

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	Author
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

Note: Highlighter is used in this document to indicate **outstanding actions** or where **links** to other documents under review, are required.

Contents

1. SPSO Records Management Plan
2. SPSO Records Management Policy
3. SPSO Business Classification Scheme
4. SPSO Retention and Disposal Policy
5. SPSO Clear Desk and Screen Policy
6. SPSO Protective Marking System
7. SPSO Managing Personal Data
8. SPSO Complying with Information Legislation
9. SPSO Out-of-Office Records Management and Security Guidance

1. SPSO Records Management Plan

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

Submitted to The Keeper April 2015

Approved by The Keeper [xx]

Contents

Introduction.....	2
The Public Records (Scotland) Act 2011	2
Records Management Plan.....	2
<i>Element 1: Senior management responsibility:</i>	3
<i>Element 2: Records manager responsibility:</i>	4
<i>Element 3: Records management policy statement:</i>	5
<i>Element 4: Business classification</i>	6
<i>Element 5: Retention schedules</i>	7
<i>Element 6: Destruction arrangements</i>	8
<i>Element 7: Archiving and transfer arrangements</i>	9
<i>Element 8: Information security</i>	10
<i>Element 9: Data protection</i>	11
<i>Element 10: Business continuity and vital records</i>	12
<i>Element 11: Audit trail</i>	13
<i>Element 12: Competency framework for records management staff</i>	14
<i>Element 13: Assessment and review</i>	15
<i>Element 14: Shared Information</i>	16

[Back to the main Contents Page](#)

Introduction

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

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.

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

The Plan has 14 elements which are:

1. Senior management responsibility
2. Records manager responsibility
3. Records management policy statement
4. Business classification
5. Retention schedules
6. Destruction arrangements
7. Archiving and transfer arrangements
8. Information security
9. Data protection
10. Business continuity and vital records
11. Audit trail
12. Competency framework for records management staff
13. Assessment and review
14. Shared information

The compulsory elements to ensure the records management plan will be agreed by the Keeper are 1, 2, 3, 6, 7 and 8.

RMP Element Description	SPSO Statement	Evidence
<p><i>Element 1: Senior management responsibility:</i> 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 Director: Niki Maclean.</p> <p>The Director 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 Director post and is evidenced by the job description. This plan is supported by the Senior Management 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>Director's Job Description [Doc 1]</p>

RMP Element Description	SPSO Statement	Evidence
<p>Element 2: Records manager responsibility: 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: Ellie Robertson (currently seconded to cover this post for 12 months as Helen Littlemore is on extended leave).</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 [Doc 2 and 2a]</p>

RMP Element Description	SPSO Statement	Evidence
<p>Element 3: Records management policy statement:</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Read further explanation and guidance about element 3 – http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement3.asp</p>	<p>The SPSO Records Management Policy is contained in one of the suite of SPSO Handbook - Information Governance (this document) at Section 2.</p> <p>The SPSO Handbooks are easily accessed by all staff from the SPSO intranet site, which provides a link to the document stored on the internal file management system. This particular handbook is also published on our website here: http://www.spsso.org.uk/corporate-information</p>	<p>SPSO Records Management Policy [Link in this document to Information Governance Section 2]</p> <p>Internal Audit of SPSO's public records management in March 2014 [Doc 3]</p> <p>SMT Minute 09/10/14 noting approval of Record Management Plan and Policy [Doc 04] Published: http://www.spsso.org.uk/sites/spsso/files/communications_material/minutes/2014/SM T2MeetingNote9Oct2014.pdf</p> <p>AAC Minute 21/10/14 noting endorsement of the Record Management Plan and Policy [Doc 05]</p>

RMP Element Description	SPSO Statement	Evidence
<p>Element 4: Business classification</p> <p>A business classification scheme describes what business activities the authority undertakes – whether alone or in partnership.</p> <p>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.</p> <p>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.</p> <p>A business classification scheme allows an authority to map its functions and provides a structure for operating a disposal schedule effectively.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>An authority will need to demonstrate that its business classification scheme can be applied to the record systems which it operates.</p> <p>Read further explanation and guidance about element 4: http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement4.asp</p>	<p>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 complaint handling, FOI/EIR/DP, and most complaint standards authority, outreach and media work. Individual records are created and stored electronically by reference number, with a corresponding paper file also retained by reference number.</p> <p>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 strives to be a paper-less office for these functions; therefore, there is no central storage or archiving of paper files.</p> <p>Some personnel functions, such as payroll, are contracted out to MoorePay, who manage and retain personnel details to provide this service.</p> <p>Throughout 2013-14 the SPSO developed a business classification scheme (BCS) for the non-casework business records. In September 2014 the SPSO implemented the BCS through an electronic records management system (ERMS) on a SharePoint platform.</p> <p>The BCS is described in Section 3 of the SPSO Handbook - Information Governance (this document). The BCS will be reviewed every two years by the Senior Management Team, with the Director providing oversight of the review.</p>	<p>CAS WorkPro ICT System Documentation [Doc 6]</p> <p>SharePoint Document Management Overview [Doc 7]</p> <p>Planning email for BCS workshop with IG April 2014 [Doc 8]</p> <p>Invoice for BCS workshop with IG April 2014 [Doc 9]</p> <p>SPSO Business Classification Scheme [Link in this document to Information Governance Section 3]</p>

RMP Element Description	SPSO Statement	Evidence
<p>Element 5: Retention schedules</p> <p>A retention schedule is a list of records for which pre-determined disposal dates have been established.</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 the authority's public records.</p> <p>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).</p> <p>The principal reasons for creating retention schedules are to:</p> <ul style="list-style-type: none"> • 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. <p>'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.</p> <p>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.</p> <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>	<p>The SPSO Retention and Disposal Policy is included in the SPSO Handbook - Information Governance (this document) at Section 4. 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. When agreed, it will also include a MoU with National Records Scotland for the long-term archiving of particular records of national interest.</p> <p>ACTION PLAN: Complete the on-going negotiations with NRS to finalise MoU. (2015) Senior Personal Assistant</p>	<p>SPSO Retention and Disposal Policy [Link in this document to Information Governance Section 4]</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) at Section 4. 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 Compendium Officer.</p> <p>Destruction 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>Destruction arrangements for electronic records contained in the filing system are managed in-house using the electronic file management arrangements contained within WorkPro and SharePoint. Email records are archived and destroyed in line with SCOTS Connect arrangements using MS Exchange 2010 and Enterprise Vault 10.</p> <p>IT hardware must be returned to ISIS 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 [Link in this document to Information Governance Section 4]</p> <p>Compendium Officer Job Description [Doc 10]</p> <p>WorkPro case file destruction log [Doc 11]</p> <p>Paper Shredding Services [Link to contractor's website]</p> <p>PSS Shredding Procedures [Doc 12]</p> <p>PSS Certificate of physical destruction by onsite shredding [Doc 13]</p> <p>SG Intranet page outlining Physical and Environmental Security [Doc 14]</p> <p>SG Intranet page outlining Administrative and Procedural Security Policy [Doc 15]</p>

RMP Element Description	SPSO Statement	Evidence
<p><i>Element 7: Archiving and transfer arrangements</i></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) at Section 4. 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 [Link in this document to Information Governance Section 4]</p>

