I. 1999 / 584; Taxes Management Act 1970; Prescription and Limitation (Scotland) Act 1973 c.52 and 1984 c.45;

Category	Type	Retention Period	Legislation/Guidance
			Statutory Sick Pay (General) Regulations S.I. 1982 / 894 The Statutory Maternity Pay (General) Regulations S.I. 1986 / 1960 as amended by SI 2005 No 989
	Pension scheme reports	six years after end of current year	Taxes Management Act 1970; Income and Corporation Taxes Act, 1988
	Individual staff pension files	ten years after date of payment	The Local Government Pension Scheme (Management and Investment of Funds) (Scotland) Amendment Regulations, SSI 2000 No. 74
	Internal Audits records re provision and management of internal audit service (not specific to individual audits); investigations involving prosecution, disciplinary action etc	five years	Prescription and Limitation (Scotland) Act 1973
Procurement and Risk Management	Contract management files - ordinary contracts	five years from end of contract	Prescription and Limitation (Scotland) Act 1973 c.52 and 1984 c.45 S.I. 1991 No.2680 The Public Works Contracts Regulations 1991 S.I. 1993 No.3228 The Public Services Contracts Regulations 1993 S.I. 1995 No.201 The Public Supply Contracts Regulations 1995 S.I 2003/46 The Public Contracts (Works, Services and Supply) and Utilities Contracts (Amendment) Regulations 2003
	Approved supplier evaluation criteria records	five years after being superseded	Prescription and Limitation (Scotland) Act 1973 c.52 and 1984 c.45
	Purchase ordering records	six years from end of financial year	Prescription and Limitation (Scotland) Act 1973 c.52 and 1984 c.45

Category	Type	Retention Period	Legislation/Guidance
			HM Customs & Excise Notice 700/21: Keeping [VAT] records and accounts (December 2007)
	Tenders – Initial proposal, including business case/requisition; contract advertisement, statements of interest (successful); pre-qualification questionnaire (PQQ) and evaluation, draft and agreed specification, evaluation criteria, ITT	five years from end of contract	Prescription and Limitation (Scotland) Act 1973 c.52 and 1984 c.45 Records required by S.I 1991/2680; S.I 1993/3228; S.I 1995/201; SI 2003/46
	Tender evaluation, negotiation and notification records - Successful tenders	five years from end of contract	Prescription and Limitation (Scotland) Act 1973 c.52 and 1984 c.45; S.I 1991/2680; S.I 1993/3228; S.I 1995/201; SI 2003/46
	Tender evaluation, negotiation and notification records - Unsuccessful tenders	one year from award of contract	S.I 1991/2680; S.I 1993/3228; S.I 1995/201; SI 2003/46; records relating to second and third choice contractors may be kept throughout contract to avoid re-tendering if successful contractor withdraws service
	Statistical reports to Scottish Government on contracts awarded	five years from date of creation	Prescription and Limitation (Scotland) Act 1973 c.52 and 1984 c.45
Human Resources	Employee files, including Counselling, discipline, employment conditions, Grievances, training, sickness monitoring, equal opportunity documents	six years from termination date	Prescription and Limitation (Scotland) Act 1973 c.52 and 1984 c.45 The Employment Act 2002 ACAS Code of Practice Disability Discrimination (Public Authorities) (Statutory Duties) (Scotland) Regulations 2005. SSI 2005 No 565 Regulation 2.

Category	Type	Retention Period	Legislation/Guidance
			Sex Discrimination (Public Authorities) (Statutory Duties) (Scotland) Order 2007 SSI 2007 No 32. Article 3, 5, 6 The Equality Act 2010 (Gender Pay Gap Information) Regulations 2017 No. 172 Regulation 15
	Employee details (posts subject to disclosure checks)	25 years from termination date	Statute of Limitation 1980. Need to retain record of: Name, DOB, Date of Appointment, Work history details, Titles and dates of posts held, as evidence of employment and for pension purposes
	Equalities and diversity - Investigations - Case Files	five years after investigation concludes and action is spent / Retain current information throughout employment	SCARRS
	Occupational health – sickness monitoring, personal risk assessments, absence reporting	six years from termination date	Access to Medical Reports Act 1988 c28 provides the general provisions on the right of access to records created after 01 January 1989
	Occupational health (separate from employee file)	75 years from DOB	Where statutory health surveillance has been undertaken records to be retained for 40 years after last consul, or 75 years after DOB, whichever is longest
	Major injuries	40 years from termination date	Access to Medical Reports Act 1988 c28 provides the general provisions on the right of access to records created after 01 January 1989
	Job evaluation Final Report	Retain permanently	SCARRS

Category	Type	Retention Period	Legislation/Guidance
Health and Safety	Health and safety inspection reports	one years after issue	National Archives
	Risk assessment	three years since last assessment	Management of Health and Safety at Work Regulations 1992
	Fire Safety Training – proof of training	ten years after current year	Fire Safety (Scotland) Regulations 2006. SSI 2006 No 456 Regulation 20
	Accident and Incident reports - adults	three years after action	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 SI 2013 No 1471
	Plant and equipment condition surveys	two years after date of survey	SCARRS
	Control of hazardous substances	File closure + 40 years	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11
ICT	Security protocols for an ICT system	five years from decommissioning	Prescription and Limitation (Scotland) Act, 1973 and 1984
	Maintenance of the software licence(s) for an ICT system	five years from termination of licence	Prescription and Limitation (Scotland) Act, 1973 and 1984
Risk management and Business Continuity	Insurance policy documents, Certificate of Insurance	five years from date all obligations and entitlements concluded	Prescriptions and Limitations (Scotland) Act 1973 and 1984.
	Certificate of insurance: employers' liability insurance	40 years from date all obligations and entitlements concluded	Prescriptions and Limitations (Scotland) Act 1973 and 1984. The Employers Liability (Compulsory Insurance) Regulations 1998

Annex 3: British Library Web Archive Licence

1. Title of Website: Scottish Public Services Ombudsman (SPSO)

Web Address (URL):
<http://www.spsso.org.uk/>

Licence Granted By:
Name: Scottish Public Services Ombudsman

Contact Position: Corporate Services Manager

Third-Party Content:
Is any content on this web site subject to copyright and/or the database right held by another party? No

Agreement Date: 20-Mar-2014

Would you allow the archived web site to be used in any future publicity for the Web Archive? Yes

2. Title of Website: Valuing Complaints

Web Address (URL):
<http://www.valuingcomplaints.org.uk/>

Licence Granted By:
Name: Scottish Public Services Ombudsman

Contact Position: Corporate Services Manager

Third-Party Content:
Is any content on this web site subject to copyright and/or the database right held by another party? No

Agreement Date: 20-Mar-2014

Would you allow the archived web site to be used in any future publicity for the Web Archive? Yes

Personal details you provide on this form are protected by UK data protection law. Please view our Privacy Statement.

Contact information:

Permissions Officer
Web Archiving
The British Library
96 Euston Road
London NW1 2DB
United Kingdom
Email: web-archivist@bl.uk

The British Library is very pleased to have received your submission for the UK Web Archive which we will process as soon as possible. Please note that although we make every effort to archive websites as completely as possible there is much that cannot be archived for technical reasons. Further details can be found in the Technical information section: <http://www.webarchive.org.uk/ukwa/info/technical>.

Your website may not be available to view in the public archive for some time as we archive many thousands of websites and perform quality assurance checks on each instance. Due to the high number of submissions we receive, regrettably we cannot inform you when individual websites will be available to view in the archive at <http://www.webarchive.org.uk/> but please do check the archive regularly as new sites are added every day.

In the meantime many thanks for participating in the UK Web Archive and please do nominate other websites that you think may be in scope for us:
<http://www.webarchive.org.uk/ukwa/info/nominate>.

Regards, British Library Web Archiving Team

Annex 4: National Records of Scotland

1. Title of Website: **Scottish Public Services Ombudsman (SPSO)**

Web Address (URL):
<http://www.spsso.org.uk/>

Licence Granted By:
 Name: Scottish Public Services
 Ombudsman

Contact Position: Corporate Services
 Manager

Agreement Date: 14-09-2017

2. Title of Website: **Valuing Complaints**

Web Address (URL):
<http://www.valuingcomplaints.org.uk/>

Licence Granted By:
 Name: Scottish Public Services
 Ombudsman

Contact Position: Corporate Services
 Manager

Agreement Date: 12-10-2017

Contact information:

Web Archivist
 National Records of Scotland
 West Register House
 17A Charlotte Square
 Edinburgh EH2 4DJ

We will begin archiving your site as part of our October 2017 crawl. Captured content will then go through our quality assurance process before eventual release into the web archive about late November. We would be able to capture your corporate site at a further point in the year – in April (six months after October) and continue archiving on this twice-a-year basis. Just to ensure our service continues to deliver for you, please do keep us abreast of these – particularly if your core URL is changed as we will need to change our crawling scope to reflect this.

The web archive is available to access here: <http://webarchive.nrscotland.gov.uk/>. All archived content has a banner across the top of the page, signalling to the user that they are looking at an archived snapshot, or 'instance'. A side bar is also shown, which shows the user the date on which the particular page was archived:

<http://webarchive.nrscotland.gov.uk/20170726142725/http://www.audit-scotland.gov.uk/>

<https://www.nrscotland.gov.uk/research/researching-online/web-continuity-service>

In terms of seeing web continuity in action, thus far we have archived the old National Archives of Scotland website, and the old website of the Scottish Records Advisory Council. Both of these websites have since be closed down, to help relieve pressure on our IT team, though the web continuity code continues to provide permanent access to

archived versions of these sites though their original URL: have a go by clicking on <http://www.nas.gov.uk/> or <http://www.scottishrecordsadvisorycouncil.info/> and you will see you automatically get redirected into archived versions of these. Similarly, the other use case of web continuity is to provide access to links which have since been removed from the original site, which in turn can boost public transparency and support a user's journey around your site. In cases where pages are removed from the site, the web continuity code will kick in and redirect the user to an archived version of the page in question. We feel that the arresting side bar and banner clearly and quickly shows the user they are no longer in the live site, and there are plenty of supporting links and information in the web archive UI should they require any further information.

Transfer of long-term strategy and planning and SMT minutes to be arranged.

Back to the main [Contents Page](#)

Information sharing policy

Issued: October 2020

Contents

Introduction	2
Processing personal data	2
Why we share information	3
Statistical information and themes and trends	4
Supported signposting.....	5
Threat to health or safety	6
Information we can take into account	7
Likelihood of a threat	7
Who to inform about the risk.....	8
Who to tell about the disclosure of information	8
Recording the decision	8
General enquiries	9
Sharing under section 20 of the Scottish Public Services Ombudsman Act 2002	9
Confirming that we hold relevant data.....	9
Before sharing	10
Consider individual data rights	10
Seek assurances about how data will be handled.....	10
Ensure a secure method for transmission	11
When sharing	11
Record the decision.....	11

Back to the main [Contents Page](#)

Introduction

1. This policy is about sharing information with parties external to the SPSO when it is not for the purposes of a welfare fund review, or complaint. Consult the relevant guidance when sharing for those purposes.
2. Important: The SPSO Act 2002 places strict limits on when we can share information obtained during our complaints or review work. This applies whether or not the information contains personal data, for example information about a specific authority policy or approach.
3. The purposes for which we can share information obtained include: when a person is a likely threat to the health or safety of others (s 19 (4)) and when we have been given explicit power to share information, this includes:
 - 3.1. Section 20 which allows us to share with certain named scrutiny organisations for named purposes. (These are set out in schedule 5 of the Act); and
 - 3.2. Section 21 which allows us to share with other UK Ombudsman in certain circumstances.
4. We can also share statistical information and may be able to pass on information when it has been sent to us but we are not the appropriate organisation (supported signposting).
5. The policy sets out:
 - 5.1. why we share information;
 - 5.2. when we can share;
 - 5.3. how to identify what information we should share; and
 - 5.4. how to do so securely.

IMPORTANT: When sharing personal data outside of the SPSO secure network you must follow the guidance about identifying and using a secure method of transmission set out in the [Records Management and Security Guidance: Information sharing off-network and out-of-office](#).

Processing personal data

6. When processing personal data, we must always comply with the Data Protection principles. These say personal data should be:
 - 6.1. fairly and lawfully processed in a transparent manner;
 - 6.2. processed for limited purposes;
 - 6.3. adequate, relevant and not excessive;

- 6.4. accurate and up to date;
 - 6.5. not kept for longer than is necessary;
 - 6.6. secure; and
 - 6.7. the controller must be responsible for, and be able to demonstrate, compliance with the principles.
7. For organisations with which we share information regularly, we may hold an information or data sharing agreement, that agreement will provide more detail about methods and reasons for sharing but processing should always be in line with the principles. It is important to note that processing personal data to provide anonymised data still needs to meet with the above principles.
8. Please note, in this context, processing includes internal processing of personal information, for example, to analyse data even if the information we then share is anonymised or pseudonymised.

Why we share information

9. Whenever we are considering sharing personal data or processing personal data to support information sharing we need to identify:
- 9.1. the purpose or reason for which we are sharing; and
 - 9.2. be able to demonstrate that there is a lawful basis in terms of Data Protection legislation for the purposes or reason for which we are sharing.
10. We have identified it would be suitable to share information for a number of purposes. When identifying these purposes, we have looked at the underlying intent of the legislation that gives us the power to share. For example, in 2019 a policy document, approved by the Scottish Parliament identified specific reasons why it would be of benefit for us to share information to named organisations under section 20. The reasons identified were to:
- 10.1. support the SPSO to more effectively help organisations fulfil their statutory functions, building in best practice and greater efficiency at the point of delivery;
 - 10.2. reduce the likelihood of multiple, overlapping complaints by being able to share information about the SPSO's findings at any stage, not just the outcome; and
 - 10.3. support inspections that are more efficient by ensuring they are targeted and that organisations have access to all relevant information.
11. We, therefore, consider we may share information when it would achieve those purposes.
12. We will also share information to:

- 12.1. protect the health or safety of individuals (section 19);
 - 12.2. support improvements in the delivery of public services;
 - 12.3. support our statutory function as a setter of complaints standards with a duty to monitor and identify trends and support best practice and co-operation (section 16 G); and
 - 12.4. inform the public and others about our work and the quality of services under our jurisdiction.
13. In terms of data protection legislation we have identified that these purposes meet the following lawful basis:
- 13.1. performing a task in the public interest
- And when the information contains special category data:
- 13.2. protection of vital interests; and
 - 13.3. substantial public interest.
14. Whenever we are sharing special category information we should remember the lawful bases are 'substantial public interest and' 'vital interests require protection'. These are high standards and that should inform what and how much we share. Information relating to criminal convictions is covered by rules similar to special category data and it is good practice to treat any sensitive data with the same level of care as special category data.

Statistical information and themes and trends

15. The SPSO database allows us to create metadata which can be used to generate statistical, anonymised information. Data protection legislation allows for the processing of information for statistical purposes and we would not generally regard the statistical processing and creating of data as information obtained during an review or investigation¹. This means we can share statistical, anonymised information generally and with individual organisations for the purposes set out in paragraph 10. This is information which cannot be linked to and so identify an individual and will not include any information which is shared with an identifier, such as an SPSO reference number. While generally statistics are not information obtained, there are some circumstances where they may be.

- 15.1. We publish our annual statistics in formats which can be re-used.

¹ While this is generally the case, and is always the case for performance data, there are some circumstances where the specific processing and data does reveal information obtained. Advice should always be sought before undertaking new statistical processing.

15.2. We may publish additional statistics in either reports to Parliament or publicly which support the purposes set out in paragraph 10.

15.3. We may also provide information on themes and trends from case work and bespoke statistics on request, or as part of a joint project or regular pattern of engagement with organisations whose aim is to improve the public service and protect the public.

15.4. This may include providing:

15.4.1. sectoral information to a scrutiny organisation or regulator;

15.4.2. specific statistical or trend information about an individual organisation to a scrutiny organisation or regulator; and

15.4.3. statistics or trend information as part of our involvement in a group or project (for example, the health and social care intelligence group or complaints handling network group).

15.5. When providing this information we need to ensure it is accurate, we have identified an appropriate purpose for the statistics (see paragraphs 9 to 13) and that it is anonymised. Our annual reporting statistics do include reporting of low numbers (ie >5) but that data is limited and focussed on the performance of the organisation. We should consider providing an indicator ie >5 when the numbers are so low that individuals may be able to identify themselves or others and that information relates to special category or other sensitive data (for example monitoring data).

Supported signposting

16. Generally, if a complaint is sent to us which would be more appropriate for a different scrutiny or complaints organisation we provide contact details and it is for the complainant to decide if they want to send their complaint to that alternative organisation. However, there are cases where we may consider that it is appropriate to offer to send the correspondence to us direct to that alternative organisation. This is likely to be when there is an identified vulnerability or to help accessibility.

17. We can only do this with [consent](#). This consent requires to be informed so we should ensure there is a discussion and that we have provided the person with clear information about what we are doing and have evidence of their agreement to do so. If the information contains special category data it needs to be explicit. Careful recording of the discussion or correspondence around consent in all cases will mean we should meet that standard when required.

18. It may be appropriate to contact the alternative organisation to prevent us passing them information which they would not consider. To avoid this, we may contact them prior to sharing information, we should obtain consent before doing so.
19. We should not automatically send all the information sent to us. We need to assess whether there is information in the bundle we have received that it would not be appropriate to share. This may be the case where third party information has been sent to us, for example and it is unlikely that the alternative organisation will need this or that information is special category data.
20. Consent can be withdrawn. If we are contacted prior to sharing and informed consent has been withdrawn, we should not process the information.

Threat to health or safety

21. Section 19 of the SPSO Act 2002 says that:

[...](3) Where information referred to in subsection (1) [information obtained by us or by our advisers in connection with a complaint or request] is to the effect that any person is likely to constitute a threat to the health or safety of individuals (in particular or in general) the Ombudsman may disclose the information to any person to whom the Ombudsman thinks it should be disclosed in the interests of the health or safety of the particular individuals or, as the case may be, individuals in general.

(4) In relation to information disclosed under subsection (3), the Ombudsman must -
(a) where the Ombudsman knows the identity of the person to whom the information relates, inform that person of the disclosure of the information and of the identity of the person to whom it has been disclosed, and (b) inform the person from whom the information was obtained of the disclosure.

(4A) The duty under subsection (4)(a) to inform a person about the identity of a person to whom information has been disclosed does not apply where informing the former person is likely to constitute a threat to the health or safety of the latter person.

22. A direct or indirect threat to physically harm staff in this office or an individual(s) in any other location are clearly purposes for which we can release information and the details of how and when we may do so is dealt with in our separate policy on managing engagement.
23. This policy deals with situations where we do not have a directly worded or indirectly worded threat of an imminent physical threat, but we do have a concern that the actions or failure to act by an individual could mean a person or persons are at risk

from them. The legislative wording is broad and not limited to specific situations. Risk may come from individuals who work for organisations or individuals who complain to us or even about third parties who are referred to in information received. It may relate to professional practice or may not. Threat could include an unintentional threat to others, by an individual acting with good intentions, but showing dangerously inadequate professional practice for example.

Information we can take into account

24. We have taken legal advice which can be consulted in the case of uncertainty. We can only base our information on evidence we hold. If evidence is given to us by a third party we can put that together with evidence we hold and make a decision on the basis of all the information that is now held.
25. However, we cannot take into account the simple fact that a regulator or professional body has told us they have concerns when making this decision – that is not direct evidence of a risk.
26. This does not prevent us from releasing information in line with our normal process. For example, if we consider a regulator or third party may have relevant information for our investigation, we can release information to them that we consider they need in order to provide us with the information we are seeking. To give an example, if we know that the General Medical Council are investigating a case and they have indicated they may hold or we consider they may hold information that could be relevant to our investigation, we can release information to them (ie tell them details of the complaint) to clarify whether this is the case.

Likelihood of a threat

27. In this case, we are simply acting on a judgment that a person is 'likely' to constitute a threat. This judgment is going to involve a subjective assessment, but the threat should not be farfetched and likelihood suggests a more than 50 percent possibility. We do not though require to believe that actions will occur or that harm will result, only that there is a 'likely' threat to health or safety.
28. Therefore, while we have a responsibility to protect the public and we should proceed from a precautionary basis, it is also important that this legislation is used appropriately, and the legislation does require us to assess that there is a realistic threat, not a vague or alleged threat. Such decisions should always be made with care. Outside of some very immediate threats covered by a separate policy, all decisions to release information on this basis should be made after discussion with a member of LT, failing which a manager.

29. If concerns are being raised by an adviser, a discussion should be held with them as a matter of urgency as to whether they consider there is a 'likely threat' to health or safety. If the original adviser is not available within a reasonable timeframe, a second adviser can be consulted.

Who to inform about the risk

30. This legislation does not say who we should inform of the risk. This means we could inform the police; a registering body; a local social work department; the organisation who employs the individual or any other person or organisation we consider to be appropriate.

Who to tell about the disclosure of information

31. We are required to tell: the person who gave us the information and, if we know them, the person to whom the information relates. This means we need to tell the person we think is a risk that we have released the information. The reference to 'if we know the person' is to cover situations where we may be aware of a person who is a potential threat to others but not have an ability to contact them or may be aware of only a generalised risk.
32. We do have discretion - if we think that disclosing information to the person we think may be a threat may make the threat worse, we should not do so. This is most likely to happen in situations where the person at risk is vulnerable and the person we think is a risk to them has close proximity or control over them.
33. We need to record clearly our reason for doing so if we do exercise our discretion not to tell the person we think may be a threat.

Recording the decision

34. A note of the decision should include:
- 34.1. an assessment of the quality and credibility of the information and any actions taken to verify this (such as raising with the adviser);
 - 34.2. assessment of the risk;
 - 34.3. who made the decision to release [LT /manager];
 - 34.4. why we chose to release to that particular person /organisation;
 - 34.5. the specific details of the information released;
 - 34.6. when and how we informed the person the information was about; and
 - 34.7. if we decided not to inform or were unable to inform that person, the reasons why.

General enquiries

35. This guidance does not preclude us from making general, anonymised enquiries of other regulators or authorities where we feel this is necessary as part of our enquiries and investigation.

Sharing under section 20 of the Scottish Public Services Ombudsman Act 2002

36. Section 20 allows us to share information with named organisations for named purposes. If we hold an information sharing agreement with one of those organisations or another agreement that should be followed.
37. Where we do not have an agreement we should follow the process below. If we are sharing on a more than occasional basis (ie more than once a year or so) we should consider putting an agreement in place. Note: even where there is a pre-existing agreement, the process is broadly the same:

Confirming that we hold relevant data

38. SPSO may identify that we potentially hold relevant data because of:
- 38.1. our knowledge and experience of the relevant organisation and its work;
 - 38.2. our awareness of public information indicating this is a concern to the organisation;
 - 38.3. direct contact from the organisation; and
 - 38.4. comments made to us by one of our independent advisers.
39. Before taking any further steps we should test the assumption to see whether that is the case by:
- 39.1. identifying whether we have a lawful basis for sharing. To do so we need to:
 - 39.1.1. confirm the purposes for sharing are –covered by the purposes set out in schedule 5 – where we hold an information sharing agreement it may include examples to help us identify these but this assessment should be done on each individual case.
 - 39.2. Where there is no agreement, before proceeding we should contact the organisation and explain in general terms and without disclosing personal data. We should discuss with them our understanding of the statutory provision in schedule 5 to ensure that we are only sharing information that meets their purposes.

40. NOTE: the decision whether or not to share is one for SPSO and we cannot rely simply on a request by a named organisation. We should ensure we understand how the statutory provision listed in schedule 5 covers this request.
41. All Decisions about whether or not we hold relevant data should be clearly recorded on file.

Before sharing

Consider individual data rights

42. While there is reference to the possibility of sharing in these circumstances in our privacy notice, we should proceed on the basis that we will inform data subjects of an intention to release whenever possible.
43. In addition when the data to be released is special category or a similar type of data, we should also consider whether we should give the data subject the opportunity to make representations before we release data.
44. However, this will not possible when:
 - 44.1. our own legislation restricts us from informing third parties of an investigation; or
 - 44.2. informing the data subject would risk the investigation or other purpose of the organisation with whom we are sharing information.
45. We should note and record our reasons for sharing or not with the data subjects and for seeking representations from the data subjects before sharing or not.
46. When we are sharing special category or other sensitive personal data and are not informing the data subject, we need to take particular care to ensure that we respect the rights of those individuals and actively consider what concerns they may have raised if they had been given the chance to make representations when making our decisions.

Seek assurances about how data will be handled

47. Seek written (this includes email) assurance from the organisation that they have appropriate measures to retain and process the data in line with our / their obligations ([we have a template](#)). This may be tailored to the specific situation shared but we would anticipate organisations being able to provide evidence that they process information in line with data protection legislation, that they have appropriate arrangements for dealing with subject access requests, securing data and dealing with breaches. Where we have an information sharing agreement in place there will

be express commitments within that which means we do not need additional assurance in an individual case but note the paragraph below still applies.

48. Where relevant, if you have identified the data is particularly sensitive you may want to seek specific reassurances to, for example, protect the identify of a third party or a vulnerable person or whistleblower.