RMP Element Description	SPSO Statement	Evidence
<p>Element 8: Information security</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Read further explanation and guidance about element 8: http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement8.asp</p>	<p>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.</p> <p>To ensure the proper level of security for all the SPSO records:</p> <ul style="list-style-type: none"> • 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). 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. • all employees have met the requirements for receiving a Disclosure Scotland Certificate; • the building at 4-6 Melville Street is adapted to meet the Scottish Government security requirements for the SCOTS GSI network; • the SPSO Clear Desk and Screen policy is described in Section 5 of 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; • a full security check of office cabinets, desks and other storage facilities is undertaken annually; • the SPSO Complying with Information Legislation User Guide is described in Section 8 of 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; • the SPSO policy 'Working from home' in the SPSO Handbook - Health and Safety describes confidentiality and security rules for business conducted on behalf of the SPSO; • the SPSO Out of Office records Management and Security User Guide is described in Section 9 of 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 access and exploitation; and • the Corporate Information Governance Officer provides training to all staff regarding the DPA requirements. 	<p>Internal Audit 04/13 – IS Installation and Network Services [Doc 16]</p> <p>ISIS MoU [Doc 17]</p> <p>SG Intranet page outlining Administrative and Procedural Security Policy [Doc 15]</p> <p>SG Disclosure Scotland Guidance [Doc 18]</p> <p>SCOTS Connect Security Standards [Doc 19]</p> <p>ISIS Security Survey 03/11 [Doc 20]</p> <p>SG Intranet page outlining Access Control Policy [Doc 21]</p> <p>SPSO Clear Desk and Screen policy [Link in this document to Information Governance Section 5]</p> <p>SPSO Facilities Security Audit 2014 [Doc 22]</p> <p>SPSO Complying with Information Legislation User Guide [Link in this document to Information Governance Section 8]</p> <p>SPSO Protective Marking System [Link in this document to Information Governance Section 6]</p> <p>Staff Confidentiality Statement [Doc 23]</p> <p>SPSO Working from home [Doc 24]</p> <p>SPSO Out of Office records Management and Security User Guide [Link in this document to Information Governance Section 9]</p> <p>Training Presentation [Doc 25]</p> <p>Email to team managers re compulsory training [Doc 26]</p>

RMP Element Description	SPSO Statement	Evidence
<p>Element 9: Data protection</p> <p>An authority that handles personal information about individuals has a number of legal obligations to protect that information under the Data Protection Act 1998.</p> <p>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.</p> <p>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.</p> <p>Read further explanation and guidance about element 9: http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement9.asp</p>	<p>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). The SPSO Complying with Information Legislation User Guide is described in Section 8 of 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. The SPSO outlines its duty to employees in the policy 'Managing Personal Data' in Section 7 of the SPSO Handbook - Information Governance (this document).</p> <p>The SPSO publishes a privacy notice on its website and summarises its duties in leaflets for complainants. It also provides a statement on the footer of all template letters to complainants.</p> <p>The SPSO is a registered data controller with the Information Commissioner's Office (ICO).</p> <p>When completed, the SPSO will have a Data Protection Policy Statement included in the SPSO Handbook - Information Governance (this document).</p> <p>ACTION PLAN: Write a DP Policy Statement and an Information promise. (Delayed until 2016 as CIGO is on extended leave) Corporate Information Governance Officer</p>	<p>Registered data controller with ICO. Registration Number: Z7336887 Date Registered: 29 Nov 2002 Registration Expires: 28 Nov 2014</p> <p>SPSO Complying with Information Legislation User Guide [Link in this document to Information Governance Section 8]</p> <p>SPSO Managing Personal Data [Link in this document to Information Governance Section 7]</p> <p>SPSO Website Disclaimer and Privacy Policy [Doc 27]</p> <p>Template letter privacy notice [Doc 28]</p> <p>Notice in Complainant leaflet containing Anonymity statement [Doc 29]</p> <p>SPSO Data Policy Statement [Link to Information Governance Section xx]</p>

RMP Element Description	SPSO Statement	Evidence
<p><i>Element 10: Business continuity and vital records</i></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 ISIS 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>Link to SPSO Business Continuity Plan which is published on SPSO website</p> <p>ISIS MoU [Doc 17]</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 (SharePoint) 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 file. The results of the audit are reported to the Senior Management 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 those that will be agreed for long-term archiving by NRS.</p>	<p>CAS WorkPro ICT System Documentation [Doc 6]</p> <p>CAS SharePoint ICT System Documentation [Doc 7]</p> <p>2015 File Location Audit Results – email to all staff 9 Apr 15 [Doc 30]</p> <p>Screenshot showing the location of the associated paper file on a case in WorkPro [Doc 30a]</p>

RMP Element Description	SPSO Statement	Evidence
<p><i>Element 12: Competency framework for records management staff</i></p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Read further explanation and guidance about element 12: http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement12.asp</p>	<p>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.</p>	<p>Director's Job Description [Doc 1]</p> <p>Corporate Information Governance Officer's Job Description [Doc 2 and 2a]</p>

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. 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 Senior Management Team for approval and the Audit and Advisory Committee for information. The Keeper will be informed of the outcome from this review.</p> <p>The first review will be in April 2017.</p> <p>ACTION PLAN: Report the results of the first review to the Keeper. (May 2017) Corporate Information Governance Officer</p>	

RMP Element Description	SPSO Statement	Evidence
<p>Element 14: Shared Information</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Read further explanation and guidance about element 14: http://www.nas.gov.uk/recordKeeping/PRSA/guidanceElement14.asp</p>	<p>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 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 Section 7 of the SPSO Handbook - Information Governance (this document).</p> <p>SPSO moved onto the SCOTS network in 2011 to access the secure GSI email network for the safe sharing of electronic documents. SCOTS is an Impact Level 3 (IL3) (restricted) network under the HMG Security Policy Framework. As such, all users have security clearances appropriate to handling IL3 data. The network is officially accredited to handle data up to 'restricted' level and is connected to the Government Secure Intranet (GSI), which means that data transmitted to other organisations within the GSI is protected against interception during transmission. The security procedures are accredited under the CESG GSI Code of Connection and are reviewed and renewed by CESG/OGC annually.</p> <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>ACTION PLAN: Methods for bulk sharing of electronic records are currently being researched by SCOTS using the Egress solution and is due to be piloted in 2015.</p>	<p>SPSO Handbook - Complaints Handling Guidance Section C Step 9a SPSO Sharing Information User Guide [Doc 31]</p> <p>Eagle Couriers Tender for Contract November 2013 outlining security clearance of drivers and security checks [Doc 32]</p> <p>SCOTS Connect Security Standards [Doc 19]</p>

[Back to the main Contents Page](#)

2. SPSO Records Management Policy

Contents

- Introduction.....2
- Purpose and Scope.....2
- What is Records Management?2
- Why is Records Management important?3
- Policy statement and commitment3
- Roles and responsibilities.....4
- Legislative Framework4
- Relationship to other SPSO policies5
- Training5
- Monitoring and Review.....5

[Back to the main Contents Page](#)

Introduction

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.

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.

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

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 recordkeeping, and to act as a mandate for the support and delivery of records management policies, procedures and initiatives across the organisation.

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.

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.

The aims of this policy include:

- the improvement of business efficiency through less time spent searching for information,
- increased joined up working and improved communications across the organisation as a whole;
- the demonstration of compliance with statutory and regulatory recordkeeping obligations including the Public Records (Scotland) Act 2011, the Freedom of Information (Scotland) Act 2002, Environmental Information Regulations 2004 and the Data Protection Act 1998; and
- the promotion of openness, transparency, accountability and improved corporate governance, commensurate with the organisation's role.

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?

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.

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.

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.

We retain records that provide evidence of our functions, activities and transactions, for:

- 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.
- Internal & 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.
- 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?

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.

The benefits of implementing records management systems and processes include:

- improved information sharing and the provision of quick and easy access to the right information at the right time;
- the support and facilitation of more efficient service delivery;
- improved business efficiency through reduced time spent searching for information;
- demonstration of transparency and accountability for all actions;
- the maintenance of the corporate memory;
- the creation of better working environments and identification of opportunities for office rationalisation and increased mobile working;
- risk management in terms of ensuring and demonstrating compliance with all legal, regulatory and statutory obligations;
- the meeting of stakeholder expectations through the provision of good quality services.

Policy statement and commitment

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:

- The maintenance of a business classification scheme (BCS) to reflect the functions, activities and transactions of SPSO.
- 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.
- The review of information security policies and procedures in order to protect records and systems from unauthorised access, use, disclosure, disruption, modification, or destruction.

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.

- The review of data protection policies in order to demonstrate the SPSO's commitment to compliance with the Act and the safeguarding and fair processing of all personal data held.
- The review of the business continuity plan, encompassing strategies to ensure that vital records held by the SPSO remain accessible over time and that there are processes in place to monitor the integrity and usability of records.
- 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 (e.g. creation, access, editing, destruction or preservation).
- The identification of records management as a distinct stream within the organisation's training portfolio, with dedicated training provided to all staff.
- 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

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

The **Senior Management 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 recordkeeping 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.

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 Director as appropriate.

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.

Legislative Framework

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

All Records

- Access to Health Records Act 1990
- Data Protection Act 1998
- Electronic Communications Act 2000
- Equality Act 2010
- Freedom of Information (Scotland) Act 2002
- Environmental Information Regulations 2004
- Health and Social Care Act 2001
- Human Rights Act 1998
- Limitation Act 1980
- Medical Act 1983 (and subsequent revisions)
- Public Records (Scotland) Act 2011
- Public Records (Scotland) Act 1937
- Public Records Act 1958
- Race Relations Act 1976
- Sex Discrimination Acts 1975 and 1986

Financial and Contractual Records:

- Audit Commission Act 1998
- Civil Evidence Act 1995
- Companies Acts 1985 and 1989
- Consumer Protection Act 1987
- Financial Services Act 1986
- Latent Damage Act 1986
- Prescription and Limitation (Scotland) Act 1973
- Unfair Contract Terms Act 1977
- Value Added Tax Act 1994

Facilities

- Health and Safety at Work etc. Act 1974
- Management of Health and Safety at Work Regulations 1999

The Environmental Information (Scotland) Regulations 2004

Relationship to other SPSO policies

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

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

Compliance with this Policy and related standards and guidance will be monitored by the Corporate Information Governance Officer in consultation with the Senior Management Team.

This policy will be reviewed every two years, 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](#)

3. SPSO Business Classification Scheme

Contents

Introduction.....	2
Purpose.....	2
Definitions.....	2
Filing structure.....	3
<i>How does the filing structure aid records management?.....</i>	3
<i>Shortcuts and relating folders.....</i>	3
SPSO filing structure/business classification scheme.....	4
Annex 1 - SPSO Electronic Information Storage Good Practice Guide	5
Annex 2 - SPSO Business Classification Scheme (BCS)	6

[Back to the main Contents Page](#)

Introduction

Managing records, and in particular electronic records, presents a significant challenge for an organisation of any size or sector. Electronic records management needs to be very carefully considered and structured to ensure the integrity of the records is not compromised upon capture and they remain retrievable for as long as they are required.

Purpose

The purpose of this policy is to improve the management of non-casework electronic records within the SPSO by developing a classification structure and creating and applying records management rules to realise significant benefits including:

- improved business efficiency and effective use of IT resources
- structured management of records retained for legal and regulatory purposes
- support of accurate capture and management of electronic records (irrespective of format) into the file system
- access to records to enable informed and effective decision making
- retention of a corporate memory of transactions, decisions and actions taken by, or on behalf of, the organisation
- protection of the rights and interests of the organisation (and others) who the organisation retains records about
- protection of the characteristics of records, particularly their reliability, integrity and usability
- identification of records required for permanent preservation and archive

Definitions

Some terms used in a specific way:

Business classification scheme: An intellectual structure categorising business functions/activities or subjects to preserve the context of records relative to others. It is useful for aiding activities such as retrieval, storage and disposal scheduling of records.

Disposal: A formal decision taken on the final status of a record (or set of records) to either destroy the records, transfer to another organisation for permanent preservation or retain within the organisation's file system for further review at a later date.

Electronic records management system (ERMS): An electronic records management system (ERMS) is a computer program (or set of programs) used to manage electronic records stored in an associated database. It provides a variety of functions including access controls, auditing and disposal using a combination of system and user generated metadata.

Filing structure: A hierarchical structure of folders within a file system which provides a coherent location for capturing records.

File system: A method for storing and organising computer files and the data they contain to make it easy to find and access them.

Folder: A type of aggregation or container within a file system used to store records (and other folders). It is the principal building block of a filing structure.

Management rules: Management rules are a set of explicit instructions to users on the organisation's preferred means of managing records. These include direction on appropriate capture, access management and disposal of all records irrespective of format or media.

Metadata: Data describing the context, content and structure of all records and folders within a file system. In a file system this is essentially user-generated and 'passive' in that it can rarely be used for active management of the records. By contrast, metadata in an ERMS is more functional, often system-generated, extensive and linked tightly to system processes.

Operating system: An interface between computer hardware and a user that manages and coordinates use of computer applications using the available resources provided by a computer's processor.

Record: Information created, received and maintained as evidence and information by an organisation or person, in fulfilment of legal obligations or in the transaction of business.

Records management: The practice of formally managing records within a file system (electronic and or paper) including classifying, capturing, storing and disposal.

Shared drive: A specialisation of an operating file system, comprising a shared device (for example, hard disk or server space) used by multiple users and accessed over either a local area network or a wider area network connection.

Filing structure

A filing structure provides an environment for presenting a common understanding of how records should be stored and retrieved. This is particularly important not just for users working in a team, but also when working across the organisation by improving the retrieval of content and making it understandable to every user.

A filing structure must contain, at the very least, the following attributes:

- a structure that is easily interpreted and which discourages users from placing records in inappropriate locations
- simple names that identify the logical element of the filing structure
- established responsibilities for folder management, to ensure the filing structure is well maintained
- typically a 'functional' filing structure will have three levels (or layers) of folders that act as segregations for information. These levels represent the functions, activities and transactions of an organisation
- the fourth, and usually final, layer sits beneath these. It is defined by the business where the records are to be captured and stored. This prevents users from creating idiosyncratic, locally defined, sub-folder structures below this level, within a particular part of the filing structure, which does not conform to the corporate rules

How does the filing structure aid records management?