Ensure a secure method for transmission

49. Identify an agreed secure method to share the information (use the sharing outside of SPSO guidance in our information governance handbook which sets out our preferred methods of sharing). We have a [checklist](#) also available.

When sharing

50. Share the minimum amount of data required to meet the purpose. You may be able to identify this from generic discussions with the organisation but the general approach below may be helpful:
 - 50.1. Data should be pseudonymised unless doing so means it will not meet the purpose for sharing.
 - 50.2. If it is not clear whether or not pseudonymised data will be sufficient, share in a pseudonymised version first. This approach is strongly encouraged when special category or sensitive data is being shared.

Record the decision

51. As a data controller, SPSO needs to remain accountable for and demonstrate compliance with the Data protection principles. It is important to record and document decisions. The record should include:
 - 51.1. Why we consider the release meets the purposes and any steps taken to confirm this;
 - 51.2. Decision to inform or not the data subject and, if informed whether we received and considered any representations prior to release;
 - 51.3. who made the decision to release [LT / manager]; and
 - 51.4. the specific details of the information released.
52. The retention period for the record of the decision to share information should be the same as the information we have released and, unless there are compelling reasons not to, stored in the same file as the information that has been shared.
53. There is additional SPSO training for staff on sharing information.

Back to the main [Contents Page](#)

Electronic information sharing – eRDM Connect

Issued: October 2020

Contents

Introduction	2
When to use Connect?	2
How to share documents?	3
Connect structure and user types.....	4
Workspaces.....	5
Requesting a new Workspace	5
Workspace naming convention	5
Data protection and security	6
Participant permission levels	7
Training.....	8

Back to the main [Contents Page](#)

Introduction

1. The SPSO has a business need to share sensitive and confidential electronic information securely with external contacts including complainants, whistleblowers, professional advisers and bodies under jurisdiction. The SPSO migrated to the Scottish Government eRDM platform in February 2020, an electronic record and document management system provided by Objective, hosted and supported by iTECS.
2. The decision to move onto the eRDM platform was to enable the SPSO to access Connect, a proven secure electronic file sharing application that will allow us to share electronic data up to 2GB with contacts, authorised for use with data up to Official Sensitive level¹. Information is shared by creating secure workspaces and inviting external parties to collaborate in that space.
3. Key benefits of this application include:
 - 3.1. widely and increasingly being used across the Scottish public sector;
 - 3.2. allows two-way sharing of information, maintaining a single source of truth. All parties have access to the same version of a document from the shared workspace;
 - 3.3. workspace audit – owners and administrators can see details of activity in the workspace;
 - 3.4. workspace record – full log of all activity in the workspace, providing retainable evidence of who has accessed the material, when, etc;
 - 3.5. data protection - restrictions can be applied to prevent downloading / editing as required, and watermarks can be applied to documents to provide a trace in the event of unauthorised disclosure or sharing;
 - 3.6. GDPR compliance – workspaces closed when no longer needed;
 - 3.7. immediate notification to both sides when a document in a shared workspace is updated; and
 - 3.8. Connect is free for external contacts to use and is web-based, thus does not require new software to be downloaded.

When to use Connect?

4. Connect provides a safe and secure environment for SPSO to share and collaborate on information with external partners. In particular, Connect is the recommended application to use when:
 - 4.1. sharing key documents for projects;

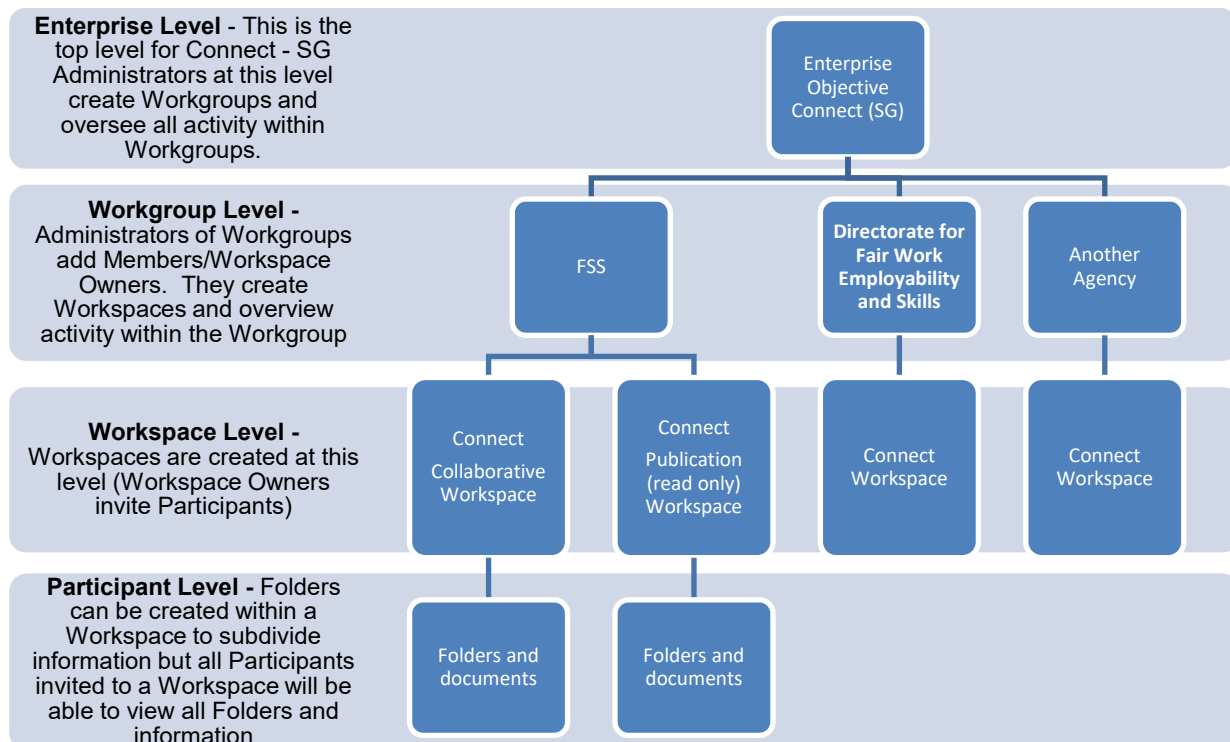
¹ [Government security classifications \(sharepoint.com\)](https://sharepoint.com)

- 4.2. sharing medical records with a professional adviser;
 - 4.3. sharing meeting documents with external attendees; and
 - 4.4. sharing documents with casework parties.
5. Additionally, it is recommended Connect is used for all larger pieces of work where there is a requirement to share a number of documents over a longer period of time.
6. See also: [Records Management and Security Guidance: Processing Information off-network and out-of-office](#).

How to share documents?

- 7. Non-casework documents to be shared must be stored in eRDM, aliases are then created to these documents and are stored in the Workspace folder. This makes them available externally via the Connect cloud-based platform following an invitation to join that workspace.
- 8. Casework documents to be shared in a Workspace must be shared to Connect using the CMS-Connect integration.
- 9. Connect Workspace areas can be 'read-only' or 'collaborative': A collaborative workspace means that participants will be able to edit the shared documents and add new ones if permissions are given to do this by the workspace owner. All edits and additions are automatically stored back into eRDM on the original document, so internal files remain up to date and the single point of truth, without the risk of duplication.

Connect structure and user types



User type	Organisation	Description
Enterprise Administrator	SG (eRDM Operations team)	The eRDM technical team. Manages the Enterprise Level. Will add Administrators / Members and designate privileges
Workgroup Administrator	SPSO (IMSOs)	Manages the Workgroup – will add members of staff to the Workgroup and designate permission rights, create Workspaces, identify and allocate Workspace Owners. They will also have the responsibility to manage the Workspaces within the Workgroup and monitor the connections being used by each Workspace. Once a Workspace has been created this will be transferred to the requestor of the Workspace. Members of SPSO staff that are currently Information Management Support Officers (IMSOs) for eRDM will become Workgroup Administrators for SPSO eRDM Connect
Member	SPSO	Those designated by the Workgroup Administrator to be able to access and work within a Workgroup and, when invited, Workspaces within this Workgroup

User type	Organisation	Description
Workspace Owner	SPSO	When a member requests a Workspace they are known as a Workspace Owner. They manage who can access this workspace (internal and external), what access rights are given and what documentation is available within this Workspace
Participant	External	People invited to a Workspace by the Workspace Owner. Can be designated a range of privileges (Participants with full permissions can invite others)

Workspaces

10. A Workspace is defined as an area within eRDM which holds information that is shared with others. Each Workspace is allocated a number of connections. Connections are based on the number of documents being shared multiplied by the number of people they are shared with. For example: four documents shared with five people = 20 connections in use. There will be limitations initially in the number of connections available, which will be monitored by SG (eRDM Operations).

Requesting a new Workspace

11. To request a new Workspace, the following procedure must be followed:
- 11.1. the member of staff requiring a new Workspace (the Workspace Owner), must fill out a Workspace request form or email which is sent to the team Workgroup Administrator and is stored on SPSO's casework management system if relating to casework, or eRDM if non-casework related;
 - 11.2. the team IMSO must set up the new Workspace and invite the relevant members of SPSO staff; and
 - 11.3. the Workspace Owner invites external participants to the Workspace and sets the relevant permissions.
12. If the new Workspace needs to contain documents that are restricted in eRDM, the request to set up the Workspace must be submitted via iFix.

Workspace naming convention

13. It is vital that all SPSO Workspaces are named consistently to ensure Workspaces are easily identified within eRDM.
- 13.1. each Workspace name must start with 'SHARED' to make it clear to staff members that the area contains shared documents;

- 13.2. if the purpose of the Workspace is to share information with external contacts regarding a case, the case reference must be included in the Workspace name; and
 - 13.3. the Workspace name must make the participants in that Workspace clear for example, adviser, complainant, BUJ.
14. Closing a Workspace:
- 14.1. if the documents within the Workspace need to be saved outwith eRDM, it is the responsibility of the Workspace Owner to save these to the correct location, for example, to a WorkPro case;
 - 14.2. the Workspace Owner must contact their team Workgroup Administrator to request closure of the Workspace, and the Workgroup Administrator must run an audit events report for the Workspace and save this in the relevant eRDM Level 5 (if the level 5 is restricted, the audit events report can be run and saved by SG) or the WorkPro case record. The naming convention for audit events reports is 'Connect – Name of Workspace – Audit Trail – closure date'.









Data protection and security

- 15. The named controller under data protection legislation is the SPSO.
- 16. Connect has been certified as secure to share OFFICIAL and OFFICIAL-SENSITIVE documents. When inviting an external participant to access documents it is extremely important that care is given to the type of access afforded to the participant (guidance for this can be found in ([Participant permission levels](#))).
- 17. Group emails are only permissible for use in Workspaces used for BUJs to share case documentation with SPSO. They should only be used if the BUJ is unable to use direct email addresses for accessing Connect. This is to reduce the possibility of other parties accessing the shared documents and is also vital for audit purposes. Group emails cannot be used for Workspaces for complainants or advisers.
- 18. This Handbook provides the SPSO's policies regarding managing personal data and should be consulted by Workspace Owners when deciding which documents can be shared within a Workspace and whether personal information (such as complainant names and addresses), needs to be redacted. Workspace Owners should also inform participants with collaborative access to a Workspace that their contributions and activities may be released if subject to an information request.
- 19. Support for Connect is provided by the Scottish Government iTECS Technical Team. iTECS eRDM system administrators have access to all documents stored within

eRDM and Connect. The team is fully security checked. Additionally, Connect has full audit facilities. We are able to see who has accessed any document stored within eRDM at any time. All Workspaces will also have a full audit report downloaded and saved when they are closed. This will document all activity undertaken within the workspace.

20. SPSO Connect Workspace Administrators will have an overview of all active Workspaces they have set up. Once a month, an audit check of open Workspaces will be undertaken in each team by the Workspace Administrator. This will enable the SPSO to ensure documents and Workspaces are being deleted from eRDM when they are no longer in use.

Participant permission levels

Icon	Description
	Participant(s) will be able to preview documents. When a Participant has not been given the Download ability, previewed documents are watermarked. Preview permission will only allow documents up to 30Mb in size to be viewed. If they do not have the Download permission then they will only see documents
	Participant (s) will be able to download documents to their local device without the watermark applied
	Participant(s) will be able to add documents
	Participant(s) will be able to create folders
	Participant(s) will be able to edit documents to upload new versions and rename documents
	Participant(s) will be able to invite/remove participants
	Participant(s) will be able to create and reply to comments
	Participant(s) will be hidden from and unable to see any other participants details in the Workspace

21. Permission levels will be set up for the following scenarios:

- 21.1. Advisers - should only have ability to preview documents, download documents (if necessary), add documents, create and reply to comments;
- 21.2. Complainants - should only have ability to preview documents, download documents, add documents, create and reply to comments; and
- 21.3. BUJs – should only have permission to preview documents, download documents (if necessary), add documents, create and reply to comments.

Training

22. There are three training modules for Connect on the Scottish Government Pathways Learning Portal: 03 – Connect
<https://erdm.scotland.gov.uk:8443/documents/fA473035/details>
23. The modules required to be completed will vary depending on the role each member of staff will have in Connect:
 - 23.1. Introduction to Connect (all staff);
 - 23.2. Workspace Owners (members of staff expected to own a Workspace); and
 - 23.3. Workspace Administrators (only for designated SPSO Workspace Administrators).
24. Each module takes roughly 20 minutes to complete. The SPSO will also provide guidance for participants for how to set up an account and use Connect.

Back to the main [Contents Page](#)

Records management and security guidance: processing information off-network and out-of-office

Issued: May 2018

Contents

Introduction	2
For whom is this guidance intended?.....	2
What is the purpose of this guidance?	2
Why is it important to consider data protection and access to information when working outside the SPSO secure working spaces?.....	2
How does this affect how I work?	3
Step 1: Identifying whether data is being processed / shared in a secure space	3
Step 2: Minimise processing or sharing personal data outside the SPSO.....	4
Step 3: Identifying the risk	5
Data in documents / on paper	5
Electronic data.....	6
Step 4: Protecting the data	6
Data in documents / on paper	6
Electronic data.....	8
Emergency procedures - 72 hours!.....	9

Back to the main [Contents Page](#)

Introduction

1. The SPSO provides secure systems for storing and processing information through the SCOTS network and our secure premises. These are referred to in this guidance as the SPSO secure work spaces.
2. This guidance applies to situations where information is processed or shared either physically or electronically outside those secure work spaces.

For whom is this guidance intended?

3. This guidance is intended for all SPSO staff and those contracted to provide services to the SPSO.

What is the purpose of this guidance?

4. This guidance gives general advice on the issues you need to consider to ensure that information we process (ie hold, work on or share) outside our secure work spaces is kept secure, confidential and is protected from loss or unauthorised access and exploitation. At the same time ensuring that it is accessible to anyone that needs to use it for their work.
5. It applies to data in all formats, including: paper files and documents; electronic data, files and documents; emails; images and video, and sound files.
6. You must comply with these guidelines to ensure that the SPSO meets its duties under Data Protection legislation, Access to Information legislation (ATI, for example, FOISA, EIRs) and the Scottish Public Services Act 2002 confidentiality provisions.

Why is it important to consider data protection and access to information when working outside the SPSO secure working spaces?

7. Data protection legislation, and ATI legislation apply to all the paper and electronic data, and information, you receive and create as part of your employment/contract with the SPSO, regardless of where you work or store it.
8. Data protection legislation requires the SPSO to ensure:
 - 8.1. we process data lawfully, fairly, and in a transparent manner, and only for specified purposes;
 - 8.2. that personal data is adequate, relevant and limited to what is necessary, and is accurate and, where necessary, kept up to date;

- 8.3. we hold data about living identifiable individuals for no longer than is necessary;
 - 8.4. we adopt security measures for this information to protect it from unauthorised access, amendment or deletion; and
 - 8.5. we take responsibility for how we handle personal data and for compliance.
9. More information about our duties and rights can be found in our DP policy and privacy notices.
10. The Data Protection Act also gives people certain rights, including the right to restrict, object, erase, rectify, and to access their own personal data that the SPSO holds about them, while ATI legislation (for example, FOISA and the EIRs) gives people the right to receive other information that the SPSO holds in a recorded, permanent, format.
11. We have a month to respond to a request under the Data Protection Act and 20 working days for FOI or EIRs requests. These deadlines mean that the SPSO must know what data and information it holds, and must be able to retrieve that information even if those holding it are away from the office. Section 61 of The Freedom of Information (Scotland) Act 2002 provides for a statutory code of practice on records management which describes the systems we should have in place for managing our information so that we can do this. The Scottish Minister's Section 61 Code of Practice is available on the Scottish Government website:
<https://beta.gov.scot/publications/code-of-practice-on-records-management/>

How does this affect how I work?

12. Secure working spaces have been set up to protect the data we hold electronically and physically. When working outside those spaces, we need to take additional steps to ensure that the data is covered, as far as possible, by equivalent levels of protection.

Step 1: Identifying whether data is being processed / shared in a secure space

13. On most occasions it will be obvious you are processing or sharing data outside the secure spaces: for example you might be sending information electronically to an individual or organisation outside the SPSO, or you might be physically sending or taking files, laptops, mobile devices and documents out of the office. Information might also be shared orally, for example, over the telephone or other audio visual conferencing platforms, or face to face meetings.
14. Think about where you are working, how and with what data. You can still be in a secure space when you are not physically in the office by working remotely on our

network with electronic data, or in a secure physical environment when working with hard copy data.

15. But beware! Being in the office does not automatically mean you are in a secure space. Working on a standalone PC, using an email address that is not your SPSO address, working where there are non-SPSO staff and/ or contractors present are all examples of non-secure spaces, even in the office. Some very sensitive personal data may need extra security even in the office. For example, an adviser may need to see specific medical records, but that does not automatically mean they should be able to see or access other complainant data.
16. You should always identify whether you are or are not sharing or processing information within the secure working spaces because if you are not you should be asking yourself why, and thinking about what other steps you need to take.
17. If you are unsure, seek advice before sharing or processing information.

Step 2: Minimise processing or sharing personal data outside the SPSO

18. When processing or sharing personal data consider:
 - 18.1. What do I need to process/share?
 - 18.2. Why do I need to process/share it?
 - 18.3. Have I anonymised/ pseudonymised it as much as possible (if not completely)?
 - 18.4. Could a person(s) still be identified because of the context it is in?
 - 18.4.1. anonymised data is data that cannot not be linked to an individual, and
 - 18.4.2. pseudonymised data is data that cannot be linked to an individual without additional data (for example by replacing names with a reference number) . It provides a layer of protection when compared to including names (or other identifiers that are easily attributed to an individual) so should be considered whenever possible.
19. Case reference number and name of organisation should generally be sufficient to identify most cases without sharing individual names.
20. Any concerns raised by individuals about processing or sharing personal data should be addressed before proceeding.
21. When taking personal data out of the office consider:
 - 21.1. Do you need to take the personal data out of the office at all?

- 21.2. Could you take it out of the office more securely electronically rather than physically (for example on an encrypted laptop)?
- 22. The best way to keep data secure is to keep it in the office (and know and track its location).

Step 3: Identifying the risk

- 23. Loss or damage could result in harm to individuals, legal action against you or the SPSO; damage to the SPSO's reputation; damage to collaborative relationships caused by the inappropriate disclosure of data; or regulatory action from the ICO, including fines. The severity of the impact is closely linked to volume, the sensitivity of the data, whether it is publicly accessible, mitigating actions taken to reduce the risk of loss or theft and the adequacy of policies and procedures. The more sensitive and private the data, the greater the impact of loss is likely to be.
 - 23.1. For information that is in the public domain or that we would disclose if asked for it under a FOISA / EIRs request, the risks are low, and so minimal security measures are likely to be required.
 - 23.2. Sensitive information, whether about identifiable individuals or information that would affect the SPSO's or another party's business, will require a higher level of security precautions.
 - 23.3. For some information the risks are very high. This might include prison files or medical information about identifiable patients (where a strong duty of confidentiality applies), or information whose disclosure is forbidden by law.

Data in documents / on paper

- 24. Information held on paper could leave the office in several ways, including:
 - 24.1. taken by SPSO staff for home working or meetings;
 - 24.2. shared for advice or comment;
 - 24.3. recorded in handwritten notes;
 - 24.4. being stolen; and/or
 - 24.5. accidentally included with other documents leaving the office or sent to the wrong address.
- 25. Data on paper is vulnerable to loss or unauthorised access in a number of ways. These are some examples, to consider, but it is good practice when taking data out of the office to consider the particular circumstances. Loss or unauthorised access may occur:

- 25.1. as a result of leaving papers in household (or other office) areas where they may be seen by other members of your household or by visitors. This is most likely to cause difficulties when the information is about identifiable individuals;
- 25.2. as a result of crime, for example, theft of a briefcase;
- 25.3. as a result of loss, particularly while travelling;
- 25.4. as a result of loss or crime in the courier / mail system; and/or
- 25.5. being opened by the wrong person.

Electronic data

- 26. Data held electronically is vulnerable to loss or unauthorised access or amendment:
 - 26.1. physically, through the loss, damage or access to the storage medium on which the record is held;
 - 26.2. accidentally, for example, if information is stored on a PC or on a shared network where others who do not have permission to see this information have access to the system, or you are working in a position where you can be viewed by others, or if it is accidentally disclosed;
 - 26.3. through technical issues such as a virus, system failure or hardware failure; and
 - 26.4. as a result of criminal action such as a cyber-attack (for example, such as hacking or deliberately sent virus), or theft of hardware or the storage medium.
- 27. Data is also vulnerable to unauthorised access as a result of accidental disclosure orally, such as over the telephone.

Step 4: Protecting the data

- 28. Once you have identified and assessed the risk you must take appropriate steps to protect the data.

Data in documents / on paper

- 29. If you are physically taking documents off-site to work
 - 29.1. take only what is necessary;
 - 29.2. do not take original documents out of the office ie where we hold the original version and not a copy;
 - 29.3. if there are exceptional circumstances that make it necessary to take original documents out of the office you must seek the permission of the Corporate

Information Governance Officer (CIGO) first, or if the CIGO unavailable the HoCSS or the Ombudsman;

- 29.4. ensure a copy is held in the office either physically or electronically so any loss does not mean the total loss of the data;
- 29.5. transport copy paper files in an SPSO authorised locked bag to and from the office. When the documents are not in use, store them securely and in the locked bag until returned to the office;
- 29.6. go directly between locations without putting the bag down in any public place, or leaving it unattended in a vehicle. Take extreme care not to misplace SPSO information on the journey to and from work;
- 29.7. if you know you are not going straight home or back to the office you should not take the data out of the office (using the SPSO approved courier may be appropriate instead);
- 29.8. ensure others cannot see the information while you are working;
- 29.9. papers or handwritten notes should be brought back to the office for secure disposal; and
- 29.10. notify your TA which file documents you are taking off-site and the date they will be returned. Your TA will keep a record as an audit trail of the movement of documents out of the office. It is important to sign the documents out and back in.

30. If you are sending documents or receiving documents off-site:

- 30.1. only send / request what is necessary;
- 30.2. avoid sending original documents and ensure if this is necessary a copy is held in the office either physically or electronically so any loss does not mean the total loss of the data;
- 30.3. use the SPSO approved courier; and
- 30.4. be clear about who will receive the data: where, when and how. Consider for example:
 - 30.4.1. is it a private home or an office where there may be a mail system which means someone other than the recipient may be involved?;
 - 30.4.2. does it need to be double-bagged or enveloped?;
 - 30.4.3. should arrangements be made so only the recipient can sign for it;
 - 30.4.4. ensure only information that is necessary for the file to get to its recipient (or return to sender) is on the outside of the file to prevent information being seen accidentally (and marked private and confidential); and
 - 30.4.5. ensure a record is kept, and that delivery is followed up.

Electronic data

31. Note: Electronic information is capable of being moved physically as well as virtually. If you are doing so by using a USB stick for example you should take the same steps as you would if you were moving paper documents but also ensure that you use any encryption or password protection available on the device. Laptops should be logged off if not in use.
32. Sending electronic data:
 - 32.1. only send what is necessary;
 - 32.2. ensure data is sent to another secure network rather than to a personal email;
 - 32.3. make clear in the email header if it is confidential and from SPSO;
 - 32.4. consider using encryption or a password protected workspace. SPSO will share details of tools it has access to that can be used to create safer methods of sharing information electronically particularly when the alternative is a personal email;
 - 32.5. check your recipient list/ addressee BEFORE clicking on send; and
 - 32.6. if you have any concerns, take advice before sharing.
33. 'If you are sharing information orally you should ensure that:
 - 33.1. you only share what is necessary.;
 - 33.2. the space you are working in is as secure as possible, for example, can you be overheard?;
 - 33.3. you carry out any appropriate identity checks before giving out personal details; and
 - 33.4. you are wary of people who may try to trick you into giving out personal details.
34. If working on a document electronically outside the SPSO secure network you should ensure that:
 - 34.1. you limit the amount of information being worked on as far as possible and consider anonymising/ pseudonymising the work;
 - 34.2. the space you are working in is as secure as possible, for example:
 - 34.2.1. Does it have appropriate security software?
 - 34.2.2. Is this up-to-date?
 - 34.2.3. Do you know what network you are linked to?
 - 34.2.4. Is the network you are linked into secure?
 - 34.2.5. Are you accessing the network through secure wi-fi?

- 34.2.6. Can you work outside of the network (ie switch broadband and wi-fi off)?
- 34.2.7. Can you be over-looked?
- 34.2.8. Does anyone else have access to the email / workspace you are using and if so can that be limited?
- 34.2.9. Can you use encrypted removable storage rather than storing on the system?
- 34.3. use passwords on individual documents if they will be stored for any length of time; and
- 34.4. do not store data for longer than is necessary and destroy all copies when the data has been uploaded / sent back to the SPSO secure network.

Emergency procedures - 72 hours!

- 35. Seventy-two hours is all the time we have from learning of a data breach to report it to the ICO. That includes weekends, out of office, bank holidays, sickness and annual leave.
- 36. As soon as you are aware of a data breach, or a potential data breach (for example, cannot find a file, even in the office), you must:
 - 36.1. contact the Corporate Information Governance Officer (CIGO) and your manager if you are a member of staff, immediately or as soon as is practicable. Ideally this should be by telephone, but can be by email if that is the only option;
 - 36.2. report exactly what data has been breached and under what circumstances this came about. If you use a non-secure email or can be overheard take care not to compound the matter by unintentionally including personal data. Describe the data, rather than repeat it;
 - 36.3. take appropriate steps to contain the breach; and
 - 36.4. notify the police immediately if there has been a theft, making sure you get an incident number and the name of the officer you spoke to.
- 37. There is a [data security checklist](#) when you are considering sharing information outside of the SPSO secure workspace. This checklist is also available as a template in WorkPro.
- 38. See also the [working from home data security checklist](#)
- 39. The Information Commissioner's website has further guidance on information security <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/>

Back to the main [Contents Page](#)

Clear desk and screen policy

Issued: July 2007

Contents

Introduction	2
Policy Statement.....	2
Clear Desk Procedure.....	2
Clear screen procedure.....	3
Training implications.....	3
Review / monitoring arrangements	3
Audit arrangements	4
Managerial responsibilities	4
Non conformance	4

Back to the main [Contents Page](#)

Introduction

1. Our Act states that we must not disclose information obtained in the course of our work except for purposes set out in the legislation. The SPSO is also legally obliged under the Data Protection Act 2018 to protect any personal information we hold.
2. Information security is characterised as the preservation of:
 - 2.1. Confidentiality: ensuring that information is accessible only to those authorised to have access;
 - 2.2. Integrity: safeguarding the accuracy and completeness of information and processing methods; and
 - 2.3. Availability: ensuring that authorised users have access to information when required.
3. Confidentiality, integrity and availability of information are essential to maintain legal compliance.

Policy Statement

4. This clear desk policy for papers and removable storage media, and a clear screen policy for information processing facilities, is one of many measures to ensure the security and confidentiality of information. Implementing this policy will reduce the risk of unauthorised access, loss of, and damage to information during and outside normal working hours.

Clear Desk Procedure

5. The aim is for all work areas to be cleared of confidential papers and media at the end of each working day.
 - 5.1. Paper and computer media should be stored in the lockable cabinets and drawers when not in use, especially outside working hours (and stored securely when working from home) . It is also worth noting that information left on desks is more likely to be damaged or destroyed in a disaster such as fire, flood or explosion.
 - 5.2. Any original medical records must be copied and returned as soon as possible. If they are required to be kept for a period of time, seek advice about storing in a fireproof location.
 - 5.3. Lock cabinets and drawers at the end of each working day (and lock the keys in the key-cabinet in the office).

- 5.4. A spare copy of team keys will be stored in a keypad operated key cabinet on each floor in the office.
- 5.5. Sensitive or classified information, when printed, should be cleared from printers immediately.
- 5.6. Mailroom pigeonholes must be cleared of sensitive or classified information every evening. Each team is responsible for their pigeonhole.
- 5.7. The reception desk can be particularly vulnerable. This area should be kept as clear as possible at all times; in particular medical records or other complainant identifiable information should not be held on the desk within reach / sight of visitors.

Clear screen procedure

- 6. All laptops are password protected.
- 7. Laptops should be shut down when not in use.
- 8. Computer screens should be angled away from the view of unauthorised persons.
- 9. The lock (log out) should be set when you leave your desk, automatically set to activate when there is no activity for 15 minutes, and be password protected for reactivation.

Training implications

- 10. It is essential that all staff are made aware of the key principles of information security. Training on this will take place as part of the induction for new starts.
- 11. See also [working from home data security checklist](#).

Review / monitoring arrangements

- 12. All staff are responsible for monitoring their compliance with the principles/procedures detailed in this policy.
- 13. This policy will be continually monitored and will be subject to a regular review which will take place one year from the date of issue and annually thereafter. The review will be carried out by the Corporate Services Manager and HR Officer.
- 14. An earlier review may be warranted if one of the following occurs:
 - 14.1. as a result of regulatory / statutory changes or developments;

- 14.2. due to the results/effects of critical incidents; and/or
- 14.3. for any other relevant or compelling reason.

Audit arrangements

- 15. The HoCSS will audit compliance periodically on behalf of, and report back to, the Audit and Advisory Committee.

Managerial responsibilities

- 16. The Ombudsman has ultimate responsibility for compliance of this policy. The Leadership Team and Management Team have the responsibility of developing and encouraging good information handling practice within their teams and for ensuring that staff clearly understand and adhere to this policy. However, it is the responsibility of all staff to adhere to the policy's principles and procedures to help maintain the security and confidentiality of information.
- 17. All staff have a responsibility for reporting information security incidents, including any breaches of confidentiality, to their manager and the CIGO.

Non conformance

- 18. There is a requirement for all staff to comply with this policy, and where requested, to demonstrate such compliance. Failure to comply will be regarded as a disciplinary incident, and will be dealt with under the appropriate Human Resource policy.

Back to the main [Contents Page](#)

Protective marking system

Issued: April 2015

Contents

Introduction	2
Purpose	2
Protective marking classifications	2
Determining the level of protective marking	3
Confidential	3
Marking information	4
Casework	4
Meeting reports	4
Non SPSO information	4
Emails.....	4
Review of markings	4
Assessing the consequence of compromise	5
Carriage of protectively marked assets	5
Bulk personal data transmissions	5
Incident reporting	6

Back to the main [Contents Page](#)

Introduction

1. The SPSO holds a wide range of information, some of which is subject to disclosure restrictions and some of which is either currently publicly accessible or to be made available in the future. As an Information Asset Owner and Data Controller the SPSO is responsible for this information. Everybody who works for the SPSO - including contractors and suppliers - are responsible for protecting information they work with.
2. A protective marking system is the method by which the originator of information indicates to others:
 - 2.1. the levels of protection required when handling the information in question, in terms of its sensitivity, security, storage, movement both within and outside the organisation and its ultimate method of disposal;
 - 2.2. the procedures to be followed regarding the handling, transmission, storage and disposal of the document;
 - 2.3. the severity or impact of the loss or disclosure of the document; and
 - 2.4. it is designed to protect information from intentional or inadvertent release to unauthorised readers.

Purpose

3. This guidance is designed to help SPSO staff determine when to use additional protective marking on their documents in order to indicate to others the levels of protection required to help prevent the compromise of information.
4. The protective markings do not impose any specific restrictions on the supply of information under the Freedom of Information (Scotland) Act 2002, the Data Protection Act 2018 or the Environmental Information Regulations 2004.

Protective marking classifications

5. From April 2014, the Cabinet Office introduced three levels of protective markings - TOP SECRET, SECRET and OFFICIAL. In line with this, the Scottish Government also adopted the three-tier system of classification.
6. All information the SPSO handles meets the criteria for OFFICIAL status only. There is no requirement to mark every document as 'official' as it is understood that this is the default for SPSO documents. The risk for 'official' data anticipates that individual hackers, pressure groups, criminals, and investigative journalists might attempt to get information. Any publicly available material is unclassified, including all SPSO published reports and material.

7. With this classification taken as understood, additional marking is used to indicate the nature of the document.

Determining the level of protective marking

8. It is the responsibility of the originator to determine when additional protective marking should be applied to the information, based upon an assessment of the sensitivity of its content and the impact of its compromise, often referred to as a harm test. Applying a marking unnecessarily will lead to unnecessary, restrictive and expensive controls, which may deny access to those who have a real business requirement, or need to know. Conversely, not applying a marking may put assets at risk of compromise, since appropriate security controls may not be in place.

Confidential

9. Confidential should be assigned where the compromise of information or material would be likely to:
 - 9.1. cause inconvenience, embarrassment, harm or distress to individuals;
 - 9.2. cause financial loss or loss of earning potential, or to facilitate improper gain or advantage;
 - 9.3. damage to the SPSO's standing or reputation and loss of public confidences;
 - 9.4. cause financial impact to the SPSO;
 - 9.5. breach obligations to maintain the confidentiality of information provided by individuals or third parties;
 - 9.6. breach statutory restrictions on the disclosure of information (for example, the Data Protection Act);
 - 9.7. prejudice the investigation of, or facilitate the commission of, low-level crime, or hinder the detection of serious crime; and
 - 9.8. undermine the proper management of the public sector and its operations.
10. Examples:
 - 10.1. complete set of an individual's social care files or health records;
 - 10.2. investigation files; and/or
 - 10.3. a smaller multiple of complete customer/employee records where information is sensitive, or includes financial or identity data (the protective marking should always reflect the highest impact individual item in a collection of records).

Marking information

Casework

11. On all template letters used for casework the marker confidential has been included above the address field to indicate the nature of this type of correspondence. The inclusion of a footer to appropriate correspondence further indicates how the document should be handled.

Meeting reports

12. All papers prepared for the senior management meetings and audit and advisory committee meetings indicate whether the paper is Open or Confidential. This is also described in the electronic naming of the document.
13. An additional descriptor may be used to describe the reason for the protection or restriction. For example: Restricted – Finance. The use of a descriptor is not mandatory, but they may provide helpful information to users.

Non SPSO information

14. Any material originating outside of SPSO that is marked in such a way to indicate sensitivity, for example 'Commercial in Confidence', 'Private' will be handled as indicated.
15. The SPSO in its statutory capacity receives and holds information sent by users which is not protectively marked. Staff must at all times treat this information with confidentiality and must not copy or disclose such information without an agreed lawful basis for doing so, and in line with SPSO policies.

Emails

16. If required in an email, protective marking should be added in bold by the sender to the start of the email subject header line and also the top of the body of the email message. This will ensure that all recipients, regardless of what email application they use, will see the sensitivity setting.

Review of markings

17. Some protective markings will need to be reviewed during the life of the information or document to ensure the marking is appropriate and still relevant.

Assessing the consequence of compromise

18. It is essential that a risk assessment be undertaken to determine the likelihood and impact that loss or compromise of the information asset will have on its: (a) confidentiality, (b) integrity; and (c) availability as this will determine the necessary security controls that will need to be applied to the information.
19. The accumulation and aggregation effect also needs to be taken into account when considering the business impact of a compromise. For example, the compromise of a mass of data, particularly one involving personal details, is likely to have a bigger impact and cause greater damage than the loss of one piece of data, and thus an adjustment to the impact level, but not necessarily the protective marking, may be required.

Carriage of protectively marked assets

20. Protectively marked or other valuable assets are at risk during transit from accidental or deliberate compromise. To protect such assets when in transit the means of carriage must be reliable, the packaging robust, and the attractiveness, identity and source of the assets concealed under plain cover. Where higher levels of protectively marked assets are involved, a system of audit must be built in to track such assets and to reveal any actual or attempted tampering.
21. Please refer to the [SPSO Records Management and Security Guidance](#). This guidance gives general advice on the issues you need to consider to ensure that any SPSO information you work on out of the office is kept confidential and protected from loss or unauthorised access and exploitation, while at the same time ensuring that it is accessible to anyone that needs to use it for their work. It applies to information in all formats, including paper files, electronic data, word-processed documents and emails.

Bulk personal data transmissions

22. Before bulk data transfer is established with another organisation the following must be considered:
 - 22.1. that there is a valid business requirement to perform bulk data transfers and that it is legal, appropriate and acceptable;
 - 22.2. that the recipient, where appropriate, is contractually aware of the use that they can make of the personal data SPSO provides to them;

- 22.3. that the minimum amount of data is transferred to meet the business requirement and not the entire data set simply because this is the easiest or cheapest option;
- 22.4. that the method of transfer is secure (for example using eRDM Connect);
- 22.5. where transfers take place with other external parties, the parties should ensure, where possible, that contractual and other agreements specify the transfer mechanism and incident management procedures; and
- 22.6. where SPSO cannot agree or enforce data transfer standards with an external party the risks associated with that transfer must be understood and owned at a senior level.

Incident reporting

- 23. Any incident involving the suspected loss or compromise of any protectively marked material must be reported immediately to the Corporate Information Governance Officer.

Back to the main [Contents Page](#)

Access to information legislation

Issued: February 2012

Contents

Requests for Information	8
Complaint Files.....	8
Verbal Requests	9
Initial Handling and Recording Information Requests	9
Freedom of Information (Scotland) Act 2002	10
Scottish Information Commissioner.....	11
Publication Scheme.....	11
Requests for Information Received	12
Advice and Assistance	12
Responding to a Request.....	13
Common Requests for Information.....	15
Exemptions.....	17
Right of Review	21
Right of Appeal.....	22
Offences under the FOISA	22
Environmental Information (Scotland) Regulations 2004	22
Charging.....	22
Right of Review	23
Right of Appeal.....	23
External Guidance	23
Annex 1: Information Request Flowchart.....	25

Back to the main [Contents Page](#)

Requests for information

1. The SPSO is considered a Scottish public authority under the Freedom of Information (Scotland) Act 2002 (FOISA), Environmental Information (Scotland) Regulations 2004 (EIR) and Data Protection Legislation. As such, we must always ensure that we respond to all requests for information in accordance with the statutory requirements of these Acts.
2. Requests to the SPSO for information held (or believed to be held) by the SPSO must usually be in writing or some other permanent format (EIR requests can be made orally). Under Data Protection Legislation requests can now be made orally. The SPSO aims to acknowledge all information requests within three working days, providing a timescale for responding. It is imperative that all Information Requests are passed to the Information Governance Team immediately on receipt (or advice on handling is sought straight away).
3. Requesters must give an adequate description of the information they require, but do not need to state reasons for the request or refer to relevant legislation. The requester may also express preference for the format for information to be provided in.

Complaint files

4. Our legislation states that our investigations must be conducted in private, that the procedure for conducting the investigation and obtaining information is to be such as the SPSO thinks fit, and information obtained in respect of a complaint to our office, to include details of the authority complained about, can only be disclosed in specific circumstances. Releasing information under FOISA is not one of those circumstances. Therefore, obtained information is exempt from being released under section 26(a) of FOISA, which is an absolute exemption, so we do not need to consider the public interest test. We would consider the information is also exempt under regulation 10(5)(d) of the EIR if it comprises environmental information. However, individuals have a right to request information that we hold about them under Data Protection Legislation. In light of our duty to provide requesters with advice and assistance, we will often advise complainants that we will continue to consider a request for information from our file on their complaint as a subject access request under Data Protection Legislation (note, we must still also provide a response under FOISA / EIR, even if the requester has asked for personal data, unless they specifically state they are making a SAR or a request under the Data Protection Act or GDPR).
5. During consideration of a complaint, it is essential that those parties providing information to the SPSO are reminded of our obligations under our own Act and

under Data Protection Legislation; are advised that information could be shared; and are invited to provide reasons why any information they provide should not be shared. Listed authorities should be advised when a copy of the enquiry letter has been sent to the complainant for information, and that their response together with any relevant documents may be copied to the complainant. Where the listed authority has requested that information not be shared with the complainant, the Complaints Reviewer should ask the listed authority to provide a written statement of the reasons for this request. If the Complaints Reviewer decides that the reasons are not sufficient, then they will consult their manager and/or the Corporate Information Governance Officer. The decision, however, ultimately rests with the SPSO.

6. Where we have been provided with information that is not relevant to the complaint, we should return it or advise we will destroy it. When recording information, the complaints reviewer should use objective language. The complaints reviewer should keep in mind that individuals may have a right to see what has been recorded if they request to do so.
7. See [Case File Management](#) guidance for more information.

Verbal requests

8. If the request for information is made verbally, the person dealing with the request should consider whether it would be in the requester's interest to make the request in a recordable format so that the rights under the FOISA,. This should certainly be discussed with the requester where there is any doubt whether all the information can be provided. Under EIR and Data Protection Legislation, there is no legal requirement for requests to be in writing, but they must make clear what information is being sought. It is a good idea to confirm the request in writing.

Initial handling and recording information requests

9. Information requests may, for example, come in by post, telephone, InfoRequests@, ask@ or our online request form, or by our other group mailboxes and advice lines via the front office or direct to SPSO staff. All staff should deal with straightforward information requests as far as they can, liaising with the Information Governance Team . Where they are unable to deal with the request, they will pass it on to the Information Governance Team to progress.
10. Where the SPSO has simply been copied into correspondence, we should acknowledge receipt but advise that we will not take any further action, and ask the sender not to copy us into correspondence in future.

11. The request should be recorded on WorkPro as soon as the request is received.
12. Setting up a new case:
 - 12.1. Create a new case on WorkPro choosing case type Information Request. The person dealing with the request is the Case Owner.
 - 12.2. All available contact /applicant details from the request should be entered into the record and saved.
 - 12.3. The type of request, ie FOI or DP or EIR, should be selected from the dropdown list, and the request receipt date and request details entered (do not include identifiable data in free text fields). Refresh the target date if necessary (20 working days for FOI/EIR, one month for SARs).
 - 12.4. The 'casework involved' box should be checked if the request relates to a complaint with the details recorded. This is to allow checks to be carried out when archiving to prevent information being destroyed in case of appeal.
 - 12.5. The case reference(s) the request relates to should be entered into the Associated cases field.
 - 12.6. Link the case to any other related case records. If the request will relate to a high volume of case records, ensure the Information Governance Team is aware for archiving. Similarly, for any non-casework.
 - 12.7. Information request cases are electronic records only. Where letters and paper documents are received, these should be scanned and logged on the electronic record. All emails should be attached to the WorkPro record. File/telephone notes should also be used where appropriate. Prepared templates can be adapted when dealing with information requests.
 - 12.8. Use the enquiry tracker for consults.
 - 12.9. When closing the case, the response date, response details (remember do not include identifiable data in free text fields), and exemptions should be entered, along with an estimate of the time taken in minutes.
13. See information request flowchart at the end of this [section](#).
14. See also [link](#) to information request process guidance document.
15. The remainder of this guidance focusses mainly on FOISA (and the EIRs). There is additional Subject Access Requests, or SARs, guidance in this Handbook.

Freedom of Information (Scotland) Act 2002

16. Any person has a right to see any kind of recorded information held by a Scottish public authority, subject to certain exemptions.

Scottish Information Commissioner

17. The Scottish Information Commissioner (SIC) is responsible for enforcing and promoting the right to access information held by Scottish public authorities. Information and guidance on the Freedom of Information (Scotland) Act 2002 (FOISA), the Environmental Information (Scotland) Regulations 2004 (EIR), exemptions, the public interest test, vexatious/repeated requests, fees/excessive cost of compliance, validity of requests, previous SIC decisions, records management, and much more can be found on the SIC website at www.itspublicknowledge.info, which should be the main point of reference. The website also provides many other resources including links to the FOISA, the EIR, Codes of Practice, Fees Regulations and FAQs for public authorities on fees and timescales (including calculation of working days). This SPSO guidance document is not intended to be used in place of the SIC guidance, and will not repeat that guidance in detail.

Publication scheme

18. All Scottish public authorities must produce and maintain a publication scheme which is approved by the SIC. Publication schemes describe the information that the authority publishes, how to access that information and whether it is free of charge or available for a payment. Information in the publication scheme can always be released. There is a chance, however, that information which has not yet been uploaded may contain elements that ought not to be released and should be redacted. The SPSO publication scheme is available on our website at www.spsso.org.uk and we publish information that we hold within the following classes:

- 18.1. Class 1: About us
- 18.2. Class 2: How we deliver our functions and services
- 18.3. Class 3: How we take decisions and what we have decided
- 18.4. Class 4: What we spend and how we spend it
- 18.5. Class 5: How we manage our human, physical and information resources
- 18.6. Class 6: How we procure goods and services from external providers
- 18.7. Class 7: How we are performing
- 18.8. Class 8: Our commercial publications
- 18.9. Class 9: Our open data

Requests for information received

Identity of the requester

19. Section 8(1)(b) of the FOISA requires that the requester provides their name (shown in email address is not sufficient) and an address for correspondence. An email address, or a PO Box would be sufficient contact information to enable the SPSO to respond. Requests made on behalf of another person must name the third party (the 'true applicant') in order to be valid.
20. The reason for this is that any appeal to the Court of Session in Scotland in connection with a request must be made using the true name of the applicant and this must be the name used in the original request to the public authority.

Broad, general or unclear requests

21. If the request is too broad or general (for example, seeks all information on a topic over many years), we have a duty to provide advice and assistance to the requester in order to focus the request before either accepting a revised request which meets the criteria or closing the request. The breadth of a request is not in itself an automatic reason to refuse it, although cost considerations might well be relevant here. The advice is to contact the requester, and ask for clarity about what they are specifically looking for. Section 1(3) of the FOISA (regulation 9(2) of the EIR) deal with the issue of unclear requests and those which have been formulated in too general a manner for an authority to comply.

Mixed EIR / FOISA requests

22. If a request covers both environmental information and non-environmental information or some of the information is not held, the person dealing with the request must separate out all the elements of the request and deal with each element individually. However, all parts of the request can be dealt with in one letter of response.

Advice and assistance

23. At all times, SPSO must provide advice and assistance to a person who has made, or proposes to make, a request for information. This is a statutory duty under section 15 of the FOISA and regulation 9 of the EIR. This could include seeking clarification in relation to an information request or assisting the requester in identifying and describing relevant information. If the request is unclear and clarification is sought, the clock does not start until clarification is received. The section 60 and section 62 Codes of Practice expand on this and recommend a number of practical steps.

Assistance to make a request in a recordable format

24. If the requester is having difficulty making a request in a recordable format, whether because of a disability or any other reason, the person dealing with the request can offer to write it down for them. In such cases, the requester should be asked to sign and return the written request to the SPSO. It is appropriate to provide the requester with two copies of the request (one for their records) and a freepost envelope for the reply.

Assistance in framing or clarifying a request

25. If the requester has had difficulty in stating what information they want, the person dealing with the request can work with them to try to clarify the request into something we can help with or which might be more useful. For example, a requester asks for all the information we hold on a particular public authority. This wide request would embrace (but not be limited to) information relating to investigations, enquiries, research/events - and it is unlikely that the requester actually wants everything. In this instance, it would be good practice to describe the sorts of information we do hold, helping to identify the elements the requester would like to see. The process of seeking clarification must be recorded in WorkPro. The 20 working days for responding to the request will commence on the day after receipt of the clarification. If no clarification response has been received, the person dealing with the request should write to the requester again, stating that we are unable to proceed with the request. Where the information requested is not held by the SPSO, the duty to advise and assist includes advising which public authority holds the information requested, if this is known. Where the person dealing with the request does not know which public authority would hold the information, there is no obligation to carry out research on behalf of the enquirer.

Responding to a request

26. The SPSO must establish whether it holds the information requested, consider whether all or part of the information falls within an exempted class, and respond to the request within 20 working days following the date of receipt of the request. For email requests, the received date is the actual date of the email, even if the email is received outside office hours.
27. Where information cannot be provided, the SPSO must issue a refusal notice, stating the reasons for refusal and informing the requester of their rights of appeal. Reasons for refusal include:
- 27.1. do not hold the information requested (section 17 of the FOISA);
 - 27.2. information is covered by an exemption;

- 27.3. excessive cost of compliance exceeds £600 (section 12 of the FOISA);
and/or
- 27.4. vexatious or repeated request (section 14 of the FOISA)

Information not held

- 28. The requester must be informed that the information is not held, or no longer held, by the SPSO. The SPSO [Retention and Disposal Policy](#) may be useful in explaining our procedures for retention, archiving and disposal. In limited circumstances, it may be necessary to issue a refusal letter (section 18 of the FOISA) which neither confirms nor denies that the information is held by the SPSO. The requester must be advised that they have a legal right to request a review of the response and to address any request for review to the SPSO HoCSS.