The filing structure reflects the relationship of business activities through careful structuring of folders (with meaningful titles) 'containing' the records. This structure illustrates what the organisation's business is, and it provides a means of managing its records.

From the user's perspective, a filing structure provides a logical structure which makes it easy to see where a specific record (or new folder) should be located. Organised filing structures support records management by providing an understandable and accessible location for all records which encourages users to work within it. This helps an organisation reduce the risk of business critical information being lost within an uncontrolled file system. It also helps motivate users to move records out of personal drives or email accounts where it may be deleted without anyone knowing it existed.

Shortcuts and relating folders

In an ERMS it is possible to create a record or container (folder) in one location but have it appear in multiple areas of the filing structure using a system of 'pointers'. These pointers are an interactive shortcut to an object that replaces the need for duplicate copies of a record and are coded to resolve any conflicts in access control and disposal management.

This technique can significantly reduce the amount of duplication present in a filing structure. It will also support organisations trying to respond to requests for information by ensuring only one copy of a record, or location for record exists.

SPSO filing structure/business classification scheme

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. This application provides an electronic records management system for all casework, including complaints handling, FOI/EIR/DP, and most complaint standards authority, outreach and media work. Individual records are created and stored electronically by reference number, with a corresponding paper file also retained by reference number.

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 strives to be a paper-less office for these functions, therefore, there is no central storage or archiving of paper files.

The main purposes of a BCS may be summarised as being:

- providing links between records that originate from the same activity or from related activities
- determining where a record should be placed in a larger aggregation of records
- assisting users in retrieving records
- assisting users in interpreting records
- assigning and controlling retention periods
- assigning and controlling access rights and security markings

Annex 1 - SPSO Electronic Information Storage Good Practice Guide

Folder conventions	Documents	All documents must be housed in a folder (bottom level) – try not to mix folders and docs at any level
	Folders	Only create a folder if it will contain 20+ items.
	Rules	If possible, one type of retention/destruction rule per library. Resist creating rules for folders where possible. Therefore, it helps to keep one 'type' of record in folders.
Naming conventions	CamelCase	Use CamelCase convention for naming of documents and folders. CamelCase (camel case) or medial capitals is the practice of writing compound words or phrases such that each word or abbreviation begins with a capital letter. The use of medial caps for compound identifiers is recommended by the coding style guidelines of many organisations or software projects. A study that specifically compared under_score style and CamelCase found that camel case identifiers could be recognised with higher accuracy among both programmers and non-programmers, and that programmers already trained in CamelCase were able to recognise CamelCase identifiers faster than underscored identifiers.
	Date	ShortNameYYMMDD - Default YYMMDDShortName - Alternate where appropriate
	ShortNames	Use the shortest name possible for all documents and folders. Library and file names are used as the full URL address links for documents. If they are too long, they will not work. Example URL format - SITE\RecordsLibrary\Folder\SubFolder\DocName
Significant Documents	Major Versioning	For all significant documents, use version control and declare a major version of the agreed final document.
Storage conventions	MyDocs	Must only be used for personal and private documents. SCOTS archiving policy will be in place.
	Location	Only one copy of each document should be stored. Using the Business Classification Plan, locate all documents in appropriate FUNCTIONAL folder and use URL links for ease of access when a document may also be required in another folders.

Annex 2 - SPSO Business Classification Scheme (BCS)

Electronic Record Management Scheme (ERMS) Site and Library Structure

R = Restricted access to Site or Library

K = Retain contents for a longer period

SITE	Document Library
WORKPRO (Casework)	Bespoke Complaints Handling application, files stored by reference number only. Corresponding paper files are stored by reference number only.
CASEWORK	Case Review PSOW Guidance Intranet Knowledge Legal Legal advice to retain MoUs Performance Management-R Professional Advisers Service Improvement Statistics Team Admin Water
COMMS	Admin Annual Reporting Design External Information Media Presentations Projects Published Reports
CORPORATE	AAC-R Audit External Audit Internal Documents Information Governance Meetings-R Planning Register o Interests Risks Security SPCB-R SPSO-K
CSA	LA RSL FE HE NHS SG etc. Social Care Social Work Water SPS Valuing Complaints Training Crerar Sinclair CSA Management Comms CSA Good Practice Guidance Good Practice External Advisory Committee AJT

SITE	Document Library
	DWP Mapping Model CHPs Performance and Costs PSOW Resources
FACILITIES	Car Parking Environment Floor Plans Health Safety Procedures Staff Reminders Works
FINANCE	Contracts Credit Card Finance Arrangements Order Nos Resourcing-R Transactions-R
HR-R	Discipline & Grievance Employee Relations Equal Opps Establishment HR Archive Learning and Development Pay and Reward Pensions-D Reporting Resourcing Union
ICT	Desktop Scanner Intranet Websites Laptops Printers Scotlands Digital Future SCOTS SharePoint SQL Report Builder Stylewriter Telephony User Guides WorkPro

SITE	Document Library
LEARNING AND DEVELOPMENT	2009 Review Training PowerPoints Apology Away Days Building Resilience Diversity Handling Difficult Contacts ICT Information Gov ILM First Line Management 2012 Investors in People Legal Meaningful Conversations NLP Organisations Intro Plans Forms Pre 2010 SPSO Functions
POLICY	Committees Consultations Development Research SWF
SPSO HANDBOOK (Policies)-K	Archived Policies Forms Handbooks
STAKEHOLDER S	WorkPro Contacts BUJs NHS Sounding Boards Scotland UK OA International Parliament (Scots Westminster) Pressure Groups Positive Feedback Staff Survey Christmas Greeting Stakeholder Engagement Strategy Comment Regulators
TRAINING UNIT	2013 Review Admin eLearning FEHE LA NES Joint NHS RSL Tailored (Other BUJs) Water Managing Difficult Behaviour

[Back to the main Contents Page](#)

4. SPSO Retention and Disposal Policy

Document history: first issued December 2010

Contents

Introduction.....	2
Statutory Obligations	2
Legislative considerations and models of best practice	2
SPSO casework retention and disposal periods	3
Other records	4
Disposal.....	4
Transfer of records to National Records of Scotland (NRS)	4
Roles and Responsibilities	4
Monitoring and review	5
Annex 1: SPSO Non-casework records retention periods	6
Annex 2: Memorandum of Understanding with National Records Scotland.....	9
Annex 3: British Library Web Archive Licence	10

[Back to the main Contents Page](#)

Introduction

The SPSO recognises that its administrative records are a unique and irreplaceable resource. The effective management of our records, 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 development of an efficient and effective records management system. Crucial to the success of the policy is the development and implementation of a retention and disposal schedule.

This retention and disposal policy aims to support the development of greater control over the records created by the SPSO. It will enable the SPSO to dispose of records promptly when they cease to be of any continuing administrative/legal value and will identify records which should be retained because of their long-term historical/research value.

The policy is to be read in conjunction with the [Records Management Policy](#) for the SPSO, which details the importance of managing records 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 records management policies, procedures and initiatives across the organisation.

Statutory Obligations

The management of the SPSO's records 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

Freedom of Information (Scotland) Act 2002 (FOISA), Environmental Information Regulations 2004 and Data Protection Act 1998 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. In Schedule 1 Part 1 of the Data Protection Act 1998, the 5th principle states that 'personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.'

These Acts, therefore, do not determine standard retention periods, but, with the exception of the 5th principle of the DPA, where possible information that has been requested under FOISA, EISR or DPA but withheld by SPSO should not be destroyed until the time allowed for the requestor to request a review and/or appeal has lapsed.

The Scottish Public Services Ombudsman Act 2002 does not determine specific periods for retaining case-related information. It 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'

This statement provides a benchmark upon which to base the SPSO retention periods.

The National Archives and National Archives of Scotland have developed Codes of Practice in line with the Freedom of Information (Scotland) Act 2002^{2 3}. In the Records Management: Retention

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

² Freedom of Information (Scotland) Act 2002. *Code of practice on Records Management*. Prepared in consultation with the Scottish Information Commissioner and the Keeper of the Records of Scotland. Laid before the Scottish Parliament on 10th November 2003 pursuant to Section 61(6) of the Freedom of Information (Scotland) Act 2002. November 2003

³ <http://www.nationalarchives.gov.uk/recordsmanagement/>

Scheduling, 7. Complaints Records, Section 3.1 states: 'The retention of records relating to complaints should be considered in the light of business requirements, taking account of the cost of retention and the use of the records in the future.' The Code requires policies to be in place on Retention, Disposal, Transfer and links to the Business Continuity Plan.

In the absence of prescriptive legislation and regulations, the overriding determinant is what suits the business requirements of the organisation. Determining this, however, is not necessarily straightforward. An additional consideration is that long retention periods of paper files is a costly and ineffective way to manage casework knowledge and could be seen as a contravention of DPA 5th principle if retention serves no business purpose. There are, however, cross-referencing benefits to retaining some case information such as referencing multiple complaints by a complainant, linked complaints, and tracking complaint trends. This is achieved to a great degree by retaining the case header for each complaint in electronic form.

SPSO casework retention and disposal periods

Following consideration of the existing legislation, peer practice and business requirements of SPSO the retention and disposal times for SPSO casework is approved as follows:

Reports

- SPSO Reports laid before the Scottish Parliament are published and kept by the SPSO and the Scottish Parliament indefinitely in electronic form. Individual reports are also held by the complainant and Bodies under Jurisdiction.

Electronic casework file:

- The electronic documents relating to the case file are permanently deleted after three years with no activity after last activity date.
- Except for surname and postcode, all other personal data (first name, address, telephone, email) electronically stored on the case file for the complainant, aggrieved and interested party is anonymised after three years with no activity after last activity date.
- All other information contained in the fields of the electronic case is retained indefinitely.
- 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.

Physical casework file:

- The physical casework file is retained for 24 months after the last activity date. The file is then destroyed.
- Separate folders of sensitive material, such as medical records and social work files, are separated from the casework file and destroyed before storing the case file in the office archive, usually three months after the last activity date.
- 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.

Notes:

- Last activity date is calculated from the most recent of either:
 - case closure date,
 - decision review closure date,
 - post activity closure date, or
 - customer service complaint closure date.
- The Ombudsman and management reserve the right to identify any case where the information is to be retained beyond the recommended period.

Corporate services will implement a monthly process for retaining and destroying records. This will be supported by the electronic case handling system (WorkPro) through:

- identifying cases due for disposal according to the policy;
- highlighting which files are currently subject to on-going activity, such as FOI/EIR/DPA requests, review of decision requests, service complaints; and

- recording all files disposed. Details recorded include case reference number; complaint's surname; authority; closure reason; confirmation that the case has been disposed and date of disposal.

Other records

The SPSO creates and receives a variety of records which are necessary for the carrying out the business of SPSO which are subject to more specific controls and regulations than is the case with complaints records. Organisations do not have any discretion over the retention period for many types of record as the legislation dictates the required period.

For those records where there is discretion, the SPSO policy is to retain records for only as long as there is a business requirement for the record, and no more than six years after last modified date, unless of national historic interest. This is in line with the general recommended disposal time for most types of significant corporate activities.

The table at Annex 1 outlines the retention periods for non-casework records which are not discretionary. The table is based on the recommendations from Scottish Council on Archives Local Authority Records Retention Scheme ([SCARRS](#)). Whilst this model has been designed specifically with Local Authorities in mind, it has wider application and identifies statutory and regulatory retention periods for those records where these exist and suggests typical retention periods based on common practice and/or business requirements where statutory and regulatory periods do not exist. The Scottish Council on Archives is the lead body for the advocacy and development of archive and records management services in Scotland.

The SPSO website and Valuing Complaints website are listed with the [UK Web Archive](#), whose purpose is to give permanent online access to key UK websites for future generations. The current licences are attached at [Annex 3](#).

Disposal

Secure arrangements for the disposal of materials are in place using the following processes:

- identification of eligible records for disposal as outlined in this policy, ensuring precedents and other material for longer term retention are removed for secure storage;
- 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
- updating and secure storage of disposal audit file.

Transfer of records to National Records of Scotland (NRS)

The NRS has arrangements with a number of organisations to receive their records and make them available to members of the public, normally after a defined period of time. These are records of enduring historical, cultural and research value. The SPSO has identified, in collaboration with the NRS, relevant SPSO documents for permanent preservation. Additionally, some information related to cases closed by the predecessor Local Government Ombudsman is retained by NRS. The SPSO retains a complete list of these cases.

Roles and Responsibilities

The Ombudsman has overall responsibility for ensuring that the SPSO complies with the requirements of legislation affecting the management of records, and with any supporting regulations and codes.

The Director is responsible for:

- ensuring that the Records Management Policy is implemented effectively;
- the provision of record management guidance to staff;
- producing procedures documenting all necessary record management arrangements;

- regularly reviewing and where necessary amending record management policies and procedure statements; and
- making recommendations to the Senior Management in relation to changes or improvements.

Line managers are responsible for:

- ensuring that the agreed records management policy and procedures are fully observed and implemented within their area of responsibility; and
- ensuring that all staff within their area of responsibility receive the appropriate training.

All members of staff are responsible for documenting their actions and decisions, and for maintaining the records in accordance with the SPSO's agreed policies and practices.

Monitoring and review

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

Annex 1: SPSO Non-casework records retention periods

For those records where there is discretion, the SPSO policy is to retain records for only as long as there is a business requirement for the record, and no more than **six years** after last modified date, unless of national historic interest.

The table below identifies retention periods for non-casework records which are not discretionary. The table is based on the recommendations from Scottish Council on Archives Local Authority Records Retention Scheme (**SCARRS**). The Scottish Council on Archives is the lead body for the advocacy and development of archive and records management services in Scotland.