Information held

- 29. If the information cannot be supplied straight away, an acknowledgement should be sent to the requester within three working days.
- 30. The person dealing with the request must first establish whether we hold the information. This will depend on the information requested and how specific the request is. Electronic and paper records are held in several locations (WorkPro, complaint files, eRDM, individual outlook boxes, Microsoft Teams channels conversations and chat etc). The person dealing with the request must also consider whether information may be held in some of the less obvious locations or formats (diaries, deleted email folders, etc). The person dealing with the request should do some initial searching for relevant information (searches on WorkPro, asking colleagues who may be able to help). If unsure of what is held and by whom, the person dealing with the request should issue an email to all relevant staff, setting out the detail of the information request and asking for any relevant information.
- 31. For wide-ranging requests involving multiple records, the person dealing with the request should collate the record titles so that a schedule of the documents can be supplied when responding to the request.
- 32. The person dealing with the request should also ensure that a record of the searches carried out is available in WorkPro. This may simply consist of the email sent to colleagues and their responses, but where record sets have been searched in more detail, this should be noted.
- 33. The person dealing with the request must evaluate all the information identified and reach a view on whether it should be released or withheld under any exemptions, including consideration of the public interest test where appropriate. In some cases, some information may need to be redacted. All information withheld, including

redactions, must be explained in the response by citing the relevant exemption and why it has been applied, how the public interest test has been applied, and why the conclusion has been reached that release is not in the public interest.

34. If a request is being dealt with by somebody other than the Information Governance Team, draft refusal responses should be forwarded, along with the information that is to be withheld or redacted, to the Information Governance Team for checking before the response is sent out. Where the information can be released in full, it should be collated and, if necessary, transferred into the agreed format.
35. The requester must be advised that they have a legal right to request a review of the response and to address any request for review to the HoCSS at the SPSO, and to appeal to the Scottish Information Commissioner (and to the Court of Session on a point of law). Our Information Rights leaflet containing this information should be provided.

Charging

36. The SPSO can calculate the estimated cost of complying with FOI requests and may charge within the framework provided by the [Freedom of Information \(Fees for Required Disclosure\) \(Scotland\) Regulations 2004](#).
37. We cannot take account of costs incurred in determining whether information is held, or whether the requester is entitled to receive it.
38. The estimate of staff costs cannot exceed £15 per hour.
39. Where the cost of providing information is over £100, the SPSO may charge a fee in line with the Fees Regulations. The fee cannot exceed ten percent (£50).
40. Where the cost of providing the information would be over £600, the SPSO is not obliged to provide the information under the FOISA. If we do so, we may charge the full cost.
41. In all cases where fees are applied, a fees notice must be issued and must detail how projected costs were calculated.
42. Where the fees will exceed the upper cost limit of £600, requesters must be advised on how to bring their request within the cost threshold.

Formatting information

43. Responses should be sent by the same means that the request was made. We will comply with the requesters' preference for the format of the information where it is reasonably practical to do so. The Disability Discrimination Act 1995 applies to

information requests just as it does to all other service provision. If the requester has specified a format because of a disability, we must comply. The only exception to this is where it would be unreasonable to do so. The burden of proof of what is reasonable lies with the SPSO. The Race Relations (Amendment) Act 2000 places similar duties on public authorities in terms of provision of translated information.

Redacting information

44. Redaction is the process of blanking out information on a document before it is released. This applies to individual words, sentences or whole sections of a document. Redaction should be done by a person who has knowledge of the subject matter to decide which material should be exempt.
45. When redaction is used on Freedom of Information requests (FOI) or Environmental Information Regulation requests (EIR) you need to explain to the applicant which exemptions have been applied and why. Redaction may also be needed when dealing with subject access requests.
46. Redactions should always be carried out on a copy, never the master or original version of a document. Words should not be visible or be able to be guessed due to incomplete redaction.
47. Information can be deleted from Word documents and replaced with [redacted], then the document printed as a PDF.
48. Spreadsheets can have multiple sheets that must be checked, and they must also be checked for hidden data (hidden tabs, columns, rows). They can be copied by exporting as a .csv format file, information can be deleted and replaced with [redacted], and the redacted version can be reimported to the spreadsheet.
49. Using the highlighter tool in Microsoft Office (Word, Excel, PowerPoint) to highlight the text in black to 'hide it' does not properly redact information (even if then converted to a PDF).
50. PDFs can be redacted using Adobe Pro if available. See Adobe Acrobat redaction guidance (or WorkPro Training for [Editing a PDF document](#) in WorkPro).
51. Hard copy documents can be scanned and redacted as PDFs. For manual redaction using black marker pens or fluid, documents must be photocopied again for release (hold paper up to the light to check words not visible).
52. See ICO guidance '[How to disclose information safely](#)'.

Common requests for information

Requests for qualifications and experience

53. The SPSO Job Descriptions and Person Specifications contain this information.

Requests for names and qualifications of advisers

54. Normally we will not release the names of advisers. In terms of qualifications, we will normally give details of their background that qualify them to give advice on that subject. Normally complainants are really only looking for reassurance that the adviser 'knows what they are talking about'. Biographical details about our Scottish in-house advisers (where available) can be released as written (with appropriate anonymisation). All SPSO advisers should be made aware of our position on release of this information. Adviser biographical information should be edited down to clinical qualifications etc. Advisers are aware that they will not be named in reports. It is good practice to contact the adviser before releasing the information.

Requests for SPSO processes or policies

55. If someone requests information which we already have in printed form, or available on our website, this can be sent directly. This does not usually need to be dealt with under the FOISA, although we should respond within 20 working days in case of appeal to the SIC. It may also be appropriate to provide our 'Information Rights' leaflet when responding.

Requests for statistics

56. These should always be handled under the FOISA, however, some information is already available in the annual reports or on our website. In case of more specific requests where the information has not already been published, the ISE Officer (Insight) will collect the relevant information and Information Governance will respond to the request. Statistics may still be exempt information under FOISA.

Requests for legal advice

57. Section 36(1) of the FOISA states that 'Information in respect of which a claim to confidentiality could be maintained in legal proceedings is exempt information'. In a briefing note explaining this exemption, the SIC confirms that this applies to information shared between a public body and professionally qualified and instructed lawyers. The SPSO feels that there is a public interest in maintaining client/lawyer confidentiality where appropriate. However, in the spirit of the FOISA, the SPSO might be happy to share the substance of the advice that was received. This should be considered on a case by case basis.

Exemptions

Absolute exemptions

58. Absolute exemptions are listed in section 2(2) of the FOISA. Some absolute exemptions mean there is no requirement for a harm test or a public interest test under the FOISA (although other rules of law imported into the FOISA by exemptions may contain such tests). Other absolute exemptions cover information that can be accessed through other legislation, for example, subject access requests under Data Protection Legislation.

Qualified exemptions

59. Where a qualified exemption is applied, the SPSO must go on to consider the public interest test in order to determine whether the information should be released or could legitimately be withheld.

Public interest test

60. Although not defined in the FOISA, the public interest has been described as something which is of serious concern and benefit to the public, not just something of individual interest, and as something that is in the interest of the public, not just of interest to the public. When applying the test, public authorities are deciding whether it serves the interests of the public better to withhold or disclose information. The 'public' does not necessarily mean the entire population, but might relate to a relatively localised public, for example, a small community or interest group.

Key exemptions - absolute

Section 26(a) of the FOISA 'Prohibitions on disclosure'

61. Information is exempt information if its disclosure by a Scottish public authority is prohibited by or under an enactment. For example, Section 12 of the SPSOA requires that an investigation by the Ombudsman must be conducted in private, and section 19 of the SPSOA specifically prohibits the Ombudsman from releasing information obtained in respect of a complaint, except for the purposes specified in that Act. Even the documents that are generated by the SPSO will in many cases be constituted by, discuss and pertain to information that has been obtained. Information prohibited by or under an enactment is exempt from release under section 26 of the FOISA.

Section 36(2) of the FOISA 'Confidentiality'

62. Information obtained from a third party and whose disclosure would be an actionable breach of confidence.

Section 38(1) of the FOISA 'Personal information'

63. Information is exempt information if (a) it is personal data of which the requester is the data subject and has a right of access under Data Protection Legislation (subject access request – deal with under Data Protection Legislation); or (b) it constitutes third party personal data and disclosure of the information to a member of the public would either contravene any of the data protection principles, or be likely to cause damage or distress (contravene right to object); or the information would be exempt from release to the data subject under Data Protection Legislation.

Key Exemptions - qualified

Section 30(b) of the FOISA 'Prejudice to effective conduct of public affairs'

64. Information is exempt information if its disclosure would, or would be likely to, inhibit substantially (i) the free and frank provision of advice; or (ii) the free and frank exchange of views for the purposes of deliberation. For example, the comments of individuals who attended and spoke at internal meetings and who may be discouraged from speaking freely and frankly at future meetings should their comments be made public.

Section 30(c) of the FOISA 'Prejudice to effective conduct of public affairs'

65. Information is exempt information if its disclosure would prejudice substantially, or be likely to prejudice substantially, the effective conduct of public affairs. For example, information relating to particularly sensitive matters which, if made public, would substantially inhibit the Ombudsman from conducting SPSO affairs.

Section 33(1)(b) of the FOISA 'Substantial Prejudice to Commercial Interests'

66. Information is exempt information if its disclosure would, or would be likely to, prejudice the commercial interests of any person, including a public authority. For example, commercially sensitive details of a contract entered into between the SPSO and another organisation.

Section 36(1) of the FOISA 'Confidentiality'

67. Information which could be subject to a confidentiality of communications claim in legal proceedings.

Personal data

68. Complaint files are likely to contain a mixture of personal and non-personal information. Personal information is also exempt from release under section 38 of the FOISA.

Vexatious, manifestly unreasonable or repeated requests

69. The SPSO can refuse to comply with a vexatious or repeated request. A vexatious request is determined by the information requested, not the person making the request, and is only relevant to requests made under the FOISA, not Data Protection Legislation (SARs may however be manifestly unfounded or unreasonable). An individual can make as many requests for information as he/she wishes, and cannot be labelled as vexatious - each of their requests must be determined on a case-by-case basis. There is no provision for aggregating the cost of responding to multiple requests received from the same person.
70. Vexatiousness needs to be assessed in all the circumstances of an individual case. If a request is not a genuine endeavour to access information for its own sake, but is aimed at disrupting the work of the SPSO, or harassing individuals in it, then it may well be vexatious.
71. There are a number of ways in which it may be possible to identify individual requests as being vexatious, notably:
- 71.1. If a requester explicitly states that it is their intention to cause the SPSO the maximum inconvenience through a request, it will almost certainly make that request vexatious.
 - 71.2. If we have an independent knowledge of the intention of the requester. Similarly, if a requester (or an organisation to which the requester belongs, such as a campaign group) has previously indicated an intention to cause us the maximum inconvenience through making requests, it will usually be possible to regard that request as being vexatious.
 - 71.3. If the request clearly does not have any serious purpose or value. Although the FOISA does not require the person making a request to disclose any reason or motivation, there may be cases which are so lacking in serious purpose or value that they can only be fairly treated as vexatious. For instance a request for the number of unmarried employees in an organisation, could be classified justifiably as a vexatious request. Such cases are especially likely to arise where there has been a series of requests. Before reaching such a conclusion, however, we should be careful to consider any explanation which the requester gives as to the value in

disclosing the information which may be made in the course of an appeal against refusal. It would be reasonable to ask why they require the information if it helps you to decide.

71.4. If the request can fairly be characterised as obsessive or manifestly unreasonable. These requests will be exceptional and we must have valid reasons for making such a judgement. An apparently tedious request, which in fact relates to a genuine concern, must not be dismissed. However, we are not obliged to comply with a request which a reasonable person would describe as obsessive or manifestly unreasonable. It will obviously be easier to identify such requests when there has been frequent prior contact with the requester or the request otherwise forms part of a pattern, for instance when the same individual submits successive requests for information. Although such requests may not be 'repeated' in the sense that they are requests for the same information, taken together they may form evidence of a pattern of obsessive requests so that we may reasonably regard the most recent as vexatious.

72. We therefore need to keep records of all FOI receipts as evidence when assessing potentially vexatious requests. We should contact the SIC for advice before declaring any request to be vexatious.

Right of review

73. If the requester is dissatisfied with the response to an information request, they have the right under section 20(1) of the FOISA to request a review (and a right of further appeal to the SIC, and to the Court of Session on a point of law).

74. Requesters must be advised to:

- 74.1. write to the SPSO to request a review within 40 working days of receipt of the decision;
- 74.2. specify their name and address for correspondence;
- 74.3. identify the decision that they wish to have reviewed, or the aspect of the handling of the request that they are unhappy with; and
- 74.4. to address their review request to the SPSO HoCSS.

75. Requests for review should be acknowledged within three working days. The review must be an objective assessment of the complaint and involve a thorough assessment of the handling of the request. Reviews will be undertaken and completed as quickly as possible, and in all cases will be completed within the statutory 20 working days.

Right of Appeal

76. If the requester is dissatisfied with the outcome of the review, they should be advised of their right under the FOISA to appeal to the SIC within six months following the date of receipt of the review notice.
77. It is important that all relevant information, to include information withheld, and any audit trail of decisions taken, is retained until the period for review and appeal to the SIC is complete.

Offences under the FOISA

78. Where a request has been made and the information would be communicable under the FOISA, it is an offence for any person to take any action with the intention of preventing disclosure of information. This applies to both the SPSO and to any person who is employed by, is an officer of, or is subject to the direction of, the SPSO.

Environmental Information (Scotland) Regulations 2004

79. The Environmental Information (Scotland) Regulations 2004 (EIR) give everyone the right to ask for environmental information held by a Scottish public authority. Requests do not need to be in writing, and the 20 working day response deadline can be extended by a further period of up to 20 working days if the volume and complexity makes it impracticable for the authority to deal with the request within the original 20 days. If the request is made in writing, the authority has an obligation to deal with the request under the EIR and an option to also deal with the request under the Freedom of Information (Scotland) Act 2002 (FOISA). However, the authority may choose to apply the exemption in section 39(2) of the FOISA for environmental information, if it is in the public interest to maintain that exemption, and so only deal with the request under the EIR. Review, enforcement and appeals procedures in the EIR mirror those in the FOISA.

Charging

80. The SPSO can charge a 'reasonable amount' under the EIR for environmental information.
81. Where the request is for environmental information which will cost more than £600 to supply, the requester can be asked to pay the full cost of providing the information.

Right of Review

82. If the requester is dissatisfied with the response to an information request, they have the right under regulation 16 (1) of the EIR to request a review (and a right of further appeal to the SIC).
83. Requesters must be advised to:
 - 83.1. write to the SPSO to request a review within 40 working days of receipt of the decision;
 - 83.2. specify their name and address for correspondence;
 - 83.3. identify the decision that they wish to have reviewed, or the aspect of the handling of the request that they are unhappy with; and
 - 83.4. address their review request to the SPSO HoCSS.
84. Requests for review should be acknowledged within three working days. The review must be an objective assessment of the complaint and involve a thorough assessment of the handling of the request. Reviews will be undertaken and completed as quickly as possible, and in all cases will be completed within the statutory 20 working days.

Right of Appeal

85. If the requester is dissatisfied with the outcome of the review, they should be advised of their right under regulation 17 of the EIR to appeal to the SIC within six months following the date of receipt of the review notice.
86. It is important that all relevant information, to include information withheld, and any audit trail of decisions taken, is retained until the period for review and appeal to the SIC is complete.

External Guidance

Scottish Ministers' Section 60 Code of Practice on The Discharge Of Functions By Scottish Public Authorities Under The Freedom Of Information (Scotland) Act 2002 And The Environmental Information (Scotland) Regulations 2004

87. Under section 60 of FOISA and regulation 18 of the EIR, Scottish Ministers may publish a Code of Practice which describes the practice which they consider would be desirable for Scottish public authorities to follow in connection with the discharge of their functions under FOISA and the EIR. This can be found on the Scottish Government website at:
<https://www.gov.scot/publications/foi-eir-section-60-code-of-practice/>.

88. This guidance stresses in particular the best practice to be followed in providing advice and assistance to requesters, and promotes the importance of proactively publishing information.

Scottish Ministers' Section 61 Code of Practice on Records Management by Scottish Public Authorities under the Freedom of Information (Scotland) Act 2002

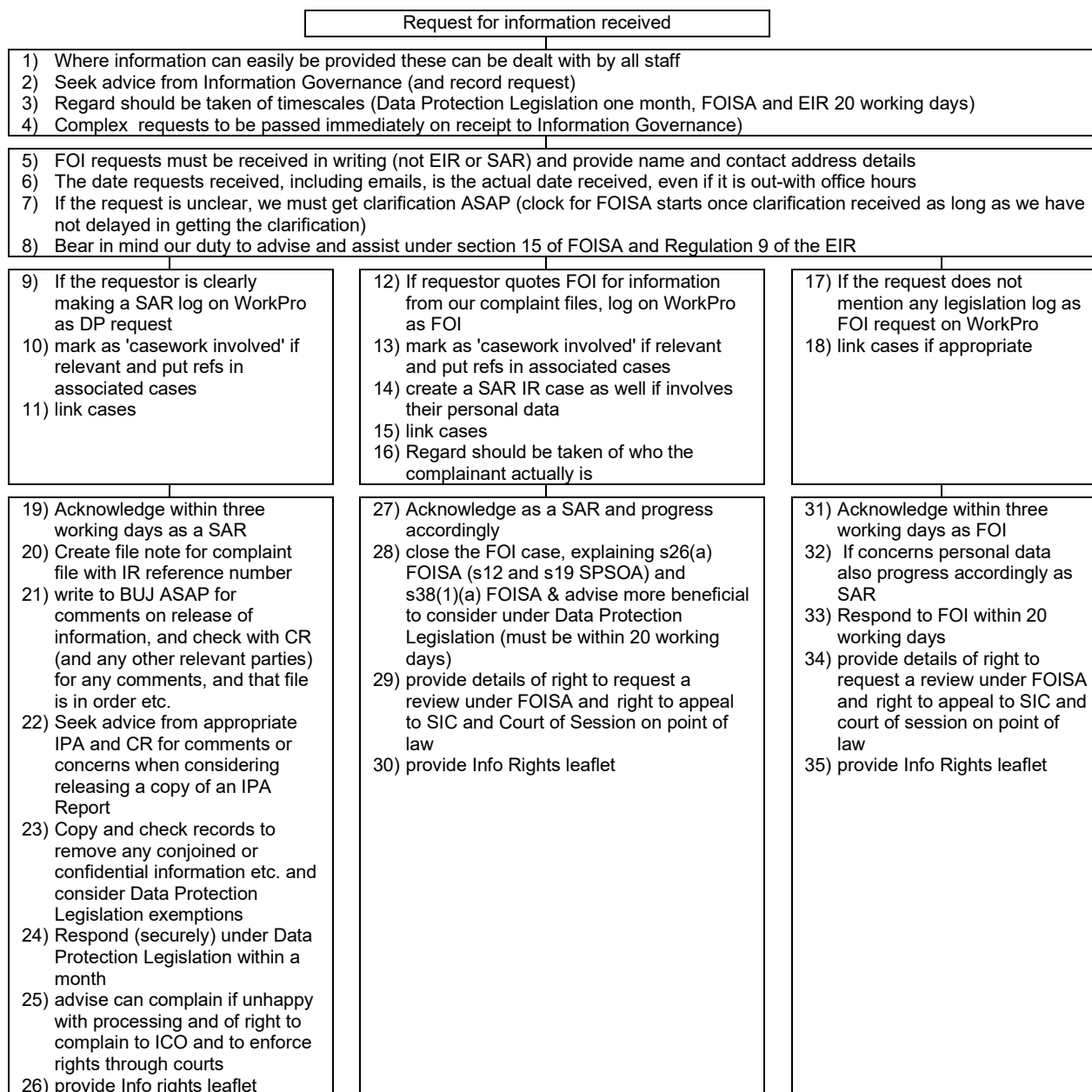
89. Under section 61 of FOISA, Scottish Ministers may publish a Code of Practice (the Code) which describes the practice which they consider would be desirable for Scottish public authorities to follow in connection with the keeping, management and destruction of the authorities' records. The Code of Practice is available on the Scottish Government website at:
<https://www.gov.scot/publications/code-of-practice-on-records-management/>

Scottish Information Commissioner's website

90. [The Scottish Information Commissioner's website](https://www.itspublicknowledge.info/) is the primary reference point. The website has a lot of helpful information, for example, their [publication scheme](#); information on [rights](#), and [FAQs](#); a [law and guidance](#) section; [briefings and guidance on key concepts, and exemptions](#); their [get it right first time infographic](#); previous [decisions](#); a [self-assessment toolkit](#); and their own [internal guidance on responding to requests](#) (under class 2 of their publication scheme). Link to Commissioner's website: <https://www.itspublicknowledge.info/>.

Back to the main [Contents Page](#)

Annex 1: Information request Flowchart



Request for review received (must be made in writing within 40th working day after IR response has been issued)	
<p>Data Protection Legislation</p> <p>No right of review exists for SARs. Concerns with our handling of SARs are logged as data protection complaints (see separate guidance in this handbook).</p>	<p>FOI / EIR</p> <p>36) Log on WorkPro as FOI/EIR review for the HoCSS</p> <p>37) Acknowledge (within three working days)</p> <p>38) Respond within 20 working days</p> <p>39) provide details of appeal to SIC (and to Court of Session on point of law)</p> <p>40) Provide Info Rights leaflet</p> <p>41) retain information for six months from date of final decision in case of appeal</p> <p>42) Log any appeals made to SIC on WorkPro</p>

Back to the main [Contents Page](#)

Data Protection Legislation

Issued: February 2012

Contents

The Information Commissioner's Office (ICO)	28
Data Protection Audit	28
Data Controller	28
Processing	28
Data Protection Principles	29
Rights	29
Correcting information	29
Preventing processing of information	30
Subject access requests	30
Data protection complaints	30
Gender Recognition Act 2004	31
External Guidance	31
The ICO Guidance	31
The Ombudsman Association guidance	31

Back to the main [Contents Page](#)

The Information Commissioner's Office (ICO)

1. The SPSO is legally obliged to protect any personal information that we hold, and we are currently registered as a data controller with ICO (Registration Number: Z7336887; Date Registered: 29 Nov 2002). The ICO is there to help organisations understand their obligations and keep them updated as and when they change. Information and guidance on all areas of Data Protection and our responsibilities can be found on the ICO website at www.ico.gov.uk which should be the main point of reference.
2. If an individual believes there has been a breach of the Data Protection Legislation they can ask the ICO to assess whether our processing of personal data complies with the Legislation. The ICO can ask us to take steps to comply with the Legislation, issue enforcement notices and even impose financial penalties in respect of deliberate or reckless handling of personal data which seriously breaches the Legislation. The ICO cannot award compensation, only the courts can do this.

Data Protection Audit

3. The ICO may make an assessment as to whether an organisation's processing of personal data follows good practice. Following completion of the audit, the ICO will provide a comprehensive report to the organisation along with an executive summary, which is published on the ICO website with the data controller's agreement. Organisations can register their interest with the ICO on their website to be considered for a data protection audit.

Data Controller

4. A data controller is a person who determines the purpose for which and the manner in which any personal data are, or are to be, processed. The SPSO is a data controller.

Processing

5. Processing means obtaining, recording, or holding the information or carrying out any operation or set of operations on it, including:
 - 5.1. organisation, adaptation or alteration;
 - 5.2. retrieval, consultation or use;
 - 5.3. disclosure by transmission, dissemination or otherwise making available; and
 - 5.4. alignment, combination, blocking, erasure or destruction.

Data Protection Principles

6. Data Protection Legislation works in two ways. Firstly, it helps to protect individuals' interests by obliging organisations to manage the information they hold in a proper way. It states that anyone who processes personal data must comply with the data protection principles, which make sure that it is:
 - 6.1. fairly and lawfully processed in a transparent manner;
 - 6.2. processed for limited purposes;
 - 6.3. adequate, relevant and not excessive;
 - 6.4. accurate and up to date;
 - 6.5. not kept for longer than is necessary;
 - 6.6. secure; and
 - 6.7. the controller must be responsible for, and be able to demonstrate, compliance with the principles.

Rights

7. The second area covered by Data Protection Legislation gives individuals important rights, including but not limited to the right to know what information is held about them and the right to correct information that is wrong.

Correcting information

8. If individuals believe the personal data that we hold is inaccurate, they can write to us to tell us what they believe is wrong with their information and what should be done to correct it.
9. If a member of the public is concerned about our information rights practices, where they felt inaccurate information was contained within our file, we the organisation are responsible to deal with this, to put right anything that's gone wrong.
10. The Data Protection Legislation imposes obligations on us to ensure the accuracy of the personal data we process.
11. We must comply with these provisions by:
 - 11.1. taking reasonable steps to ensure the accuracy of any personal data we obtain;
 - 11.2. ensure that the source of any personal data is clear;
 - 11.3. carefully consider any challenges to the accuracy of information; and
 - 11.4. consider whether it is necessary to update the information.

12. A concern in the content of a document can be someone else's opinion; opinions are naturally subjective and can depend on the understanding and experiences of the individual concerned. The fact that someone else might hold a different opinion does not make the first opinion inaccurate. A view expressed by the complaints reviewer is a statement of opinion rather than fact and a difference of opinion may not constitute inaccurate information we hold.