Schedules referenced are:

- 12 Finance
- 13 Health and Safety
- 15 Human Resources
- 16 Information and Communication Technology
- 17 Information Management
- 20 Management
- 22 Procurement
- 24 Risk Management

<i>Category</i>	<i>Type</i>	<i>Retention Period</i>	<i>Legislation/Guidance</i>
Information Management	Data Protection - record of subject access request processing where appeal made to UK Information Commissioner	6 years from outcome of appeal	Data Protection Act 1998 c.29, s.7
	Freedom of information (FOISA) - processing of requests for information where appeal made to Scottish Information Commissioner	6 years from outcome of appeal	Freedom of Information (Scotland) Act 2002 asp 13
	Environment Information Regulations - processing of requests for information where appeal made to Scottish Information Commissioner	6 years from outcome of appeal	The Environmental Information (Scotland) Regulations 2004 SSI 2004/520

Category	Type	Retention Period	Legislation/Guidance
Finance	Annual accounts	Permanent	The Local Authority Accounts (Scotland) Regulations 1985. SI 1985 No. 267 (S. 24) Taxes Management Act 1970, c9
	Records documenting the preparation of the consolidated annual accounts and financial statements	6 years from end of financial year	
	Asset registers, depreciation and disposal registers	6 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	6 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	10 years	Business Requirement - Standards Commission
	Payroll records	6 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;
	Pension scheme reports	10 years	The Local Government Pension Scheme (Management and Investment of Funds) (Scotland) Regulations 2010. S.S.I.
	Individual staff pension files	10 years after date of payment	The Local Government Pension Scheme (Management and Investment of Funds) (Scotland) Amendment Regulations, SSI 2000 No. 74
	Procurement and Risk Management	Contract management files - ordinary contracts	5 years from end of contract
Approved supplier evaluation criteria records		5 years after being superseded	Prescription and Limitation (Scotland) Act 1973 c.52 and 1984 c.45
Purchase ordering records		5 years from end of financial year	Prescription and Limitation (Scotland) Act 1973 c.52 and 1984 c.45 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		5 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		5 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

Category	Type	Retention Period	Legislation/Guidance
Human Resources	Tender evaluation, negotiation and notification records - Unsuccessful tenders	1 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
	Contract award reports (OJEU)	5 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
	Insurance policy documents, Certificate of Insurance	5 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.
	Counselling	6 years from termination date	Prescription and Limitation (Scotland) Act 1973 c.52 and 1984 c.45
	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	5 years after investigation concludes and action is spent / Retain current information throughout employment	Statutory?
Health and Safety	Occupational health – sickness monitoring, personal risk assessments, absence reporting	6 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
	Risk assessment / Health and safety inspection reports	1 years after issue	National Archives
	Fire Safety Training – proof of training Maintenance schedules, diaries, logs Accident and Incident reports - adults	10 years after current year 16 years after superseded 3 years after action	Fire Safety (Scotland) Regulations 2006. SSI 2006 No 456 Regulation 20 National Archives Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 SI 2013 No 1471
ICT	Plant and equipment condition surveys	2 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	5 years from decommissioning	Prescription and Limitation (Scotland) Act, 1973 and 1984
	Maintenance of the software licence(s) for an ICT system	5 years from termination of licence	Prescription and Limitation (Scotland) Act, 1973 and 1984

Annex 2: Memorandum of Understanding with National Records Scotland

Currently in negotiations to finalise the MoU. Aim to be in place by March 2016.

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 name: Fiona Paterson

Position: Senior Personal Assistant to the Ombudsman

E-mail: fpaterson@spsso.org.uk

Tel: 0131 240 8850

Any other information:

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 name: Fiona Paterson

Position: Senior Personal Assistant to the Ombudsman

E-mail: fpaterson@spsso.org.uk

Tel: 0131 240 8850

Any other information:

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

Tel: +44 (0)20 7412 7184

E-mail: 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

[Back to the main Contents Page](#)

5. SPSO Clear Desk and Screen Policy

Document history: first issued Jul 2007

Contents

Introduction.....	2
Policy Statement	2
Clear Desk Procedure	2
Clear Screen Procedure.....	2
Training Implications	2
Review/Monitoring Arrangements	2
Audit Arrangements.....	3
Managerial Responsibilities.....	3
Non Conformance	3

[Back to the main Contents Page](#)

Introduction

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 legally obliged under the Data Protection Act 1998 to protect any personal information we hold.

Information security is characterised as the preservation of:

- Confidentiality: ensuring that information is accessible only to those authorised to have access;
- Integrity: safeguarding the accuracy and completeness of information and processing methods; and
- Availability: ensuring that authorised users have access to information when required.

Confidentiality, integrity and availability of information are essential to maintain legal compliance.

Policy Statement

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

The aim is for all work areas to be cleared of confidential papers at the end of each working day.

- Paper and computer media should be stored in the lockable cabinets and drawers when not in use, especially outside working hours. 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.
- Original medical records must be copied and returned as soon as possible. If they are required to be kept for a period of time, the original records must be stored in the fireproof cabinet. The Administrative Officer holds the keys for this cabinet.
- Lock your cabinets and drawers at the end of each working day and lock the keys in the key-cabinet.
- A spare copy of team keys will be stored in a keypad operated key cabinet on each floor.
- Sensitive or classified information, when printed, should be cleared from printers immediately.
- Mailroom pigeonholes must be cleared of sensitive or classified information every evening. Each team is responsible for their pigeonhole.
- 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

- All computer terminals are password protected.
- Computer terminals should be shut down when not in use.
- Computer screens should be angled away from the view of unauthorised persons.
- 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

It is essential that all staff are made aware of the key principles of information security. Training on this policy will take place as part of the induction for new starts.

Review/Monitoring Arrangements

All staff are responsible for monitoring their compliance with the principles/procedures detailed in this policy.

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 at three-year intervals thereafter. The review will be carried out by the Senior Personal Assistant and HR Officer.

An earlier review may be warranted if one of the following occurs:

- as a result of regulatory / statutory changes or developments;
- due to the results/effects of critical incidents; or
- for any other relevant or compelling reason.

Audit Arrangements

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

Managerial Responsibilities

The Ombudsman has ultimate responsibility for compliance of this policy. The Senior Management 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.

All staff have a responsibility for reporting information security incidents, including any breaches of confidentiality, to their Manager.

Non Conformance

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](#)

6. SPSO Protective Marking System

Contents

Introduction.....	2
Purpose.....	2
Protective Marking Classifications.....	2
Determining the level of Protective Marking.....	2
Marking Information.....	3
<i>Casework</i>	3
<i>Meeting Reports</i>	3
<i>Non SPSO Information</i>	3
<i>Emails</i>	3
<i>Review of Markings</i>	3
Assessing the consequence of compromise.....	3
Carriage of Protectively Marked assets.....	4
Bulk personal data transmissions.....	4
Incident reporting.....	4

Introduction

The SPSO holds a wide range of information, some of which is subject to disclosure restrictions and some of which is either currently publically 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.

A protective marking system is the method by which the originator of information indicates to others:

- 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
- the procedures to be followed regarding the handling, transmission, storage and disposal of the document
- the severity or impact of the loss or disclosure of the document
- It is designed to protect information from intentional or inadvertent release to unauthorised readers.

Purpose

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.

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 1998 or the Environmental Information Regulations 2004.

Protective Marking Classifications

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.

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.