Preventing processing of information

13. Individuals can also ask the SPSO not to process information about them that causes substantial unwarranted damage or distress. A response must be provided within one month. The SPSO is not always bound to act on the request.
14. Where we receive a relevant request to exclude a report from publication, the Communications team have wording to provide reassurance about anonymity. If there are still concerns, the Ombudsman will make the final decision. There is a requirement to make reports available to any person, unless we direct otherwise (taking into account public interest as well as the interests of individuals). We might refuse a request if we have compelling reasons for doing so. We might also rely on an exemption if we consider it is likely to prejudice our functions (and also if the request is unfounded/excessive). A key consideration will be about possible identification, and what affect this could have.

Subject access requests

15. See separate [Subject Access Requests SPSO Guidance](#)

Data protection complaints

16. Individuals can complain to us if they are concerned about how we are handling their personal data. We must respond to any concerns as soon as possible, and within one month.
17. Advice should be sought from the CIGO when responding to any data protection problems individuals have raised. Alternatively, complaints can be passed as soon as possible to the CIGO to respond directly.
18. Data protection complaints should be recorded on WorkPro.
19. If an individual is unhappy with our response to any data protection problems they have raised, they can ask for a review from the HoCSS.
20. Individuals always have the right to [lodge a complaint](#) with the Information Commissioner's Office (ICO).

21. Further details can be found in our Information Rights leaflet, available on our website at <https://www.spsso.org.uk/sites/spsso/files/leaflets/InformationRights.pdf>

Gender Recognition Act 2004

22. See separate guidance in relation to processing gender reassignment information. Link to the [Gender Recognition Act 2004 – process](#).

External Guidance

The ICO Guidance

23. The ICO has developed guidance to assist in complying with Data Protection Legislation. This very useful guidance can be found on their website at: <https://ico.org.uk>

The Ombudsman Association guidance

24. The Ombudsman Association (OA) has developed guidance in conjunction with the ICO to assist OA members in complying with their obligations. This very useful guidance can be found at: <http://www.ombudsmanassociation.org>.

Back to the main [Contents Page](#)

Data Protection policy and procedure

Issued: July 2018

Data Controller: Scottish Public Services Ombudsman

Contents

Scope of policy	2
Purpose of policy.....	2
Data Protection fee	3
Brief introduction to Data Protection Legislation	3
Data Protection Principles	3
Satisfaction of principles	4
Record of processing	5
Personal data	5
Special categories of personal data.....	6
Individual rights	7
Policy statement	7
Key risks.....	8
Data Protection Impact Assessments.....	9
Further guidance	9
Annex 1: Responsibilities, training and non-compliance actions.....	10
Annex 2: Confidentiality.....	16
Annex 3: Security	18
Annex 4: Data recording and storage	22
Annex 5: Protecting Personal Data	23
Annex 6: Transparency	26
Annex 7: Appropriate Policy Document for special category and criminal offence data	29

Back to the main [Contents Page](#)

Scope of policy

1. This policy applies to all staff employed by the SPSO on a permanent, fixed-term, loan or temporary contract.
2. This policy applies to all situations where we process (collect, store, use, share) personal data about living individuals. It includes, but is not limited to information processed electronically, on paper, in emails, on close circuit television (CCTV), in employee files, in internal memos, in photographs and on audio equipment. Individuals may include for example current, past and prospective employees, customers, advisers and others with whom we communicate.
3. See separate HR policy specifically for managing SPSO employee personal data – SPSO Managing Personal Data in the [Working for SPSO](#) handbook.

Purpose of policy

4. The SPSO processes (collects, stores, uses, shares) personal data about living individuals as part of our operational activities, and has a duty to ensure this processing is in accordance with legal requirements. The main legislative requirements are in the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).
5. The SPSO recognises the importance of privacy by design and the correct and lawful treatment of personal data; it maintains confidence in the organisation and provides for successful operations.
6. The purpose of this policy is to enable SPSO to:
 - 6.1. establish a framework for the processing of personal data (regardless of format) which ensures we meet all our responsibilities and safeguards the rights of the individuals;
 - 6.2. comply with the law in respect of the data it holds about individuals;
 - 6.3. follow good practice;
 - 6.4. protect SPSO's staff and other individuals; and
 - 6.5. protect SPSO from the consequences of a breach of its responsibilities.
7. Staff will be provided with guidance, training and procedures to aid compliance with this policy.

Data Protection fee

8. The SPSO must pay the ICO an annual data protection fee. The SPSO have a current registration under the Act and falls within tier 2: small and medium organisations.

Brief introduction to Data Protection Legislation

9. The SPSO is committed to compliance with the requirements of the UK GDPR and the DPA (Data Protection Legislation). The Data Protection Legislation establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details.

Data Protection Principles

10. All personal data will be processed (obtained, used, shared, handled, transported, stored) in accordance with the Data Protection Principles set out in the Data Protection Legislation.
11. Article 5 of the UK GDPR requires that personal data shall be:
 - 11.1. processed lawfully, fairly and in a transparent manner in relation to individuals;
 - 11.2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
 - 11.3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
 - 11.4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
 - 11.5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific

or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

- 11.6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- 12. Article 5(2) requires that the controller shall be responsible for, and be able to demonstrate, compliance with the principles.

Satisfaction of principles

- 13. In order to meet the requirements of the principles, the SPSO will:
 - 13.1. observe fully the conditions regarding the fair collection and use of personal data;
 - 13.2. meet its obligations to specify the purposes for which personal data is used;
 - 13.3. collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements;
 - 13.4. ensure the quality of personal data used;
 - 13.5. apply strict checks to determine the length of time personal data is held;
 - 13.6. ensure all the rights of individuals can be fully exercised;
 - 13.7. take the appropriate technical and organisational security measures to safeguard personal data (from accidental destruction, theft or any other loss);
 - 13.8. put appropriate data protection measures in place throughout the entire lifecycle of our processing operations; and
 - 13.9. maintain documentation of our processing activities.
- 14. In addition, SPSO will ensure that:
 - 14.1. there is someone with specific responsibility for data protection in the organisation;
 - 14.2. a Data Protection Officer is in place;
 - 14.3. everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
 - 14.4. everyone managing and handling personal information is appropriately trained to do so;
 - 14.5. processors are compliant with Data Protection Legislation;
 - 14.6. anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;

- 14.7. queries about handling personal information are promptly and courteously dealt with;
- 14.8. methods of handling personal information are regularly assessed and evaluated;
- 14.9. performance with handling personal information is regularly assessed and evaluated;
- 14.10. privacy by design is satisfied and data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests are carried out;
- 14.11. privacy information is provided to individuals, regularly maintained and updated;
- 14.12. we have suitable accountability processes in place and can provide auditable tracking of processing;
- 14.13. the lawful basis for processing is understood and can be applied to all processing;
- 14.14. where personal data has to be taken off-site, documented procedures will be in place to mitigate against any loss; and
- 14.15. personal data is not transferred abroad without suitable safeguards.

Record of processing

- 15. We will maintain records on several things such as processing purposes, data sharing and retention and will make the records available to the ICO on request.
- 16. In particular, we document the following information:
 - 16.1. the name and contact details of SPSO and our data protection officer;
 - 16.2. the purposes of our processing;
 - 16.3. a description of the categories of individuals and categories of personal data;
 - 16.4. the categories of recipients of personal data;
 - 16.5. details of any transfers to third countries including documenting the transfer mechanism safeguards in place;
 - 16.6. retention schedules; and
 - 16.7. a description of our technical and organisational security measures.

Personal data

- 17. This policy applies to information relating to identifiable individuals. This includes any expression of opinion about the individual and any indication of the intentions of the SPSO or any other person in respect of the individual.

18. Personal data is defined as 'any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.'
19. This definition provides for a wide range of personal identifiers to constitute personal data, including:
 - 19.1. name, identification number, location data or online identifier; or
 - 19.2. one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
20. The Data Protection Legislation applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.
21. Personal data that has been pseudonymised, for example, key-coded – can fall within the scope of the Data Protection Legislation depending on how difficult it is to attribute the pseudonym to a particular individual.
22. The types of personal data that the SPSO may process includes information about: current, past and prospective employees; advisers, complainants; applicants, aggrieved individuals and interested parties; suppliers and others with whom SPSO communicates. This personal data, whether it is held on paper, on computer or other media, will be subject to the appropriate legal safeguards as specified in the Data Protection Legislation.

Special categories of personal data

23. The Data Protection Legislation refers to sensitive personal data as special categories of personal data.
24. The special categories specifically are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
25. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.
26. Where we process special category or criminal conviction and offence data:
 - 26.1. we document the condition for processing we rely on in the DPA in our register;

- 26.2. we document the lawful basis for our processing in our register and privacy notice; and
- 26.3. we retain and erase the personal data in accordance with our retention and disposal policy.

Individual rights

- 27. The Data Protection Legislation provides the following rights for individuals (subject to exemptions):
 - 27.1. the right to be informed;
 - 27.2. the right of access;
 - 27.3. the right to rectification;
 - 27.4. the right to erasure;
 - 27.5. the right to restrict processing;
 - 27.6. the right to data portability;
 - 27.7. the right to object; and
 - 27.8. rights in relation to automated decision making and profiling.
- 28. Individuals also have the right to withdraw consent where given, and the right to complain to the ICO.
- 29. Any requests to exercise these rights are forward to the CIGO for advice.

Policy statement

- 30. SPSO recognises that its first priority under the Data Protection Legislation is to avoid causing harm to individuals. In the main this means:
 - 30.1. keeping information securely in the right hands, and
 - 30.2. holding good quality information.
- 31. Secondly, the Data Protection Legislation aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account.
- 32. SPSO fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Legislation and will ensure that it treats personal information lawfully and correctly.
- 33. SPSO will:
 - 33.1. comply with both the law and good practice;
 - 33.2. respect individuals' rights;
 - 33.3. be open and honest with individuals whose data is held;

- 33.4. be accountable and demonstrate compliance;
- 33.5. take responsibility for complying at the highest management level and throughout the SPSO; and
- 33.6. provide training and support for staff who handle personal data, so that they can act confidently and consistently.

Key risks

- 34. The Information Commissioner identifies the main risks where non-compliance with the data protection principles may result in damage to both individuals and the organisation:
 - 34.1. A failure to identify and implement controls by which compliance with data protection can be measured and reported, raises the risk of the 'data controller' being unaware of whether it is meeting its obligations, resulting in poor data protection practice or potential breaches of the Data protection legislation not being identified or addressed.
 - 34.2. A failure to provide and implement staff training and awareness regarding the correct use and management of personal records raises the risk of loss or inappropriate usage of data, with the potential to cause damage and distress to individuals, and reputational damage to the 'data controller'.
 - 34.3. A failure to implement security measures which adequately protect electronically held personal data raises the risk of loss, damage or inappropriate access to data leading to distress to the affected individuals, reputational damage to the 'data controller' and non-compliance with the Data protection Legislation.
 - 34.4. A failure to appropriately control and secure manual personal data both within and outside the 'data controller's' premises raises the risk that personal data will be lost, damaged or inappropriately disclosed, resulting in distress to the individual and non-compliance with the Data Protection Legislation.
 - 34.5. A failure to ensure Subject Access Requests are dealt with appropriately raises the risk that an individual's rights to information may be compromised resulting in distress to the individual and non-compliance with the Data Protection Legislation.
- 35. SPSO has identified the following potential key risks, which this policy is designed to address:
 - 35.1. breach of confidentiality (information being given out inappropriately);

- 35.2. insufficient clarity about the range of uses to which data will be put, leading to Data Subjects being insufficiently informed;
- 35.3. failure to offer choice about data use when appropriate;
- 35.4. breach of security by allowing unauthorised access;
- 35.5. harm to individuals if personal data is not up to date;
- 35.6. insufficient clarity about the way personal data is being used and
- 35.7. inadequate Data Processor contracts.

Data Protection Impact Assessments

- 36. A Data Protection Impact Assessment (DPIA) is a process to help us identify and minimise the data protection risks of a project. We must do a DPIA for processing that is likely to result in a high risk to individuals. This includes some specified types of processing. It is also good practice to do a DPIA for any other major project which requires the processing of personal data. We can use the ICO screening checklists to help decide when to do a DPIA.
- 37. Our DPIA must:
 - 37.1. describe the nature, scope, context and purposes of the processing;
 - 37.2. assess necessity, proportionality and compliance measures;
 - 37.3. identify and assess risks to individuals; and
 - 37.4. identify any additional measures to mitigate those risks.
- 38. To assess the level of risk, we must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.
- 39. We should consult our data protection officer and, where appropriate, individuals and relevant experts. Any processors may also need to assist us.
- 40. If we identify a high risk that we cannot mitigate, we must consult the ICO before starting the processing. The ICO will give written advice within eight weeks, or 14 weeks in complex cases. If appropriate, they may issue a formal warning not to process the data, or ban the processing altogether.
- 41. [Link to DPIA guidance](#)

Further guidance

- 42. Further detailed data protection guidance is available on the ICO website at <https://ico.org.uk/>

Annex 1: Responsibilities, training and non-compliance actions

Responsibilities

Leadership Team

1. Senior Management regard the lawful and correct treatment of personal information as of vital importance to successful operations, and to maintaining confidence between the SPSO and those with whom we deal.

Head of Corporate and Shared Services (HoCSS)

2. The HoCSS has overall responsibility for:
 - 2.1. ensuring compliance with the current applicable legal framework; and
 - 2.2. ensuring that all personal data held by the SPSO is managed in accordance with the law and internally adopted standards, policies and procedures.
3. The HoCSS has the role of arbiter in respect of Data Protection complaints received. The HoCSS will review any decisions and report to the LT governance meeting on the number and outcome of DP complaints.

Data Protection Officer (DPO)

4. We have a duty to appoint a DPO. The SPCB shares the services of its DPO with officeholders, including the SPSO. The MoU between the SPSO and the SPCB gives details about the service, including DPO accessibility.
5. The DPO:
 - 5.1. assists us to monitor internal compliance with Data Protection Legislation, our policies, awareness-raising, training, and audits;
 - 5.2. informs and advises on our data protection obligations;
 - 5.3. is involved in issues relating to the protection of personal data;
 - 5.4. provides advice regarding Data Protection Impact Assessments and monitors the process;
 - 5.5. acts as contact point for data subjects and the ICO (the CIGO is the main contact point for SPSO); and
 - 5.6. reports to the LT.

Corporate Information Governance Officer (CIGO)

6. The GIGO has the following operational responsibilities:
 - 6.1. briefing the LT on Data Protection responsibilities;

- 6.2. developing and reviewing Data Protection and related policies, guidance and procedures;
 - 6.3. providing advice regarding Data Protection Impact Assessments and monitors the process;
 - 6.4. advising other staff on Data Protection issues;
 - 6.5. ensuring that Data Protection induction and training takes place;
 - 6.6. coordinating subject access requests and other data protection requests/concerns;
 - 6.7. point of contact for data subjects and the ICO;
 - 6.8. consulting on unusual or controversial disclosures of personal data;
 - 6.9. consulting on contracts with Data Processors;
 - 6.10. supporting all members of staff to comply with their obligations under the Legislation;
 - 6.11. Monitoring the proper functioning of data protection systems
 - 6.12. providing advice and guidance about third party duty of confidentiality issues that may arise;
 - 6.13. providing advice and guidance in respect of exemptions to the legislation;
 - 6.14. ensuring the capturing, indexing, preservation and destroying of information in accordance with the law and the SPSO's business requirements;
 - 6.15. agreeing access rights to documents and records; and
 - 6.16. regular assurance reporting to the LT
7. The CIGO is responsible for maintaining this policy. For any questions about this policy, or to report misuse of corporate or personal data, please contact the CIGO.

Specific other staff

8. Line Managers are responsible for ensuring that their direct reports understand the scope and implications of this policy, that good data protection practice is followed and that the CIGO is informed of any changes in the uses of personal data.
9. The Corporate Services Manager has responsibility for physical and electronic security within SPSO.
10. The HR Officer has responsibility for ensuring that all employees have a record of receiving this policy in their file.

All Staff

11. All staff are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work and to be fully aware of their duties and responsibilities under the Data Protection Legislation.
12. All employees are responsible for:

- 12.1. familiarising themselves with the implications of data protection in their job;
- 12.2. adhering to this policy and supporting guidance;
- 12.3. reporting any activities that do not comply with this policy;
- 12.4. seeking guidance and advice where necessary;
- 12.5. checking that any personal data that they provide is accurate and up to date;
- 12.6. informing the SPSO of any changes to information which they have provided, for example, changes of address; and
- 12.7. checking any information that the SPSO may send out from time to time, giving details of information that is being kept and processed

Staff training and acceptance of responsibilities

Induction

13. All staff who have access to any kind of personal data will have their responsibilities outlined during their induction procedures.

Continuing training

14. The Data Protection Legislation requires us to ensure that anyone acting under our authority with access to personal data does not process that data unless we have instructed them to do so. It is therefore vital that our staff understand the importance of protecting personal data, are familiar with our security policy and put its procedures into practice.
15. Compulsory data protection training is provided annually. We will provide further opportunities for staff to explore Data Protection issues through training, including our responsibilities as a data controller under the Data Protection Legislation; and staff responsibilities for protecting personal data – including the possibility that they may commit criminal offences if they deliberately try to access or disclose these data without authority

Staff acceptance

16. This policy will be included in the annual staff declarations

Documentation

17. Information Governance Handbook and other related policies; including:
 - 17.1. Conduct and Behaviour policy
 - 17.2. Disciplinary procedure
 - 17.3. Working from home
 - 17.4. File Management guidance
 - 17.5. Recruitment and Selection

- 17.6. Clear Desk and Screen policy
- 17.7. Records Management plan
- 17.8. Records Management policy
- 17.9. Progress Update Reviews
- 17.10. Business Classification Scheme
- 17.11. Retention and Disposal policy
- 17.12. Protective marking system
- 17.13. Business Continuity policy
- 17.14. Incident Response plan
- 17.15. Cyber Resilience plan
- 17.16. Cyber Essentials certificate
- 17.17. ICT Strategy
- 17.18. IT Security policy
- 17.19. Information sharing policy
- 17.20. Data sharing agreements / MoUs / contracts
- 17.21. Records Management and Security guidance
- 17.22. Data protection policy
- 17.23. Data protection registration
- 17.24. Data security policy
- 17.25. Appropriate Policy document
- 17.26. Breach protocol
- 17.27. SARs guidance
- 17.28. DPIA guidance
- 17.29. DPIAs
- 17.30. Code of Professional Conduct
- 17.31. Risk Management and Incident Reporting policy
- 17.32. Communications Handbook
- 17.33. Ombudsman Association Data Protection guidance
- 17.34. Privacy Notices
- 17.35. Register of Processing Activities
- 17.36. Information Asset Register
- 17.37. Information Rights leaflet
- 17.38. Quarterly Assurance reports

Non-compliance actions

Enforcement

- 18. Employees found to be in violation of this policy by either unintentionally or maliciously stealing, using or otherwise compromising corporate or personal data may be subject to disciplinary action under [SPSO's disciplinary procedures](#).

19. Any employee who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with their Line Manager or the HR Officer in the first instance

Monetary Penalties

20. The Information Commissioner can serve notices requiring organisations to pay for serious breaches of the Data Protection Legislation. In brief, the Commissioner may impose a monetary penalty notice if a data controller has seriously contravened the data protection principles and the contravention was of a kind likely to cause substantial damage or substantial distress. In addition the contravention must either have been deliberate or the data controller must have known or ought to have known that there was a risk that a contravention would occur and failed to take reasonable steps to prevent it.

Offences under the Act

21. It is an offence to knowingly or recklessly:
 - 21.1. handle personal data without the authorisation of the controller;
 - 21.2. procure or disclose the personal data of another person without the authorisation of the controller;
 - 21.3. retain personal data, after it has been obtained, without the authorisation of the person who was controller when it was obtained;
 - 21.4. re-identify de-identified personal data without the authorisation of the controller who de-identified the personal data; and
 - 21.5. process personal data that has been re-identified (which was an offence), without the authorisation of the controller responsible for the de-identification.
22. It is also an offence:
 - 22.1. to sell, or offer to sell personal data that has been unlawfully obtained, which includes advertising this data for sale;
 - 22.2. where an access or data portability request has been received, it is an offence for a controller or related persons, including a processor, to obstruct the provision of information which an individual would be entitled to receive;
 - 22.3. to require another person to request access to a relevant record (includes a health record and records relating to a conviction or caution). Such a request is not permitted in connection with recruitment or continued employment of an employee or a contract for services; and
 - 22.4. if a person requires another person to make an access request as a condition of providing goods, facilities or services to them or another (which are provided to the public or a section of the public).

23. Defences of the above offences are detailed in the Data Protection Legislation.

Annex 2: Confidentiality

Scope

1. Confidentiality applies to a much wider range of information than Data Protection. Please refer to the Terms and Conditions of Employment, Confidentiality Statement, the [Conduct and Behaviour Policy](#), and [Working From Home Policy](#).

Understanding of confidentiality

2. When working for SPSO, staff will often need to have access to confidential information which may include, for example:
 - 2.1. Personal information about our customers.
 - 2.2. Information about the internal business of SPSO.
 - 2.3. Personal information about colleagues working for SPSO.
3. SPSO is committed to keeping this information confidential, in order to protect people and SPSO itself. Confidential means that all access to information must be on a need to know and properly authorised basis. Staff must use only the information they have been authorised to use, and for purposes that have been authorised. Staff should also be aware that under Data Protection Legislation, unauthorised access to data about individuals is a criminal offence.
4. Staff must assume that information is confidential unless they know that it is intended by SPSO to be made public.
5. Staff must also be particularly careful not to disclose confidential information to unauthorised people or cause a breach of security. In particular staff must:
 - 5.1. not compromise or seek to evade security measures (including computer passwords);
 - 5.2. be particularly careful when sending information to other parties;
 - 5.3. not gossip about confidential information, either with colleagues or people outside SPSO;
 - 5.4. not disclose information — especially over the telephone — unless they are sure that they know who they are disclosing it to, and that they are authorised to have it; and
 - 5.5. never put sensitive information or personal data into generative AI tools.
6. If staff are in doubt about whether to disclose information or not, they must not guess. Staff should withhold the information while they check with an appropriate person whether the disclosure is appropriate.
7. Confidentiality obligations continue to apply indefinitely after staff have stopped working for SPSO.

Communication with Data Subjects

8. SPSO have privacy information for Data Subjects, setting out how their information will be used. This will be provided when appropriate, available on request, and on the SPSO web site.

Communication with staff

9. Staff must sign a short statement indicating that they have been made aware of their confidentiality responsibilities.
10. SPSO have privacy information for staff.

Authorisation for disclosures not directly related to the reason why data is held

11. Where anyone within SPSO feels that it would be appropriate to disclose information in a way contrary to the confidentiality policy, or where an official disclosure request is received, this will only be done with consultation of the CIGO. All such discussion and disclosures will be documented.

Annex 3: Security

Scope

1. This document defines the data security policy of the SPSO. The SPSO takes the privacy of our employees and complainants very seriously. To ensure that we are protecting our corporate and complainant data from security breaches, this policy must be followed and will be enforced to the fullest extent.
2. The goal of this policy is to inform employees at the SPSO of the rules and procedures relating to data security compliance.
3. This section of the policy only addresses security issues relating to personal data. It does not cover security of the building, business continuity or any other aspect of security.
4. The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff are responsible for ensuring that:
 - 4.1.1. any personal data which they hold is kept securely; and
 - 4.1.2. personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.
5. Data Protection Legislation states:
 'Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk'.
6. The SPSO must ensure the 'confidentiality, integrity and availability' of our systems and services and the personal data we process within them. We must ensure that:
 - 6.1. the data can be accessed, altered, disclosed or deleted only by those we have authorised to do so (and that those people only act within the scope of the authority we give them);
 - 6.2. the data we hold is accurate and complete in relation to why we are processing it; and
 - 6.3. the data remains accessible and usable, ie, if personal data is accidentally lost, altered or destroyed, we should be able to recover it and therefore prevent any damage or distress to the individuals concerned

Specific risks

7. The SPSO has identified the following risks:
 - 7.1. information passing between the SPSO and BUJ's or advisers could go astray or be misdirected;
 - 7.2. processing of sensitive and confidential information;
 - 7.3. potential damage and distress if compromised;
 - 7.4. staff with access to personal information could misuse it;
 - 7.5. advisers could continue to be sent information after they have stopped working for SPSO, if their records are not updated promptly;
 - 7.6. poor web site security might give a means of access to information about individuals once individual details are made accessible online;
 - 7.7. staff may be tricked into giving away information, either about complainants or colleagues, especially over the telephone, through 'social engineering';
 - 7.8. personal information accidentally disclosed in reports;
 - 7.9. cyber security;
 - 7.10. processing information off network and out of office; and
 - 7.11. email.

Data Types

8. The SPSO deals with two main kinds of data:
 - 8.1. Information processed in connection with our functions under the SPSO Act (including special category data).
 - 8.2. Employment and recruitment records.

Setting security levels

9. Access:
 - 9.1. to casework is by function – for business needs only;
 - 9.2. to employment information is controlled by function; and
 - 9.3. privileges will be updated as required when an employee joins or leaves the SPSO.
10. [SPSO Managing Personal Data Policy](#) provides more detail about employment and recruitment security.