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

Determining the level of Protective Marking

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 should be assigned where the compromise of information or material would be likely to:

- cause inconvenience, embarrassment, harm or distress to individuals
- cause financial loss or loss of earning potential, or to facilitate improper gain or advantage
- damage to the SPSO's standing or reputation and loss of public confidences
- cause financial impact to the SPSO

- breach obligations to maintain the confidentiality of information provided by individuals or third parties
- breach statutory restrictions on the disclosure of information (for example, the Data Protection Act)
- prejudice the investigation of, or facilitate the commission of, low-level crime, or hinder the detection of serious crime
- undermine the proper management of the public sector and its operations.

Examples:

- Complete set of an individual's social care files or health records.
- Investigation files
- 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

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 the footer to appropriate letters further indicates how the document should be handled.

[Footer: Investigations by the Scottish Public Services Ombudsman are to be carried out in private, in terms of the Scottish Public Services Ombudsman Act 2002. Accordingly, this correspondence must not be made publicly available. This does not affect the rights of recipients to seek legal advice in relation to this complaint. Where appropriate, recipients are also reminded of their obligations under the Data Protection Act 1998 in relation to the processing of personal and sensitive personal data.]

Meeting Reports

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.

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

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.

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 to a third party without prior written approval of the originator.

Emails

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

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

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.

The accumulation and aggregation effect also needs to be taken into effect 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

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.

Please refer to the [SPSO Out-of-Office 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

Before bulk data transfer is established with another organisation the following must be considered:

- that there is a valid business requirement to perform bulk data transfers and that it is legal, appropriate and acceptable.
- that the recipient, where appropriate, is contractually aware of the use that they can make of the personal data SPSO provides to them.
- 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.
- that the GSI (Government Secure Intranet) should be the default choice for bulk personal data transfers where both organisations are connected to the GSI.
- 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.
- 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

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](#)

7. SPSO Managing Personal Data

Document history: first issued 2006

Contents

Introduction.....	2
Definitions.....	2
Processing Personal Data.....	2
Personal Data Held	2
Rights of Access to Personal Data.....	2
Updating Personal Data	3
Security and Destruction of Personal Data	3
Disclosure of Personal Data to External Bodies.....	3
Access to Medical Reports.....	3
Staff Awareness and Training	4
Disputes	4
Review.....	4
Annex 1 - Guidelines on Processing Personal Data during Recruitment and Selection	5
Annex 2 - Checklist for Current Personal Files	7
Annex 3 - Checklist for Terminated Files	8
Annex 4 - Procedure for Accessing Personal Files	9
Annex 5 - Application for Access to Health Reports.....	10
Annex 6 - Notifiable Changes.....	11
Annex 7 - Personal Information – strictly confidential	12
Annex 7a - SPSO Managing Personal Data Policy.....	13

[Back to the main Contents Page](#)

Introduction

This Policy sets out the principles adopted by the Scottish Public Services Ombudsman (SPSO) on the use, maintenance and access to personal data relating to prospective, current and former SPSO staff.

Definitions

For the purpose of this Policy, personal data is defined as data relating to individuals that are held on computer or on manual files/data record systems.

Manual data record systems are those that are structured by reference either to individuals or to criteria relating to individuals, so that specific information relating to a particular individual is readily accessible.

Sensitive data is information concerning an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition, any medical information, sexual life, commission or alleged commission of any offence or proceedings for any offence committed or alleged to have been committed.

Processing Personal Data

Personal data shall be processed only for such purposes as are necessary under the employment contract or to comply with any legal obligations.

Staff members are informed of the SPSO's purpose and use of any personal data requested via express sections in application forms, equal opportunities forms, contracts of employment or documents containing/requesting personal information. In general, the SPSO seeks to inform staff members about how personal data will be used and their right of access to it.

Sensitive personal data is anonymised wherever practicable.

The SPSO obtains the explicit consent of a staff member for the disclosure of personal data to a third party. Permission will always be sought from the staff member for the issue of a reference.

Where disclosure is required by law, the SPSO seeks to inform staff member(s) in accordance with the Information Commissioner's code of practice for managing employment records.

Any third party processing data on behalf of the SPSO is required to guarantee compliance with these guidelines.

Personal Data Held

Specific guidance on the processing of personal data obtained during the recruitment and selection process is contained within [Annex 1](#). Guidance on what data will be held on manual files is set out in [Annex 2](#) and [Annex 3](#). This covers both existing and terminated files.

Personal data that may change, such as a home address, is sent annually to each staff member for verification or amendment. It is the responsibility of individual members of staff to notify such changes to the Human Resources Officer (see [Annex 7](#)).

Rights of Access to Personal Data

All staff have the right of access to personal data held on them, whether held on manual or computerised systems with the exception of:

- employment references, unless the referee has consented to disclosure or it is reasonable to do so without consent (i.e. to anonymise the data); and
- information provided in confidence by a third party.

Access to personal data is based on a need to know basis. Please refer to [Annex 4](#). The following may view or receive information from a personal file:

- staff member whose details are on file;
- Human Resources staff and the Ombudsman;
- staff member's line manager as agreed with the staff member; and
- external bodies, with the express consent of the individual or where there is a statutory requirement to provide the information.

Guidelines for staff wishing to access their personnel record/file are outlined in [Annex 4](#).

Updating Personal Data

Amendments to personnel records are made timeously by the Human Resources Officer.

Staff should provide updates by email or letter to the HR Officer. Examples of the type of data that should be notified are contained in [Annex 6](#).

Security and Destruction of Personal Data

Personal data is stored securely in lockable filing cabinets within the Human Resources' department, in order to prevent the unauthorised access and processing of personal data, ensuring at all times that confidentiality is maintained. Personal data may also be held on secure IT systems.

Personal data held on manual record systems that is no longer required is destroyed by shredding. Similar data held on computerised systems is deleted from the systems.

A diary system is used to ensure disciplinary warnings are removed and deleted from personal files on the appropriate date.

Disclosure of Personal Data to External Bodies

Personal data is disclosed where there is a statutory requirement to disclose or at the staff member's own authorised request (such as mortgage applications).

Unauthorised disclosure of personal data by a member of staff may be treated as a disciplinary matter and dealt with under SPSO [Disciplinary Procedure](#). If in doubt about whether to disclose, staff should not disclose information and seek advice from the HR Officer. In particular, staff must not give out the following where there is no evidence of consent:

- home address and telephone numbers;
- disclosure of earnings; or
- bank account details.

The SPSO has a [References Policy](#). This Policy states who is authorised to give references and in what circumstances.

Staff leaving the SPSO are asked to confirm in writing, as part of the process of dealing with their resignation, whether they wish the SPSO to respond to future requests for references.

Access to Medical Reports

(also see [Absence Policy Procedure](#) – Medical Assessment Guidance)

There are statutory rights for access under the Access to Medical Reports Act 1988. Under the Act, the SPSO cannot apply for a medical report from a doctor who has been responsible for the physical or mental health of a staff member without the staff member's consent. The consent form (see [Annex 5](#)) also asks, in accordance with the Act, whether the staff member wishes to see the report before it is sent to the occupational health physician who is authorised to provide a report for the SPSO on the state of health of the staff member.

If the staff member decides that they would like to see the report first, the SPSO informs the doctor of that fact and notifies the staff member of the date that the application for the medical report is actually made. The staff member then has 21 days in which to arrange with the doctor to see the report. It is the staff member's responsibility to make these arrangements. Whilst there is no charge for reading the report, if the staff member arranges with their doctor to have the report photocopied, and if necessary posted to themselves, the doctor may charge a reasonable fee to cover the cost of doing so.