Data Classifications

11. The SPSO business classification system is modelled on the functions of the organisation. See Business Classification policy.
12. All information the SPSO handles meets the criteria for OFFICIAL status only. Protective marking guidance helps SPSO staff determine when to use additional

protective marking on their documents in order to indicate to others the levels of protection required to help prevent the compromise of information.

Security measures

13. SPSO utilises the secure SCOTS Connect service provided by the Scottish Government to host our network services. Users of the network must be formally registered with an agreed level of access. Access rights of users who have left are removed immediately. The building is adapted to meet the Scottish Government security requirements for the SCOTS network:
 - 13.1. access to the premises is controlled;
 - 13.2. all employees have met the requirements for receiving a Disclosure Scotland Certificate;
 - 13.3. a cyber-resilience plan in place;
 - 13.4. Cyber Essentials accreditation;
 - 13.5. the [SPSO Clear Desk and Screen policy](#) details the procedures to reduce the risk of unauthorised access, loss of, and damage to information during and outside normal working hours;
 - 13.6. a check of office is undertaken annually;
 - 13.7. the [SPSO policy 'Working from home'](#) describes confidentiality and security rules for business conducted on behalf of the SPSO;
 - 13.8. the [SPSO Records Management and Security Guidance: sharing information off-network and out-of-office](#) details issues that must be considered to ensure that any SPSO information worked on out of the office and shared off-network is kept confidential and protected from loss of unauthorised access and exploitation (a data security checklist is available for use in conjunction with this);
 - 13.9. working from home data security checklist;
 - 13.10. a confidentiality statement included with annual staff declarations;
 - 13.11. DPIAs;
 - 13.12. data minimisation;
 - 13.13. retention and disposal arrangements;
 - 13.14. business continuity policy;
 - 13.15. incident response plan;
 - 13.16. assurance reporting;
 - 13.17. Data held on a secure case handling system or eRDM;
 - 13.18. closed usb drives;
 - 13.19. Data sharing via secure electronic system (or approved secure courier) and
 - 13.20. procedures, training and guidance to all staff regarding the Data Protection Legislation requirements, and on data security.

14. SPSO must only appoint processors who can provide 'sufficient guarantees' that the requirements of the Data Protection Legislation will be met and the rights of data subjects protected. We must ensure that all contractors, or other trusted third parties who have access to personal data held or processed for or on behalf of SPSO are aware of their duties and responsibilities under the DP Legislation. Agreements or contracts in place accordingly.

Protecting personal data

15. See report builder guidance, with reports clearly labelled and restricted, and personal data minimised.
16. See also '[Tips for SPSO staff on how to protect the personal data they hold](#)'

Protocol for security incidents

17. See section on [Protocol for data security incidents](#)

Annex 4: Data recording and storage

Accuracy

1. Data on any individual will be held in as few places as necessary, and all staff will be discouraged from establishing unnecessary additional data sets

Storage

2. Casework is stored on a secure bespoke case handling system. Reports generated from our casework handling system are clearly marked and restricted. Any physical case files or supporting paperwork / discs are securely locked away either within teams or archives until destroyed. Devices are encrypted/password protected. Out of office security guidance and checklists. All other non-casework is stored on an ERMS. Call recordings are held on a secure server or transferred into the case handling system. Employee paper records are stored in securely lockable filing cabinets

Retention periods

3. SPSO retention periods are set out in the [Retention and Disposal Policy](#). We will keep some forms of information for longer than others. All staff are responsible for ensuring that information is not kept for longer than necessary

Archiving

4. The procedure for archiving and destroying data is set out in the [Retention and Disposal Policy](#) and supporting guidance and is managed by Corporate Services.

Data minimisation

5. We should not hold more information than we need to. Where we have been given / hold information that is not necessary or relevant, we return, redact or delete. In most cases, reports should be pseudonymised.

Gender Recognition Act 2004

6. See also separate guidance in respect of storing gender reassignment information. Link to the [Gender Recognition Act 2004 - process](#)

Annex 5: Protecting Personal Data

Tips for SPSO staff on how to protect the personal data they hold:

1. Be aware that you can be prosecuted if you deliberately give out personal details without permission.
2. Be wary of people who may try and trick you into giving out personal details; especially be aware of media requests.
3. Do not believe emails that appear to come from your bank that ask for your account, credit card details or your password (a bank would never ask for this information in this way).
4. Do not open spam, not even to ask for no more mailings. Delete the email.
5. Carry out any appropriate identity checks before giving out personal details;
 - 5.1. Must be satisfied that you are speaking to the complainant (or authorised person) before sharing any information.
 - 5.2. Asking for reference number on open cases is recommended (these are not public for open cases).
 - 5.3. You can also ask for other details if in any doubt (CR, address, email, telephone etc.).
 - 5.4. If still unsure, a good way is to call back on the number we hold.
 - 5.5. Reference can no longer be relied on for closed/published cases so must take special care to ensure it is the complainant if contacted about a published case.
 - 5.6. Staff directly involved with the case will usually have a relationship with the complainant and should really be the only people that need to share detailed information about a case.
6. Carry out appropriate checks (of the information and recipient details) before sharing any information, by email, telephone or hardcopy.
7. Minimise personal data as much as possible. Anonymise / pseudonymise information, for example personal data in reports, which should also be labelled clearly, and restricted where appropriate.
8. Only provide personal details, for example over the telephone, when the information is necessary for carrying out our functions.

9. Only include necessary information when sharing (for example in emails, including internal emails) and anonymise / pseudonymise information as much as possible. Reference numbers should be sufficient in many cases.
10. Consider whether the content of emails should be encrypted or password protected.
11. If sending a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending. Consider using our secure file sharing system.
12. Check you selected the correct email address before you press send. Consider copy and paste to reduce risk of incorrect address being typed, or incorrect autofill occurring.
13. Be careful when using group email addresses.
14. Make sure you use bcc if you do not want to reveal recipients in emails.
15. Consider asking email recipients to acknowledge receipt of emails.
16. Do not send offensive emails about other people, their private lives or anything else that could bring the SPSO into disrepute.
17. Consider whether it is appropriate to leave a message on an answering machine, and if you do minimise the personal data you include.
18. Encrypt any personal information held electronically if it will cause damage or distress if it is lost or stolen.
19. All electronic devices leaving the office that contain confidential and personal data should be encrypted/password protected (with passwords held separately), especially where they contain sensitive information about individuals.
20. Use strong passwords (at least seven characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols.
21. Do not share passwords.
22. Dispose of all confidential paper waste in the bins provided.
23. Never put sensitive information or personal data into generative AI tools

The above should be read in conjunction with SPSO [Records Management and Security Guidance: processing information off network and out-of-office](#). See also the [WFH](#)

security checklist, and Clear Desk and Screen Policy. [Basic security tips from the ICO](#) are also available.

Annex 6: Transparency

Commitment

1. Individuals have the right to be informed about the collection and use of their personal data, subject to exemptions. This is a key transparency requirement under the Data Protection Legislation.
2. SPSO is committed to providing individuals with clear and concise information about what we do with their personal data. We will provide individuals with the following privacy information, the:
 - 2.1. name and contact details of our organisation;
 - 2.2. name and contact details of our representative (if applicable);
 - 2.3. contact details of our data protection officer (if applicable);
 - 2.4. purposes of the processing;
 - 2.5. lawful basis for the processing;
 - 2.6. legitimate interests for the processing (if applicable);
 - 2.7. categories of personal data obtained (if the personal data is not obtained from the individual it relates to);
 - 2.8. recipients or categories of recipients of the personal data;
 - 2.9. details of transfers of the personal data to any third countries or international organisations (if applicable);
 - 2.10. retention periods for the personal data;
 - 2.11. rights available to individuals in respect of the processing;
 - 2.12. right to withdraw consent (if applicable);
 - 2.13. right to lodge a complaint with a supervisory authority;
 - 2.14. source of the personal data (if the personal data is not obtained from the individual it relates to);
 - 2.15. details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to); and
 - 2.16. details of the existence of automated decision-making, including profiling (if applicable).
3. Getting the right to be informed correct can help SPSO to comply with other aspects of the Data Protection Legislation and build trust with people, but getting it wrong can leave SPSO open to fines and lead to reputational damage.

Procedure

4. When we collect personal data from the individual it relates to, we must provide them with privacy information at the time we obtain their data.

5. When we obtain personal data from a source other than the individual it relates to, we need to provide the individual with privacy information:
 - 5.1. within a reasonable period of obtaining the personal data and no later than one month;
 - 5.2. if we use data to communicate with the individual, at the latest, when the first communication takes place; or
 - 5.3. if we envisage disclosure to someone else, at the latest, when you disclose the data.
6. We must actively provide this information to individuals in a way that is easy to access, read and understand. We can meet this requirement in some cases by putting the information on our website, but we must make individuals aware of it and give them an easy way to access it.
7. When collecting personal data from individuals, we do not need to provide them with any information that they already have. When obtaining personal data from other sources, we do not need to provide individuals with privacy information if:
 - 7.1. the individual already has the information;
 - 7.2. providing the information to the individual would be impossible;
 - 7.3. providing the information to the individual would involve a disproportionate effort;
 - 7.4. providing the information to the individual would render impossible or seriously impair the achievement of the objectives of the processing;
 - 7.5. we are required by law to obtain or disclose the personal data; or
 - 7.6. we are subject to an obligation of professional secrecy regulated by law that covers the personal data.
8. We must regularly review, and where necessary, update our privacy information. We must bring any new uses of an individual's personal data to their attention before we start the processing.
9. Data Subjects will generally be informed in the following ways:
 - 9.1. Staff: notice on the staff intranet; all staff updates; recruitment packs; website; orally.
 - 9.2. Complainants/applicants: notices on the website; leaflets; statements within communications; telephony system; orally.
10. Access notification forms:
 - 10.1. We sometimes, if the data we access on a complaint is likely to include special category data (ie accessing health or social care records), issue a

notification to the person whose information it is (or someone acting on their behalf) to let them know we will be seeking access to that data and giving them a clear opportunity to object. (We may provide the BUJ with a copy of this to reassure them we are processing the data fairly, however, this is not a consent form and, technically, we do not require consent to access this information.)

- 10.2. This provides a good record of the additional privacy information we provided, who we provided it to, and confirmation that the individual understands (a copy of the signed and dated form, or an online record that includes an identifier and a timestamp, or if confirmation is given orally a note of this made at the time of the conversation, including time and date, alongside a copy of the form provided or the script used).

Responsibility

11. All staff have responsibility for ensuring privacy information is provided to data subjects.

Annex 7: Appropriate Policy Document for special category and criminal offence data

1. As part of the Scottish Public Services Ombudsman's statutory and corporate functions, we process special category and criminal offence data in accordance with the requirements of Article 9 and 10 of the General Data Protection Regulation (UK GDPR) and Schedule 1 of the Data Protection Act 2018 (DPA 2018).
2. This document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018.

Conditions for processing special category and criminal offence data

3. We process special categories of personal data under the following of the UK GDPR Articles:
 - 3.1. Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the Ombudsman or the data subject in connection with employment, social security or social protection. Examples of our processing include staff sickness absences.
 - 3.2. Article 9(2)(g) – reasons of substantial public interest. The Ombudsman's powers and duties come (predominantly) from the Scottish Public Services Ombudsman Act 2002 (SPSO Act), which gives her four distinct statutory functions:
 - 3.2.1. the final stage for complaints about most devolved public services in Scotland;
 - 3.2.2. specific powers and responsibilities to publish complaints handling procedures, and monitor and support best practice in complaints handling;
 - 3.2.3. independent review service for the Scottish Welfare Fund (SWF);
 - 3.2.4. Independent National Whistleblowing Officer for the NHS in Scotland (INWO).
 - 3.3. Our processing of personal data in this context is for the purposes of substantial public interest and is necessary for the carrying out of our role. Examples of our processing include the information we seek or receive as part of investigating a complaint.
 - 3.4. Article 9(2)(j) – for archiving purposes in the public interest. The relevant purpose we rely on is Schedule 1 Part 1 paragraph 4 – archiving. An example of our processing are our findings published on our website.

- 3.5. Article 9(2)(f) – for the establishment, exercise or defence of legal claims. Examples of our processing include processing relating to any employment tribunal or other litigation.
- 3.6. Article 9(2)(a) – explicit consent. In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing. Examples of our processing include staff dietary requirements and health information we receive from our customers who require a reasonable adjustment to access our services.
- 3.7. Article 9(2)(c) – where processing is necessary to protect the vital interests of the data subject or of another natural person. An example of our processing would be using health information about a member of staff in a medical emergency.
- 4. We process criminal offence data under Article 10 of the UK GDPR. Examples of our processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations.

Description of data processed

- 5. We process special category data of our employees because it is necessary for us to fulfil our obligations under employment law. This includes information about employee health and wellbeing, ethnicity, photographs and trade union membership. Further information is available in the Staff Privacy Notice.
- 6. [Link](#) to staff privacy notice.
- 7. Our processing for reasons of substantial public interest relates to the data we obtain in order to fulfil our statutory function. This may be evidence provided to us as part of a complaint. Further information about this processing can be found in our privacy notice.
- 8. [Link](#) to privacy notice.
- 9. We permanently retain some information from our casework for archiving, research and statistical purposes. We take steps to minimise the data we keep and ensure that individuals cannot be identified once the appropriate retention period has ended.
- 10. [Link](#) to Article 30 record of processing.

Schedule 1 condition for processing

11. When processing special category and criminal offence data we ensure that at least one of the following Schedule 1 conditions is met:
 - 11.1. Paragraph 1 - employment, social security and social protection.
 - 11.2. Paragraph 4 - Research etc.
 - 11.3. Paragraph 6(1) and (2)(a) - statutory, etc. purposes.
 - 11.4. Paragraph 8 - equality of opportunity or treatment.
 - 11.5. Paragraph 10 - preventing or detecting unlawful acts.
 - 11.6. Paragraph 11 - protecting the public against dishonesty.
 - 11.7. Paragraph 12 - regulatory requirements relating to unlawful acts and dishonesty.
 - 11.8. Paragraph 24 - disclosure to elected representatives.
 - 11.9. Paragraph 30 - Protecting individual's vital interests.
 - 11.10. Paragraph 32 - Personal data in the public domain.
 - 11.11. Paragraph 33 - Legal claims.
 - 11.12. Paragraph 36 - Extension of Public Interest Conditions in Part 2.
12. [Link](#) to privacy notice.
13. [Link](#) to staff privacy notice.
14. [Link](#) to record of processing.

Procedures for ensuring compliance with the principles

Accountability principle

15. We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:
 - 15.1. the appointment of a data protection officer;
 - 15.2. taking a 'data protection by design and default' approach to our activities;
 - 15.3. maintaining documentation of our processing activities;
 - 15.4. adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors;
 - 15.5. implementing appropriate security measures in relation to the personal data we process; and
 - 15.6. carrying out data protection impact assessments for our high risk processing.
16. We regularly review our accountability measures and update or amend them when required.
17. [Link](#) to record of processing.
18. [Link](#) to data protection policy and procedures.

Principle (a): lawfulness, fairness and transparency

19. We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice, staff privacy notice and this document.
20. [Link](#) to privacy notice.
21. [Link](#) to staff privacy notice.
22. The Scottish Public Services Ombudsman has a wide remit, covering a variety of functions and services. The Ombudsman's powers and duties come (predominantly) from the Scottish Public Services Ombudsman Act 2002, which gives her four distinct statutory functions.
 - 22.1. the final stage for complaints about most devolved public services in Scotland;
 - 22.2. specific powers and responsibilities to publish complaints handling procedures, and monitor and support best practice in complaints handling;
 - 22.3. independent review service for the SWF; and
 - 22.4. INWO for the NHS in Scotland.
23. Our processing for purposes of substantial public interest is necessary for the exercise of functions conferred on the SPSO by the Scottish Public Services Ombudsman Act 2002.
24. Our processing for the purposes of employment relates to our obligations as an employer.
25. [Link](#) to record of processing.

Principle (b): purpose limitation

26. We process personal data for purposes of substantial public interest as explained above.
27. We may process personal data for any of the other specified purposes, providing the processing is necessary and proportionate to that purpose.
28. We will not process personal data for purposes incompatible with the original purpose it was collected for.
29. If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose.

- 30. [Link](#) to record of processing.
- 31. [Link](#) to privacy notice.
- 32. [Link](#) to staff privacy notice.
- 33. [Link](#) to data protection policy and procedures.

Principle (c): data minimisation

- 34. We collect personal data necessary for the relevant purposes and ensure it is not excessive. The information we process is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.
- 35. [Link](#) to data protection policy and procedures.
- 36. [Link](#) to retention and disposal policy.

Principle (d): accuracy

- 37. Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights do not apply, we will document our decision.
- 38. [Link](#) to data protection policy and procedures.

Principle (e): storage limitation

- 39. All data processed by us for the purpose of employment or substantial public interest is, unless retained longer for archiving purposes, retained for the periods set out in our retention schedule. We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. Our retention schedule is reviewed regularly and updated when necessary.
- 40. [Link](#) to retention and disposal policy.

Principle (f): integrity and confidentiality (security)

- 41. We have put in place appropriate physical, technical and procedural controls to safeguard and secure physical and electronic information.
- 42. Electronic information is processed within our secure network.

- 43. Our electronic systems and physical storage have appropriate access controls applied.
- 44. The systems we use to process personal data allow us to erase or update personal data at any point in time where appropriate.
- 45. [Link](#) to data protection policy and procedures.
- 46. [Link](#) to business plan and risk register.
- 47. [Link](#) to records management plan.

Retention and erasure policies

- 48. [Link](#) to retention and disposal policy.

APD review date

- 49. This document will be retained for the duration of our processing, and will be reviewed annually or revised more frequently if necessary.

Back to the main [Contents Page](#)

Subject Access Requests

Issued: February 2012

Contents

Introduction	3
Responsibility	3
Procedure for making request.....	3
Provision for verifying identity	4
Third party requests	4
Children	4
Charging	5
Procedure for granting access	5
Restricted information	6
Consultation	6
Repeat requests	6
Conjoined data	6
SPSO complaint files.....	7
Exemptions	7
Complaints	7
How to deal with specific types of requests.....	8
Requests for copies of documents originally sent to us.....	8
Requests for copies of medical records	8
Requests for copies of deceased person's medical records.....	8
Requests for copies of advice	8
Requests after a report is laid.....	8
Requests for Service Delivery Complaint information	9
Requests for CCTV recordings.....	9
Requests from staff	9
Further Guidance	9

Back to the main [Contents Page](#)

Introduction

1. One of the main rights which Data Protection Legislation gives to individuals is the right of access to their personal information. As a data controller, the SPSO is required to respond to Subject Access Request (SAR)'s under Data Protection Legislation.

Responsibility

2. Subject access requests are set up by the Corporate Services Team Assistant and responded to by the Information Governance Team. Other staff can process requests in consultation with the CIGO.

Procedure for making request

3. Individuals have the right to access their personal data and the information set out below (subject to certain exemptions, for example, prejudice to our statutory functions):
 - 3.1. the purpose and legal basis for the processing;
 - 3.2. the categories of personal data concerned;
 - 3.3. the recipients or categories of recipients to whom the personal data has been disclosed;
 - 3.4. the period for which the personal data is to be preserved;
 - 3.5. the existence of data subject's rights to rectification and erasure of personal data;
 - 3.6. the right to lodge a complaint with the Information Commissioner; and
 - 3.7. any information about the origin of the personal data.
4. Requests can be made verbally or in writing and do not have to refer to a subject access request, but it must be clear that the individual is asking for their own personal data. Requesters can, but do not have to, use the online contact form on our website to make a request, or email InfoRequests@sps.gov.scot. For verbal requests, and those that are not clear, we should check with the requester that we have understood their request. We keep a record of all requests on WorkPro.
3. All staff are required to pass on anything which might be a subject access request to the Information Governance Team without delay.

Provision for verifying identity

6. If we have doubts about the identity of the person making the request we can ask for more information. However, it is important that we only request information that is necessary to confirm who they are. The key to this is proportionality.
7. We need to let the individual know as soon as possible that we need more information from them to confirm their identity before responding to their request. The period for responding to the request begins when we receive the additional information.

Third party requests

8. The Data Protection Legislation does not prevent an individual making a subject access request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them. In these cases, we need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.
9. If we think an individual may not understand what information would be disclosed to a third party who has made a subject access request on their behalf, we may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.
10. There are cases where an individual does not have the mental capacity to manage their own affairs. Although there are no specific provisions in the GDPR, the Mental Capacity Act 2005 or in the Adults with Incapacity (Scotland) Act 2000 enabling a third party to exercise subject access rights on behalf of such an individual, it is reasonable to assume that an attorney with authority to manage the property and affairs of an individual will have the appropriate authority. The same applies to a person appointed to make decisions about such matters by, for example, the Sheriff Court.

Children

50. In Scotland, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown.
51. Even if a child is too young to understand the implications of subject access rights, it is still the right of the child rather than of anyone else such as a parent or guardian.

So it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

52. Before responding to a subject access request for information held about a child, we should consider whether the child is mature enough to understand their rights. If we are confident that the child can understand their rights, then we should usually respond directly to the child. We may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

Charging

53. In most cases we cannot charge a fee to comply with a subject access request. However, where the request is manifestly unfounded or excessive we may charge a 'reasonable' fee for the administrative costs of complying with the request.
54. We can also charge a reasonable fee if an individual requests further copies of their data following a request. We must base the fee on the administrative costs of providing further copies.

Procedure for granting access

55. The SPSO has one month to respond to an access request. The period may however be extended by two further months where necessary, taking into account the complexity and number of requests. Requests should be passed to the Information Governance Team straight away to log on WorkPro, acknowledge, gather information, consult with relevant parties and respond. If staff respond directly to requests, they should consult the CIGO in the first instance.
56. If an individual makes a request electronically, we should provide the information in a commonly used electronic format, unless the individual requests otherwise. We can use Objective Connect to securely share information. Hard copy responses can be issued by secure courier.
57. It is not acceptable to amend or delete the data if we would not otherwise have done so. Under the DPA, it is an offence to make any amendment with the intention of preventing its disclosure.
58. If we process a large amount of information about an individual we can ask them for more information to clarify their request. We should only ask for information that we reasonably need to find the personal data covered by the request.

59. We need to let the individual know as soon as possible that we need more information from them before responding to their request. The period for responding to the request can be suspended until we receive the additional information. However, if an individual refuses to provide any additional information, we must still endeavour to comply with their request ie by making reasonable searches for the information covered by the request.

Restricted information

60. Request case records which contain any identifiable information related to restricted information such as, for example, INWO cases and other restricted case files, or requests from members of staff, should be restricted.

Consultation

21. Relevant SPSO staff will be asked for any comments they may have about information before it is released. Where information has been provided to the SPSO by third parties, it may be appropriate to ask for any comments from those third parties before it is released, especially where sensitive personal information is concerned. This is particularly important where the release of such information without a third party's prior consent may result in an actionable breach of confidence. However, consultation should always be proportionate. The consultation letter should set out the parameters of the consultation and make it clear that it is ultimately a matter for the SPSO to decide whether the information should be released. The letter should give a date by which responses must be made, allowing time to formulate the response to the requester. In the case of medical records, comments must be obtained from the relevant health professionals as soon as possible.

Repeat requests

22. We are not obliged to comply with an identical or similar request to one we have already dealt with, unless a reasonable interval has elapsed between the first request and any subsequent ones. SPSO practice is that a minimum of 12 months should have elapsed between the first request and receipt of the second. If the requester disputes our definition of a 'reasonable interval' in respect of their request, they may complain to the ICO.

Conjoined data

23. The SPSO may withhold information if it contains personal data of another individual who can be identified from that information, unless the other individual consents, or it is reasonable not to get consent. There could, for example, be information about

others within case files, INWO records, and within requests from staff for access to their own information. Information does not have to be released unless it is reasonable to release it, taking into account the tests in Data Protection Legislation. Redaction should be considered in these circumstances. Disclosing third party personal data without a valid reason constitutes a breach of Article 8 of the European Convention of Human Rights.

SPSO complaint files

24. Information relating to on-going complaints is likely to be more sensitive than information from a closed case, but in either situation it is important to consider whether disclosure would have any adverse consequences, either for the SPSO or for other parties. Responses to such requests should always be discussed with the CIGO.

Exemptions

25. Data Protection Legislation sets out the exemptions which may be used to withhold information from data subjects. Some exemptions to the subject access provisions include:
 - 25.1. confidential references given by the data controller;
 - 25.2. information relating to negotiations with the data subject;
 - 25.3. legal professional privilege – where confidentiality of information between client and professional legal adviser could be maintained in legal proceedings;
 - 25.4. prejudice discharge of functions;
 - 25.5. serious harm;
 - 25.6. protection of the rights of others; and
 - 25.7. self-incrimination.

Complaints

26. Individuals have a right to complain to the ICO if they consider the SPSO has not complied with Data Protection Legislation. They can first complain to us if they are concerned about how we are handling their personal data. This includes if we have not properly responded to their SAR.
27. If an individual thinks personal information is missing from the response to their SAR, we should ask them to clearly list what other information they think we also have. This will help us review our records.

28. If an individual is unhappy with our response to any data protection problems they have raised, they can ask for a review from the HoCSS.
29. In case of a complaint to the ICO, it is SPSO practice to retain all relevant information on Workpro for at least a further six months.
30. See also (link to [Data protection complaints](#) section)

How to deal with specific types of requests

Requests for copies of documents originally sent to us

31. If complainants send us original documents, we will normally take copies for our records and return the originals as a matter of course. Any request for return of their own information they provided should be handled the same way, we do not need to handle this as a formal SAR request although we should try to respond within 20 working days, to avoid any appeal to either Information Commissioner.

Requests for copies of medical records

32. We need to write to the body concerned and ask if they see any reason for not releasing the documents, and if the person making the request is not the subject of the records, we need to seek separate authorisation from the data subject for the request to be made on their behalf.

Requests for copies of deceased person's medical records

33. We may receive requests for access to a deceased person's records, quoting the [Access to Health Records Act 1990](#). The SPSO is not a 'holder' in terms of the Act, and requesters do not have the right to access medical records held by the SPSO, even if the requester is the next of kin of a deceased patient. We should not release any medical records for deceased persons but should instead refer the enquirer to the relevant health board. We have obtained legal advice on this matter.

Requests for copies of advice

34. We will often release copies of the advice we receive from the advisers when requested, minus the name of the adviser. This should always be referred to the Information Governance Team in the first instance.

Requests after a report is laid

35. Normally, the publication of a report signifies the end of any debate we can enter into about the complaint. However, complainants are still entitled to request information following the report. If we receive correspondence which may be a request for

information, staff should refer to the Corporate Information Governance Officer for advice. Generally there will be a difference between a request for information (for example, question starting who, when, what, where) and a question about our handling of the complaint (for example, a question starting how or why) however it will not always be as clear-cut as this.

Requests for Service Delivery Complaint information

36. Service Delivery Complaints are a separate process to handling complaints about authorities within our jurisdiction. Where staff have commented on the representations made against them, we maintain that the free and uninhibited provision of information by the staff member is an essential part of investigating this kind of complaint, and that the member of staff concerned should be entitled to a degree of confidentiality. We reserve the right to withhold this kind of information from the complainant. This exemption has been applied in a previous case, ICO reference RFA0141301. At that time the Commissioner agreed that the exemption was applied correctly.

Requests for CCTV recordings

37. SARs involving cctv footage should be passed to Information Governance as normal. The building co-ordinator should be asked to identify whether we hold relevant footage and whether or not the footage includes any potentially identifiable third parties. We may then need to consider limiting what we disclose, or contacting the third parties if appropriate before making a decision.

Requests from staff

21. It will most likely be appropriate for requests from staff for access to their own information to be dealt with by HR, or if for example relating to whistleblowing concerns, by an appropriate manager, confidential contact, or HoISE. Support can be sought from the CIGO. Depending on the circumstances information may need to be recorded either in a restricted WorkPro request record, or in the appropriate restricted folder in eRDM (an anonymous WorkPro request record can be created for admin purposes only).

Further Guidance

22. Further detailed guidance on subject access requests is on the ICO website at <https://ico.org.uk/>.

Data Protection Impact assessments: process and supplementary guidance

Issued: March 2019

Contents

- Our policy2**
- Do we need a DPIA?2**
- Conducting a DPIA3**
 - Drafting a DPIA3
 - Obtaining approval3
- Concluding the process4**
- Privacy notices and Asset registers4**
- Version control4**

Back to the main [Contents Page](#)

Our policy

1. Our data protection policy explains that we must carry out DPIAs in some circumstances and that it is good practice to do so whenever we are making changes to the way we process data.

Do we need a DPIA?

2. If your project / new process / process change:
 - 2.1. could change how we use/access/store/move personal data;
 - 2.2. would lead to us contacting people in a new way;
 - 2.3. would lead to people or organisations sharing information with us in a new way; and/or
 - 2.4. requires you to obtain new personal data or to process personal data we hold as part of the project/process.
3. You should consider conducting a DPIA.
4. We may also consider carrying out a DPIA:
 - 4.1. following a data incident or near-miss;
 - 4.2. when we identify or became aware of a risk; and
 - 4.3. whenever we consider it is appropriate to review our existing processes.
5. Before conducting a DPIA you should first complete a screening questionnaire to ensure you have identified whether one is needed and the scope of the DPIA. Templates for screening questionnaires can be found [here](#).
6. You can seek the advice support of IGO/LPO when completing the questionnaire but the questions at this stage are fairly straightforward and should not require much technical Data protection knowledge.
7. Once complete, the draft screening questionnaire and any other relevant project documents should be sent to the LT for approval via your LT sponsor.
8. Once LT have signed-off the draft screening questionnaire, this will go to the DPO who will comment.
9. The comments will then be shared with LT for a final decision.
10. This process will either:
 - 10.1. confirm we do not need to conduct a DPIA but evidence that we have properly considered this or

10.2. confirm we need to conduct a DPIA.

11. Once approved the final Screening questionnaire should be stored in the DPIA folder.
(see below for additional notes on version control.

Conducting a DPIA

12. We have a DPIA template which is available [here](#).

Drafting a DPIA

13. The first part of the process is evidence gathering and you should consider at an early stage whether you need to consult stakeholders or not. It will not always be necessary to do so and the critical factors are likely to be:
- 13.1. impact, is it likely to have significant impact;
 - 13.2. scope, how many people or other processes would it impact;
 - 13.3. whether there are options (if there is a statutory requirement we could consult on implementation but not on the requirement); and
 - 13.4. proportionality (a minor change may require a DPIA but may not require a full consultation).
14. The DPIA form will guide you through the questions and includes reference to some of the legal tests. At any stage in the DPIA process you can seek advice from the IGO/LPO. There is also significant additional advice available on the ICO website and the DPO can provide ad-hoc support.

Obtaining approval

15. Generally, a DPIA will need to be approved before you start the project or make any changes to our systems/methods/processing of persona data.
16. The process for approval is:
- 16.1. draft DPIA is shared with LT for comments / approval to proceed;
 - 16.2. draft DPIA is shared with DPO for comments; and
 - 16.3. DPIA with DPO comments is shared with LT for sign off.
17. DPIAs can be signed off at weekly LT meetings. They will be reported in the Data Protection paper at quarterly governance meetings.
18. Once signed off a copy of the DPIA should be stored in the DPIA folder with the naming convention: yymmdd ProjectName DPIA Start

19. Changes may also need to be made to the assessment as the project progresses. A working or live DPIA should be kept in the project folder to allow for this. Minor changes can be made by the project lead and approved retrospectively through the end of project formal DPIA sign-off process. Major changes will need to go through the approval process above.

Concluding the process

20. Once the project is complete. You should review and finalise the working/live DPIA noting any minor changes that occurred during the process.
21. The final DPIA should go through the same process at paragraph 13. The permanent record for the DPIA is yymmdd NameOfProject DPIA Final. It is the project manager's (or owner's) responsibility to ensure that the final DPIA at the end of the project to save the document.

Privacy notices and Asset registers

22. We need to ensure our privacy notice and asset registers are up to date. If the DPIA identifies that these may need changed that should be highlighted to the IGO as soon as possible and before any new personal data is obtained or changes made to how we process data.

Version control

23. It is important that we keep an auditable track of the changes and, in particular of DPO comments. Objective version control will be sufficient and should be used in the following way:
 - 23.1. minor changes should be saved as a .1 .2 etc version; and
 - 23.2. documents which have LT approval or where the DPO has commented should be saved as major versions. The version box at the top of the document should be completed with comments when you move to a major version.

Back to the main [Contents Page](#)

Protocol for data security incidents

Issued: May 2019

Contents

Personal data breach.....	2
Breach management.....	2
Process.....	2
Breach examples	4
Further guidance	5

Back to the main [Contents Page](#)

Personal data breach

1. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The Information Commissioner's office (ICO) broadly defines a personal data breach as '... a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the personal data or passes it on without proper authorisation; or if the personal data is made unavailable and this unavailability has a significant negative effect on individuals'.

Breach management

2. We must ensure we have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not we need to notify the ICO and the affected individuals. We need a strategy for dealing with the breach, including:
 - 2.1. a recovery plan, including damage limitation;
 - 2.2. assessing the likely risks to individuals as a result of the breach;
 - 2.3. informing the appropriate people and organisations that the breach has occurred; and
 - 2.4. reviewing our response and updating our information security.
3. All staff have a responsibility for reporting personal data security incidents, including any breaches of confidentiality. Staff must escalate incidents to their line manager and the Corporate Information Governance Officer (CIGO) immediately to determine whether a personal data breach has occurred. On becoming aware of a data security incident it is essential that it is managed effectively. The CIGO will coordinate and ensure all the appropriate investigation and reporting processes are undertaken, and will liaise with the Data Protection Officer (DPO) as appropriate.

Process

4. In the event of a personal data breach it is important to deal with the breach effectively. The breach may arise from a theft, a deliberate attack on our systems, the unauthorised use of personal data by a member of staff, accidental loss, or equipment failure. We must respond to and manage the incident appropriately. The following actions must be taken:

- 4.1. the staff member should report the incident to their line manager and the CIGO within 24 hours or as soon as is practicably possible thereafter by filling out a copy of the incident log with the available details;
- 4.2. the CIGO, or, in their absence, the relevant manager, should log the incident [in WorkPro](#) and is responsible for updating the incident log and recording all the actions taken to investigate and conclude the matter;
- 4.3. we should quickly establish whether a personal data breach has occurred, contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen;
- 4.4. the HoCSS should be informed as soon as possible of the incident and the action being taken, and must approve any decision to notify with the ICO;
- 4.5. where appropriate the DPO should be informed as soon as possible of the incident and the action being taken, and should provide advice on actions, including whether we should notify;
- 4.6. the Ombudsman should be informed as soon as possible of the incident.
- 4.7. Data Protection legislation places a duty on the SPSO to report certain types of personal data breach to the ICO. Not all breaches need to be reported. If there is a likely risk to the rights and freedoms of individuals we must report to the ICO. We must do this within 72 hours of becoming aware of the breach. The ICO website has information about reporting a breach [here](#). This can be done by telephone or online. We should use their [self-assessment](#) tool to help determine if we need to report a breach. If we are unsure, we should call them for advice. All actions should be documented.' Our registration and security numbers can be found [here](#).
- 4.8. if the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform those individuals without undue delay advising steps we are taking to mitigate effects and advice on protecting themselves and who to contact if they have concerns. Our [Information Rights leaflet](#) can be provided, which gives details about pursuing any data protection concerns;
- 4.9. the HoCSS should be informed once closed/escalated to update the Leadership Team;

- 4.10. we must keep a record of any personal data breaches, regardless of whether we are required to notify. There is a WorkPro report detailing personal data security incidents.
- 4.11. Data processors must also inform us without delay if they suffer a breach to allow us to take steps to address the breach and meet our breach reporting requirements. And if any other third parties suffer a breach affecting information related to SPSO, we may still need to consider if there are any steps we can take, for example, to aid with the assessment of risk, to mitigate any potential risk to SPSO/staff/users, or simply to signpost people etc.

Breach examples

- 5. Some examples of incidents are where personal data has been disclosed in error by mail / email, where a file / mail / electronic device goes missing or is stolen, unauthorised access or alteration, or loss of availability of personal data. Some examples of personal data that could trigger a personal data security incident are data held on complaint / review / HR files, with health / social work / gender transition / criminal offence data posing a higher risk.
- 6. Personal data breaches must be contained and data recovered as quickly as possible. Below are some of the recovery steps that will need to be taken in specific instances:
 - 6.1. Personal data disclosed in error – the personal data should be retrieved as soon as possible and confirmation of deletion sought for any electronic data, as well as confirmation the information has/will not be further shared. (If the initial error was caused by use of cc instead of bcc in an email, take care to bcc recipients to advise of the error, apologise and advise on what steps those affected can take to mitigate further risks to themselves). Take care not to repeat the breach when doing this.
 - 6.2. Missing case files – the person named as the file location must confirm they have searched in the first instance, before their entire team is asked to stop what they are doing to search, and then the whole office must search.
 - 6.3. Missing mail – the person the mail is meant for (and where appropriate the person that logged the mail) must confirm searches in the first instance, before their entire team is asked to stop what they are doing to search, and then the whole office must search.
 - 6.4. Theft – notify the police immediately, making sure you get an incident number and the name of the officer you spoke to.

- 6.5. Cyber incident – see also separate cyber incident reporting policy. We also have a cyber incident response plan in place to ensure we can respond effectively to cyber incidents.

Further guidance

7. Important guidance on personal data breach management and reporting breaches is available on the ICO website [here](#). There are also [bulletins](#) and additional breach training available for staff.

Back to the main [Contents Page](#)

SPSO Covert recording policy

Issued: February 2021

Contents

Requests to record and covert recording.....	2
What do we mean by covert recording?	2
Can we use covert recordings in our work?.....	2
What should I do if someone asks to record me?.....	2
What should I do if a covert recording is made of SPSO staff?	4
Processing and using covert recordings	4
Step 1: identifying the purpose and lawful basis for processing	5
Step 2: identifying and assessing the rights of individuals.....	6
Keep a record of the decision.....	7
Using a covert recording as evidence	7

Back to the main [Contents Page](#)

Requests to record and covert recording

What do we mean by covert recording?

1. For the purposes of this policy we mean any recording when one of the persons recorded was unaware that they were being recorded. The recording may be video or audio or both and the person who is unaware does not need to be a fully active participant but could be a bystander or an incidental participant.
2. Unaware does not include situations where there was appropriate information given that recording was ongoing but the person had not appreciated or noticed this (for example someone saying they were unaware there was CCTV recording in a public place because they had not noticed the signs).
3. There may be situations where a person was informed they were being recorded but felt they could not safely or voluntarily leave the situation and objects to the recording being used because of this. In these circumstances, the approach set out in this policy can still be used to help ensure we take their rights into account when deciding whether or not to listen to or view the recording.

Can we use covert recordings in our work?

4. Yes. Unlike a court, there are no rules about the evidence we can or cannot use. This applies to all of our statutory functions. But as an organisation we need to take into account:
 - 4.1. data protection law;
 - 4.2. the human right to privacy; and
 - 4.3. natural justice and fairness.

when deciding whether and how to process and use the information.

5. This policy looks at specific issues raised by covert recordings but should be read alongside the information governance handbook and guidance for our individual statutory functions which also help support compliance with relevant legislation and case law. If you have any concerns or uncertainty about a specific situation you can seek advice from colleagues or your line manager about how to proceed.

What should I do if someone asks to record me?

6. Generally, as an office, we are happy for a user of our services to take an audio recording of a professional interaction with our staff for their own personal use. And we would prefer that recording is being done overtly. We may record calls and our call recording policy sets out how that process is managed.

7. In some cases, a recording may be a reasonable adjustment and that means not only that we should allow recording but we should take responsibility for ensuring that it occurs. We have access to call recording to allow for this to be easily undertaken.
8. However, there are other reasons why someone may wish to record an interaction that we consider to be reasonable. This could be so they can review the interaction later or to share with a person they are representing or wish to seek advice from that cannot be present. It may also be because they have little trust in public organisations and making a recording can help them to feel more secure.
9. Video recording is more intrusive for staff and can make them self-conscious, it is also more concerning if misused because it increases the risk of identification. We would normally refuse requests to video record a meeting for personal use unless it is required as a reasonable adjustment.
10. In line with our normal policy, a member of staff can end an interaction at any time and our engagement policy provides more detailed advice on what to do if recording is being used as a threat or someone is threatening to live stream a call or to make it publicly available at a later date.
11. We also appreciate that there may be situations or circumstances when staff are more vulnerable to the misuse of recordings or personal information. Risk will be assessed on an individual basis but this could include a colleague who has been subjected to stalking or harassment or who is responsible for the care of a vulnerable child or adult. Line managers can agree that individual staff can limit their interaction or pass on to colleagues if being recorded would cause them undue distress or concern or increase risk to them personally even in circumstances we consider it is generally appropriate to allow an overt recording.
12. Care should be taken to ensure, where possible, third parties are not recorded. If you are in a situation where this is likely or possible (for example, a public reception) you should aim to move the interaction to a less public space where third parties would not be recorded. If it is not safe to do so or it is not possible, you should let the person who is asking to record you that you will let third parties who enter the space know that recording is occurring.
13. There are some spaces where it is not appropriate to agree to recording because it is accessible to third parties who may be vulnerable or have a reasonable expectation that they are in a space where information they may be sharing or the fact of their presence in that space would be treated confidentially. We may refuse to allow an overt recording for personal recording in such circumstances.

14. Note: We have call recording facilities and if the recording is being made as a reasonable adjustment you should offer to set up a call that we record so we can guarantee they have a clear and full record.

What should I do if a covert recording is made of SPSO staff?

15. A covert recording of yourself or colleagues may be produced as evidence or offered to us as evidence as part of a request that we should change a decision or as part of a customer service complaint.
16. The decision whether or not to listen to or use the covert recording should be made in line with this policy which sets out what purposes it is appropriate to use the recording for and how to balance the rights of individuals when doing so including SPSO staff.
17. Although we support overt recordings for appropriate, professional reasons, individuals can feel very uncomfortable and may experience feelings of distress or fear when they became aware that they have been recorded covertly. We should ensure that we provide support and understanding and can signpost colleagues to additional support, such as the employee assistance programme, if required.

Processing and using covert recordings

18. If someone shares or offers to share a covert recording as evidence for any of our statutory functions or to raise an issue about a decision we have made or the service we have provided to them, we need to decide whether to process that recording. Maintaining the recording in our system, even if we do not listen to that recording, will count as processing.
19. Data protection legislation applies to all processing and means we should only process personal data if we can demonstrate compliance with the Data Protection principles. These say personal data should be:
 - 19.1. fairly and lawfully processed in a transparent manner;
 - 19.2. processed for limited purposes;
 - 19.3. adequate, relevant and not excessive;
 - 19.4. accurate and up to date;
 - 19.5. not kept for longer than is necessary;
 - 19.6. secure, and
 - 19.7. the controller must be responsible for, and be able to demonstrate, compliance with the principles.

Step 1: identifying the purpose and lawful basis for processing

20. You should first identify the purpose or use we intend to make of the recording.
21. We set out in our policies and related privacy notices the purposes for which we may use evidence we obtain in our statutory functions or about our staff as part of our work and they are quite broad.
22. When we have been sent or are being offered a covert recording we should remember that it was obtained in circumstances that were not transparent and this means we should, unless there is a good reason to do so, restrict the purposes we use the recording for and only use them when it is necessary to meet those purposes.
23. We consider there will be individual cases where it may be necessary and proportionate to use a covert recording for the following purposes:
 - 23.1. helping to assess customer service complaints;
 - 23.2. protecting staff and others from harassment or abuse;
 - 23.3. providing evidence of misconduct, criminal or safeguarding issues; and
 - 23.4. direct evidence as part of our handling of a complaint (public service or INWO) or welfare fund review.
24. Our information sharing policy sets out when we may share information under section 19 and section 20 of the SPSO Act and this applies to any covert recording that may have been shared with us but we should bear in mind the context within which it was obtained when making decisions in line with that policy.
25. Our data processing register sets out the detail of the lawful bases we rely on and for these purposes we refer to:
 - 25.1. performing a task in the public interest (relating to our statutory functions);
 - 25.2. legitimate interest
 - 25.3. and when the information contains special category data;
 - 25.4. protection of vital interests; and
 - 25.5. substantial public interest.
26. Whenever we are considering processing special category data we should remember the lawful bases are 'substantial public interest and' 'vital interests require protection'. These are high standards and that should inform decisions whether and how to process information. Information relating to criminal convictions is covered by rules similar to special category data and it is good practice to treat any sensitive data with the same level of care as special category data.

Step 2: identifying and assessing the rights of individuals

27. Once we have identified the purpose and use we want to make of the recording, we need to make sure we identify and assess the rights of all individuals affected.
28. The best way to do this is to ask those who were covertly recorded if they have any particular concerns about our using the recording. When doing so we should:
 - 28.1. explain why and how we intend to use the recording.
 - 28.2. provide reassurance that we will share the recording with them for comment about whether it is a true or accurate reflection of the conversation they had before making any decisions based on the recording; and
 - 28.3. confirm we will keep it secure; and will limit who will listen to the recording to only those who need to do so to meet the purpose we have identified.
29. It is appropriate and may be necessary to listen to the recording before seeking views:
 - 29.1. in order to identify individuals,
 - 29.2. to ensure it is a relevant recording and that it is possible to access the recording; and
 - 29.3. there is sufficient quality of recording for it to be potentially useful but care should be taken to do so in a private space and to take only limited notes.
30. If listening to the recording reveals that there is a need to share information obtained from the recording or even the recording itself urgently because there is a risk to health or safety then we should use the process in our information sharing policy.

When it is not possible to obtain views

31. Restrictions in our legislation (the need to investigate in private and keep certain information confidential); or practical matters (we do not have and cannot easily obtain contact details or even identify some people who have been recorded); may limit our ability to ask individuals for their views.
32. In such situations we should proceed with care and seek to ensure we have considered what their views may be by asking, for example:
 - 32.1. Is this an incidental recording in a public space?
 - 32.2. Does it reveal their identity or special category data?
 - 32.3. Were they in a space where privacy would have been expected?

Assessing and balancing rights

33. This should be done on a case by case basis but the following is a general guide to questions that could form part of the assessment.
 - 33.1. How significant is the use or purpose we have identified.
 - 33.2. Is the recording about a significant or trivial matter?
 - 33.3. Is it necessary to process the recording to meet the purpose -- is alternative evidence available?
 - 33.4. Does the recording contain any special category data?
 - 33.5. Is the person speaking in a professional capacity?
34. When making the assessment we should bear in mind that a person acting in a professional capacity, while not anticipating the covert recording, would have less of an expectation of privacy. That may shift if the recording reveals or contains information about their private or family life or contains any special category information about them.

Keep a record of the decision

35. It is important to record and document decisions. The record should include:
 - 35.1. why we consider it proportionate and necessary to use the recording to meet the purpose; and
 - 35.2. factors we have taken into account when balancing rights of individuals covertly recorded.

Using a covert recording as evidence

36. Making a decision in relation to one of our statutory functions or whether or not to uphold a customer service complaint are separate from the decision that we can use the recording.
37. It is important to maintain that separation. Deciding to use a recording does not mean we are committing to accepting the evidence as definitive, credible or reliable. Decisions still require to be made about:
 - 37.1. the relative weight to be put on the evidence, and
 - 37.2. how it should be balanced against other evidence.
38. Asking for the views of key actors in the recording to comment helps to establish whether or not the recording is a true reflection of the full conversation. Where that is not possible, it may be difficult to establish whether or not the recording has been cut or edited and that may limit the weight we can put on the evidence. Such decisions do though need to be made on a case by case basis and in line with our normal approach to weighing and using evidence in decision-making.

Back to the main [Contents Page](#)

Digital recording policy

Issued:

Contents

Policy statement Error! Bookmark not defined.

Purpose Error! Bookmark not defined.

Scope Error! Bookmark not defined.

Roles and responsibilities Error! Bookmark not defined.

General policy Error! Bookmark not defined.

 Annex 1: Rapid data protection impact assessment template ...**Error! Bookmark not defined.**

 Annex 2: Risk Assessment Matrix **Error! Bookmark not defined.**

Back to the main [Contents Page](#)

Policy statement

1. All employees, suppliers, contractors, agents and representatives, volunteers and temporary staff working for or on behalf of the SPSO, have a duty to be compliant with legislation in relation to information management. This legislation includes, and is not limited to:
 - 1.1. the UK GDPR;
 - 1.2. the Data Protection Act 2018;
 - 1.3. Environmental Information (Scotland) Regulations 2004 (EIR);
 - 1.4. the Freedom of Information (Scotland) Act 2002 (FOISA);
 - 1.5. the Public Records (Scotland) Act 2011; and
 - 1.6. the Computer Misuse Act 1990.
2. All staff have a responsibility to be compliant with the law to reduce the risk to the SPSO's reputation and subsequent monetary fines. The SPSO has established and maintains policies and procedures to ensure compliance with Data Protection, Freedom of Information, Environmental Information and Human Rights legislation in relation to Information Management.
3. The recording of online meetings and events raises a number of legal implications for the SPSO and these must be fully considered before creating a digital record.
4. These include:
 - 4.1. The capturing of participants' identities, voices, home, and family circumstances as part of a digital record and stored within SPSO systems.
 - 4.2. Digital Recordings will be held by the SPSO and can be requested under FOISA, EIR and Data Protection legislation, as well as in civil actions, judicial reviews, or inquiries.
 - 4.3. The SPSO does not possess the technology or provide the services or expertise to search video footage in response to these requests and redact sensitive material.
 - 4.4. Many of these Web-based products are hosted in the USA, which does not offer the same protections to personal data as the UK and is likely to require a [Data Transfer Risk Assessment](#) before implementing the product.
5. All employees, suppliers, contractors, agents and representatives, volunteers and temporary staff working for or on behalf of the SPSO must take into consideration and adhere to the following policies in addition to this policy, when deciding to create a digital recording:

- 5.1. [IT Security Policy and Code of Conduct](#);
- 5.2. [Information Governance and Data Protection Policies and Procedures](#); and
- 5.3. [Conduct and Behaviour](#).

Purpose

- 6. The purpose of this policy is to protect SPSO's digital recordings from all threats, whether internal or external, deliberate, or accidental to ensure business continuity, minimise the risk of reputational damage, monetary penalties and protect data.
- 7. Recording tools are available to all staff across a range of products, however, it is recommended, where possible, that digital recordings are created using the SCOTS Connect instance⁹ of MS Teams. This instance of MS Teams has been secured to the necessary standards and is approved for use up to Official Sensitive level. A [Data Protection Impact Assessment](#) and an Equality Impact Assessment have been completed centrally for the SCOTS Connect MS Teams. These assessments can also be made available upon request to ITECS.
- 8. It should be noted that technical support is not provided for the use of any other digital recording tools.

Scope

- 9. This policy applies to all employees, suppliers, contractors, agents and representatives, volunteers and temporary staff working for or on behalf of the SPSO using any physical or virtual digital recording technology.
- 10. This policy applies to the creation and management of all digital recordings by business areas in their day-to-day operations.
- 11. This policy does not cover the situations where there may be digital recording provisions in other SPSO Corporate policies, for example instigated by HR in relation to the discipline and / or grievance policy.

Roles and responsibilities

- 12. All staff: are expected to be aware of and adhere to this policy and accompanying guidance and are responsible for the creation and management of digital recordings as defined by this policy.

⁹ Created using your SCOTS MS Teams account

13. Managers: are responsible for ensuring staff, including contract staff, are aware of, and supported to follow, the practices defined in this policy.
14. Heads of: have overall responsibility for the management of information assets within their business area. This includes authorising the creation of digital recordings and these are managed in line with this policy.
15. Head of Corporate and Shared Services: is the Senior Responsible Officer with overall strategic accountability for information risk across the SPSO.
16. CIGO: has day-to-day operational responsibility for data protection and information governance within the SPSO.
17. DPO: assists us to monitor internal compliance with data protection legislation.
18. SPSO (Ombudsman): has overall responsibility for having controls in place and ensuring information risks are managed.
19. SPSO ICT support: ISA and ICT Champions are responsible for offering ICT support to staff and liaising with iTECS.
20. iTECS: iTECS staff are responsible for maintaining the SCOTS CONNECT feature of O365 and offering technical support to staff.

General policy

21. Digital recording within business areas is permissible only where there is a legitimate business need to do so and recording falls within the guidelines below. SPSO policy is that any information created or managed in Microsoft Teams or Office 365 that is a record should be transferred to eRDM or our bespoke case management system (CMS). As digital recordings cannot be transferred and stored within eRDM or the CMS, there will be a requirement for an official record to be created. This must be completed within a limited period of time and the digital recording deleted.
22. The management of recordings is the responsibility of the meeting organiser as well as any user who records the meeting as a participant and the following must be met when making the decision to create a digital recording:
 - 22.1. the digital recording is created for [a defined and specific purpose](#) which cannot be met by other less intrusive methods;
 - 22.2. digital recordings must not be created by staff for HR or management purposes for example to make a record of 1-2-1's, performance reviews, line manager meetings etc.;

- 22.3. At least one [lawful basis](#) for creating the digital recording has been identified under data protection legislation;
- 22.4. Where the lawful basis is [consent](#), participants are asked to consent to being recorded and are given the option to opt out. Participants must actively consent by speaking or adding a note. Assumed consent is not acceptable;
- 22.5. All participants must be made aware in advance that the event/meeting will be recorded and provided with the [necessary information required under Data Protection legislation](#);
- 22.6. the rapid Data Protection Impact Assessment (annex A) must be completed for instances where the SCOTS Connect MS Teams platform is being used or If opting for another product, a full [Data Protection Impact Assessment](#);
- 22.7. the rapid or full version of the Data Protection Impact Assessment MUST BE signed off PRIOR to the event/meeting;
- 22.8. the digital recording is kept secure, with appropriate organisational and technical measures assigned to the digital recording;
- 22.9. there are processes in place to actively manage the digital recording including ensuring it is used in line with what participants were informed and can be produced in response to [access requests](#) under legislation;
- 22.10. when appropriate, there is a process in place to create an official record for transfer to eRDM or the CMS;
- 22.11. when sharing digital recordings, the key principles in data protection legislation are followed including identifying a lawful basis that enables the recording to be shared, and the data sharing is in line with what participants were informed;
- 22.12. The SPSO must own [the copyright](#) of or have permission to upload and share any digital recording; and
- 22.13. failure to record in accordance with the [IT code of conduct](#) – including covert recording may lead to disciplinary action being taken.

Back to the main [Contents Page](#)

Annex 1: Rapid data protection impact assessment template

To be completed for creating a digital recording on the SCOTS Connect M365 only

Part 1: Assessment against the data protection principles

1.	What is the purpose and objective for recording the meeting?	
2.	Why is it necessary to record the meeting? (Is this proportionate - could less privacy intrusive means achieve the objective?)	
3.	What is the lawful basis under Data Protection? If relying on consent, how will this be recorded? If applicable, please provide a link or copy of the legitimate interest assessment (LIA)	
5.	Where will the recording be stored and/or hosted? Is this location appropriately secure?	
6.	What is the retention period for the recording?	
7.	Will the recording be shared with any organisation outside of the SPSO? List these organisations if applicable.	
8.	How will information requests (FOI & SAR) be managed and facilitated? How will recordings be edited/redacted?	

Part 2: Risk assessment table

Risk	Likelihood of harm	Severity of harm	Risk Score	Mitigation	Effect on risk	Mitigated Risk Score
Describe the source and potential impact on individuals	<div><div></div> Remote</div> <div><div></div> Unlikely</div> <div><div></div> Possible</div> <div><div></div> Likely</div> <div><div></div> Almost certain</div>	<div><div></div> Negligible</div> <div><div></div> Minor</div> <div><div></div> Moderate</div> <div><div></div> Major</div> <div><div></div> Extreme</div>	<div><div></div> Very low</div> <div><div></div> Low</div> <div><div></div> Moderate</div> <div><div></div> High</div>	Identify additional measures that you can take to reduce or eliminate medium to high risks	Eliminated Reduced Accepted	<div><div></div> Very low</div> <div><div></div> Low</div> <div><div></div> Moderate</div> <div><div></div> High</div>

Part 3: Leadership team approval

The DPIA report should be approved by the Leadership Team.

Before approving the DPIA report, the LT should ensure that they are satisfied that the impact assessment is robust; has addressed and documented all the relevant risks and issues; and that appropriate actions have been taken.

By approving the DPIA, the LT is confirming that the impact of the recording has been sufficiently assessed against the individuals' right to privacy.

Approved by	[link to LT meeting where this DPIA was approved]
Date	

Annex 2: Risk Assessment Matrix

Risk assessment matrix

Likelihood	Severity of impact				
	Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
Almost certain (5)	LR (5)	MR (10)	HR (15)	HR (20)	HR (25)
Likely (4)	LR (4)	MR (8)	MR (12)	HR (16)	HR (20)
Possible (3)	VLR (3)	LR (6)	MR (9)	MR (12)	HR (15)
Unlikely (2)	VLR (2)	LR (4)	LR (6)	MR (8)	MR (10)
Remote (1)	VLR (1)	VLR (2)	VLR (3)	LR (4)	LR (5)

	HR = High risk
	MR = Moderate risk
	LR = Low risk
	VLR = Very low risk

Likelihood of occurrence definitions

	Remote 1	Unlikely 2	Possible 3	Likely 4	Almost certain 5
Likelihood	Cannot believe this would happen – will only happen in exceptional circumstances (5-10 years)	Not expected to happen but definite potential exists (2-5 years)	May occur occasionally, has happened before on occasions – reasonable chance of occurring (annually)	Strong possibility that this could occur – likely to occur (quarterly)	This is expected to occur frequently, in most circumstances – more likely to occur than not (daily / weekly / monthly)

Back to the main [Contents Page](#)

Call recording policy

First Issued: Nov 22 (Feb 23) (Oct 23)

Contents

Overview.....	2
Why we record calls	2
Recording, accessing and retaining calls	3
Recording	3
Accessing calls	6
Downloading and Retaining calls	6
Audit	6
How calls are recorded.....	7
What is recorded.....	8
Informing people calls are being recorded.....	9
How we access calls and keep them safe	10
How long we keep calls.....	10
How we handle information rights requests	11
SAR requests	12
Other Information requests.....	13
Using the system when not in Bridgeside House.....	13

Back to the main [Contents Page](#)

Overview

1. This policy covers:
 - 1.1. why we record calls;
 - 1.2. how calls are recorded;
 - 1.3. how we let people know we are recording calls;
 - 1.4. how we access calls and keep them secure;
 - 1.5. how long we will keep calls; and
 - 1.6. how we deal with information rights requests.
2. Recordings constitute the personal data of both the caller and the SPSO staff member, and any third party mentioned during the call. Therefore, they will be managed in such a way that the rights of all data subjects can be met, and all the obligations of the data controller (SPSO) are observed. The policy and our internal processes which support them are subject to both a DPIA and an EQHRIA which ensure we take a rights-based approach to its creation and implementation. They should be reviewed if any changes are proposed to the policy or supporting processes.

Why we record calls

3. Recording calls can have a number of benefits, it allows for calls to be reviewed for customer service purposes including quality assurance and dealing with complaints about our service, it can help to protect staff from abuse and allow us to share information with the police if threats are made or with other agencies if we identify someone is at risk. It can help us to accurately record long or complicated conversations. It can allow us to keep a record of evidence or important conversations. Fundamentally, recording calls can help SPSO to meet our statutory purposes.
4. The SPSO have identified it would be appropriate to record, access and, in some cases, retain calls for the following purposes:
 - 4.1. review a complex / significant call to improve a written note or as the main record of a call when a written note would not be adequate or too resource-intensive to note;
 - 4.2. establishing the facts and helping to assess customer service complaints;
 - 4.3. protecting staff and others from harassment in the form of abusive/ nuisance calls or threats;
 - 4.4. providing evidence of criminal or safeguarding issues;

- 4.5. quality and training purposes;
 - 4.6. obtaining direct evidence as part of an investigation or Welfare Fund review;
 - 4.7. retaining evidence of the following when they are provided orally during a call:
 - 4.7.1. consent, for example, for representation;
 - 4.7.2. evidence that is necessary to resolve an investigation or welfare fund review; and
 - 4.7.3. a complaint about our service; and
 - 4.8. to make a reasonable adjustment.
5. While the SPSO may record calls, nothing in this policy requires calls to be recorded. Call recording has resource implications and there is also a need to ensure that the rights of those being recorded are respected.
6. The LT may, therefore, decide to suspend all call recording, change which lines are recorded or suspend call recording for calls from an identified individual or organisation. Such decisions will be clearly documented and communicated to relevant staff.

Recording, accessing and retaining calls

7. We need to demonstrate that we are making appropriate decisions in line with this policy and relevant data protection obligations when we are:
- 7.1. Recording;
 - 7.2. Accessing; and
 - 7.3. retaining calls.
8. Calls should be processed to the minimum extent we need to meet the purpose identified. For example, an individual member of staff may be able to access a call to take improved notes, the call would not need to be downloaded or retained beyond the 90 day period. This means that we need to document the decisions to record calls, download and/or retain separately from the decision to access.

Recording

9. The system we use for recording calls is provided through our telephony provider. The system meets the requirements for security of such data but we remain responsible for ensuring appropriate management, GDPR compliance, audit and security for any recordings downloaded.

10. The system allows us to designate different levels of recording for different users. Decisions about which level of recording should be in place for each user will be based on ensuring we record calls of staff who are most likely to receive a high volume of calls which meet the purposes set out above. The Leadership Team will make the decisions about which users should or should not be recorded and to what level. This policy sets out the general approach but the Leadership Team can change this at any time.
11. The system may provide the facility to pause recording during a call (this may be limited when working from home or using the remote office setting), this, or the options below, can be used by individual staff during a call if it is clearly not for one of the purposes above or to provide a reasonable adjustment. For example this could include:
 - 11.1. union calls;
 - 11.2. manager calls with colleagues at the manager's discretion;
 - 11.3. personal calls made in line with our telephone use policy;
 - 11.4. calls with complainants or staff at public bodies or other organisations, when it is agreed that call should not be recorded. This can be on request or can be offered;
 - 11.5. calls to HR;
 - 11.6. internal calls for non-casework purposes; and
 - 11.7. external calls for non-casework purposes, for example, to IT support at SG.
12. Misuse of the pause option or the options below to avoid calls being recorded for legitimate business purposes could result in disciplinary action. Staff can also ask for calls to be deleted if they consider it clearly does not meet the purposes for recording. A manager or administrator will need to access the call to confirm this before deletion. Deletion in the system separates the call from its metadata ensuring that it cannot be searched for, deletion is temporary for seven days to allow for a period when mistakes can be rectified but after that point it will not be possible to retrieve the call. Permanent deletion will be in line with the retention plan.
13. If a user requests a call not be recorded or has concerns, staff can reassure them about the limited use of recordings and restrictions on access to the system and / or offer options which could include:
 - 13.1. To pause when the call is from a telephone where that is available;
 - 13.2. To agree the call will be deleted and not retained (this can normally be done relatively quickly and within three working days with limited processing of the call to ensure only that it is the correct call).

- 13.3. to reschedule until a call can be made where the pause facility is available.
 - 13.4. to reschedule until a call can be made that is completely unrecorded – this could be by either arranging to do so from the line of a colleague set to on demand, or by asking ICT to switch recording to on demand for a limited period (as this requires the involvement of ICT to switch recording of and their availability to do this should be checked before confirming the rescheduled time); and
 - 13.5. providing information about routes to access the office online / email / post which bypass call recording.
14. These options are likely to be particularly relevant where the data being recorded may be special category data, (including health / social work / prisons data about convictions) or if the user indicates they are uncomfortable or would find it distressing to have the call recorded. It is good practice to proactively offer this if there are indications the user is uncomfortable even where they have not said so explicitly.
 15. There are situations where it is not appropriate to offer all of these options. The option to only engage by email / post is always available – but options to allow unrecorded calls or paused recorded calls may not always be appropriate. These situations would include, but are not limited to situations where there have been difficult conversations or where the intention is to obtain direct evidence or to take consent.
 16. Staff can take advice from managers when they are considering whether or not to offer any or all of these options on an individual or regular basis.
 17. Decisions to agree one of the options should be taken forward should be noted on file along with any impact of that decision.
 18. Staff whose telephones have been set to always record will be able to pause calls but, as an additional protection, will be able to access telephones which are not being recorded for private calls or if they are undertaking work on a project or other basis which should not be recorded if they are in the office. Teams provides an alternative which can be audio only if they are not in the office or, for non-personal calls, if they are in the office but it is difficult to access the unrecorded line. Whether recorded or not, all calls remain subject to the telephone usage policy. Internal calls are incidentally captured on the system and, as they are unlikely to meet the purposes, staff can ask for these to be deleted if they confirm there is no business need to retain these.

Accessing calls

19. Staff whose telephones have call recording activated will have access to all of their own calls and can listen to them on the system. Calls should not be accessed unless there are reasons to believe the recording is for one of the purposes or because there is a request to delete the call. These reasons should be noted before access is made. If a call is accessed and it is decided it does not meet the purposes this should be noted.
20. Under the system's policies global users, company users, and team users will also be able to access calls made by other members of staff. We will use those policies to ensure that access to calls by other members of staff is limited. One global user will be a member of the corporate services team and additional global users will be authorized as required to provide cover. Company users will be able to access, calls for all users but will be unable to make changes to the settings of individual users.
21. We will set up sufficient company users for SAR / FOI and HR purposes. Team users will be able to access calls within their team but will have limited ability to make changes to the system. Managers and administrators (team officers or team assistants) may be set up as team users. It is also possible to extend the number of team users for other purposes with the approval of the leadership team. A manager can authorize access to calls by other staff and once authorization has been given may do so themselves or ask an administrator to do so on their behalf. An individual member of staff can also allow a colleague to access one of their calls as part of a reflective learning, induction or training/quality purpose.

Downloading and Retaining calls

22. Only team users, company users and global users will be able to download calls. Downloading should only occur when it is necessary and proportionate to meet the purposes. This will require the authorisation by a manager even when the request is made by the individual member of staff who is on the call.

Audit

23. The system allows for audit of its use. This will be undertaken for the following purposes:
 - 23.1. regular audits to ensure the system is being used appropriately, these will be conducted on a timetable to be agreed by the LT and the frequency of these will be decided on a risk basis, and
 - 23.2. audit where there are concerns there has been a misuse of the system. This can be authorised by managers and must also involve HR.

How calls are recorded

24. The call recording system allows for recording settings to be set for individual users. This means the setting will apply whenever they are using the telephony system through their own personal login. This will include calls through dedicated SPSO telephones but also on personal devices routed through the horizon system. The options available are:
- 24.1. always recording
 - 24.2. always recording with the ability to pause and resume during a call when accessing through an SPSO handset
 - 24.3. on demand which means that the calls are always recording but with immediate deletion. A manual override can be made keep the recording (This means that a recording is being made while the call is ongoing but automatically deleted as soon as the call ends. If a code is entered during the call the recording will not be deleted); and
 - 24.4. not recording.
25. In order to meet the purposes set out above the approach to designating recording levels for users will normally be:

Type of recording by user type	
Heads of, Director and Ombudsman	on demand when accessing through an SPSO handset
HR	not recording
Public service complaints	always recording with the ability to pause and resume during a call all lines with significant public facing use ie complainant; CRs, all A&G; Team officers, Team managers
Scottish Welfare Fund Lines with significant public facing use ie complainant / applicant	always recording with the ability to pause and resume during a call all lines with significant public facing use: CRS, Team managers, Team officers

Type of recording by user type	
INWO team	on demand when accessing through an SPSO handset
Other SPSO users	on demand when accessing through an SPSO handset
Shared telephones	the conference telephone and any other line which is used by other tenants will be set to never recording

What is recorded

26. Every call recording includes the following components:

Column name	Description
Call ID	The unique identifier of the call recording
Other party	The telephone number of the other party on a call with the user
User number	The telephone number of the user
Filename	The name of the call recording file
Telephony username	The unique username of the user
Status	Status of the call recording file on the portal (A = Available, P = Processing)
Direction	Call direction (I = Inbound, O = Outbound)
Connect time	Date and time of the call. Time is in UTC
Duration	Call duration in seconds
Retention period	How long the recording will be stored for, calculated from the day of the call

27. In addition, the system will log all actions taken in relation to the call:

Column Name	Description
Action	<p>The type of the audit event:</p> <ul style="list-style-type: none"> • Login • Add user • Delete user • Recording accessed (streamed or downloaded) • Bulk download accessed • Change password • Reset password • Add policy • Delete policy • Update user
Actor	The username of the user who performed the action
User	<p>This can be either:</p> <ul style="list-style-type: none"> • the username of the user who performed or was impacted by the action; or • the Call ID of the record that was accessed (streamed or downloaded)
IP	The IP address of the device, this is shown only for the actions Login and Recording Accessed
Date and time	Date and time of the audit event (i.e. of the action)

Informing people calls are being recorded

28. Consent is not required for recording for the purposes specified, although callers will have the ability to object to processing. In order to ensure we give appropriate notice SPSO will take steps to ensure, as far as practicable, callers are aware recording will occur and for what purposes.
29. A pre-recorded message will inform the caller that calls are being recorded on all incoming calls on outgoing calls. Users will also be notified if a call is paused or restarted by an audible bleep. A pre-recorded message / or bleep will also be played if a call is being recorded on demand.

30. Additionally, we will make our use of call recording visible on our website. We will include on relevant leaflets and templates. We will be clear that if the information to be discussed is sensitive (including special category) they can request that recording be paused.
31. Sufficient details will be included in our privacy notice to ensure users understand the purposes for use and call recording will be included in our information asset register. Staff will also be given information to allow them to answer specific questions.
32. Recording options ensure that we can quickly respond to objections and ensure that call recording does not act as a barrier to accessing the office.

How we access calls and keep them safe

33. Call recordings are kept secure by our telephony provider¹. When they are downloaded onto our system, they are kept safe by our own security protocols.

It is a breach of this policy to authorise access, or access without authorisation to recordings to others, or to use or listen to them, other than for the purposes set out in this policy.

It is also a disciplinary offence and will be addressed under the appropriate provisions of the data protection policy and / or disciplinary policy and procedure.

34. Calls should only be accessed if the relevant member of staff is satisfied that it is:
 - 34.1. necessary and proportionate to meet one or more of the purposes in this policy, or
 - 34.2. to comply with information or other legal rights.
35. We should record all decisions and when authorization is needed, when and how that has been provide. Templates may be created to support this but the absence of a template for any specific purpose / authorisation does not preclude the need to record and note appropriate reasons and authorisation.

How long we keep calls

36. The system automatically stores calls for 90 calendar days. Calls may be deleted (see above) and also may be downloaded and stored if they require to be kept for

¹ This is **GBT Technologies** who are using products from Gamma, security details here: <https://www.gamma.co.uk/products/security/>

longer to meet our purposes. Decisions to delete and download will need recorded and authorised on a case by case basis. The following table provides general advice and guidance on how to approach these decisions.

Reason	Retention period
Calls accessed to improve a written record but which we do not intend to keep on file	These can be accessed with the system and should not be downloaded
Calls which have evidence only available in the call or where it is has been decided a written record will not be adequate	Downloaded to WorkPro and kept in line with our casework retention policy
Calls kept as evidence of criminal or safeguarding issues	Retention period to be decided on a case by case basis and sufficient to meet the purpose
Calls accessed because of an allegation of nuisance/ harassment/ abuse to our staff and others	Retention period to be decided on a case by case basis and sufficient to meet the purpose
Calls accessed for the purpose of assessing a customer service complaint about us	To be kept on WorkPro in line with our normal retention policy
Calls accessed for quality / training purposes	To access them online within the three month period - with discretion by a member of the LT to download and retain for training purposes but to be held for no longer than one year

How we handle information rights requests

37. We may receive requests to access or receive copies of call recordings by someone who is seeking to use their information rights. We need to balance their rights against those of our staff and any third parties whose information may be included as well as respecting our own legislative obligations to keep information confidential and investigate in private.

SAR requests

38. We will normally provide audio copies of calls to individuals who request a call recording where they have been one of the parties to the call and are making a subject access request. We do though need to ensure the rights of SPSO staff whose voice is also captured or whose information is included in the call are respected. We also need to consider the rights of any third party discussed or involved in the call and they would also be able to make a SAR requests.
39. Therefore, before disclosing calls we will contact any SPSO staff whose data is affected. We will ask them for their views and encourage them to raise any questions or concerns they may have. Their views will be taken into account when making any decision whether or not to disclose an audio or a transcript. We will also seek the views of any third party when that is appropriate and / or possible given our legal obligations to maintain confidence and investigate in private. Each decision to disclose will be considered on its merits but there will be situations where we decide it is not reasonable to disclose a call recording. This could be because:
 - 39.1. the recording discloses sensitive personal data of someone other than the requester and that person has been asked for their views and they have said they would not wish that to be disclosed in audio format;
 - 39.2. the recording discloses sensitive personal data of someone other than the requester and that person's views are unknown and cannot reasonably be obtained;
 - 39.3. personal data would be disclosed and the individual affected has given reasons which we consider means it is not reasonable to disclose the call;
 - 39.4. disclosing in audio format would cause undue distress. This may be because the recording includes audio of a difficult conversation where someone was abused, harassed or upset;
 - 39.5. disclosing the recording may allow for the continuation of abuse or harassment or there is a reasonable risk that it will be misused;
 - 39.6. if it is decided it is not reasonable to disclose a call in audio format, we should consider whether it is possible to disclose in another format by transcribing. Again, we need to consider the rights of all data subjects when making such decisions; and
 - 39.7. we may decide that it is not reasonable to disclose even in circumstances where the member of staff does not express concern. We appreciate staff may be reluctant to voice concerns but also that it is important when it comes

to protecting staff from abuse or harassment there is a need for an office-wide approach.

Other Information requests

40. It is unlikely to be appropriate to disclose audio recordings on a regular basis in response to other information requests. However, in line with our normal approach, each request will be considered on its own merits and the same approach as set out above should be considered.

Using the system when not in Bridgeside House

41. The system will record all calls made by users including calls made via the portal when they are working from home or any other location.
42. Users who are automatically recorded on the system should avoid making calls which may meet the call recording criteria unless they can do so via Horizon. Exceptions can be made if there are technical difficulties accessing the system and not proceeding with the call would disadvantage the recipient of the call.
43. Users should not use the horizon portal if it is likely that they are in a space and / or using the system in a way where third parties may be recorded. For example, if they are at home and there are reasons to believe it is likely they may be interrupted during the time of the call.
44. While an unexpected issue arises and a third party is recorded accidentally a decision should be made with a manager about the extent to which the third party has been captured and whether the call should be deleted as a result of this.
45. Users who are accessing calls via the portal should not do so in a way that could lead to the call being overheard.

Back to the main [Contents Page](#)