If the staff member did not indicate on the consent form that they wished to see the report but later changes their mind, on their own initiative, the staff member will be able to notify the doctor that they wish to see the report before it is sent to the occupational health physician. The staff member will then have 21 days from the date of notification to the doctor to arrange to see the report. In cases where the staff member changes their mind, please note that the doctor is not obliged to delay supplying the report to the occupational health physician. By the time the staff member has decided that they would rather see the report first, the doctor may already have supplied it. If, following notification to the doctor, the staff member has seen the report, the doctor will not be able to supply the report without their further consent.

Having seen the report, the staff member is entitled to request that the doctor amend any part of the report which the staff member considers to be inaccurate or misleading. If the doctor does not agree to amend the report as requested the staff member will be able to attach a written statement to the report giving their view on its contents. Whether or not the staff member decides to see the report before it is supplied, the doctor will be obliged to keep a copy of the report for at least six months / 20 years after the date it was supplied, and the staff member is entitled to have access to the report.

The doctor is not obliged to let the staff member see those parts of the medical report that he or she believes is likely to cause serious harm to your physical or mental health or that of others, or which would reveal information about another person or the identity of a person who has supplied the doctor with information about the staff member's health unless that person also consents. In those circumstances, the doctor will notify the staff member and they are limited to seeing any remaining parts of the report.

Staff Awareness and Training

All staff are made aware of where and why their personal information is held at induction, through awareness raising processes, and by senior management communications.

Disputes

There are a number of options open to a staff member if they do not agree with a decision or action relating to this policy:

- informal discussions with their line manager as there may be some simple misunderstanding of the procedure or facts which can be resolved by an informal route;
- use of the SPSO's internal grievance procedure; and
- assistance from a third party such as a trade union representative or some other suitably experienced person

Review

The SPSO reviews this policy on a regular basis.

Annex 1 - Guidelines on Processing Personal Data during Recruitment and Selection

These guidelines cover data that the SPSO may collect, process and retain on any individual who applies for employment with SPSO. The guidelines cover the following range of applicants:

- applicants (both successful and unsuccessful);
- former applicants (successful and unsuccessful); and
- agency workers (current and former).

The SPSO seeks to strike a balance between the needs of an employer and the right of the applicant to enjoy respect for his or her private life.

The SPSO only seeks to collect personal data that is relevant to the employment relationship. It ensures the proper safeguards are in place to protect sensitive data.

Applications

- Application forms state that information provided is used solely for the purposes of recruitment and selection.
- Only personal data that is relevant to the selection process and the potential on-going employment relationship is sought on application forms.
- Information about the criminal convictions of an applicant is only requested if that information can be justified in terms of the role offered.
- Sensitive data is requested via equal opportunities monitoring forms. These are kept separate from application forms and not disclosed to recruiting managers. The purpose of requesting this data is explained on the monitoring form.
- Verification of information provided in the application form is only carried out for successful candidates.
- Applications are returned to Human Resources. Applications made online can be submitted via a secure method of transmission and can only be accessed by those involved in the recruitment process.

Verification of data

Verification of data supplied by applicants does not go beyond that which is sought on the application form or supplied later in the recruitment process and which is justified in order to meet the requirements of the position.

Short Listing

- Recruiting managers assess applications against essential and desirable criteria and record this on standard short listing forms. These are retained on the recruitment file for the vacancy.
- Where tests are used in the selection process, these are only used and interpreted by those who have received appropriate training. The tests used are reviewed periodically to ensure they fairly apply the short listing criteria to all applicants.

Interviews

Only personal data that is relevant to and necessary for the selection process is recorded and retained following interview. The SPSO uses a competency based recruitment process in which all recruiting managers are trained. Only questions and data relevant to the competencies required are asked/sought.

- All interviewers are made aware that interviewees have the right to request access to their interview notes.
- All interviewers are briefed on how to record and store interview notes.

References

- References are only taken up for candidates being offered a post and with the express consent of the individual.

- References are taken up by the Human Resources Officer.

Retention of recruitment records

- Application forms of successful candidates are retained on their personal file.
- Recruitment files, including application forms of unsuccessful candidates and interview notes, are retained by Human Resources for a period of up to one year from the date of interview.
- Manual records are kept in locked filing cabinets and electronic files are kept secure by using passwords.
- Equal opportunities forms are retained on the recruitment file for the vacancy.
- Personal data obtained during the recruitment process that is no longer relevant to the employment relationship are destroyed.
- Access to recruitment records is limited to Human Resources and the recruiting managers. With the agreement of the applicant, line managers may also receive feedback in order to discuss this with the applicant.
- Applicants will have access to interview notes made about them.
- Manual data is shredded and electronic files permanently deleted from the system when the information is no longer required in line with the [Retention and Disposal Policy](#).

Annex 2 - Checklist for Current Personal Files

'While there is no legislation to prevent records being retained in computerised or microform formats, there may be some practical difficulties which should be considered if selecting these methods of record-keeping. Most of the suggested retention periods (see Annex 7) for such records are simply the limitation period for bringing legal action. In the event that employment contracts/accident records books and other personnel records are needed for the purpose of a legal action, it is best to have the originals. Microform copies may be satisfactory but computerised records which do not resemble the original format would probably not. Therefore, employers should think carefully about which records they wish to computerise.' (CIPD – Retention of personnel and other related records 02/03/2004)

The SPSO retains the following on current personal files:

- copy of advert;
- job description;
- application form;
- signed copy of contract;
- references (in sealed envelope if no consent given for access to staff member). References will normally be sought when a job offer is made. By signing the application form authority is given to the SPSO to contact referees should a job offer be made. Successful candidates may be required to complete a criminal records check application for submission to Disclosure Scotland and will not be able to take up their post until clearance has been received from Disclosure Scotland;
- signed copy of offer letter;
- personal details form;
- bank details;
- pension form;
- confidentiality agreement (where appropriate);
- work permit details (where appropriate);
- copy of relevant qualifications;
- changes to contract;
- written correspondence between individual and the SPSO;
- current disciplinary warnings;
- grievance documentation;
- Maternity/Paternity/ Adoption/Parental leave application form;
- copy of MATB1 (maternity leave);
- accident documentation including accident report forms;
- source generated reports for the individual member of staff;
- induction checklists;
- appraisal records;
- training records;
- personal Development Plans; and
- leave records

Notes of informal counselling sessions are not held on personal files, although individuals and line managers should hold confidential copies. These are destroyed once the matter has been resolved to the satisfaction of the line manager and the individual.

Annex 3 - Checklist for Terminated Files

The SPSO retains the following on terminated personal files:

- application form;
- job description;
- references;
- personal particulars form;
- pension form;
- contract and contract changes;
- medical certificates dating back three years;
- accident documentation;
- relevant correspondence between member of staff and the SPSO;
- references given to employers;
- resignation letter;
- termination form;
- leave records;
- current disciplinary details still live at termination; and
- exit interview documentation.

Terminated files are retained in secure storage for a period of six years from the date of termination with the SPSO for the purpose of providing references for future employers and responding to any claims made against the SPSO. An electronic index of terminated files is held within Human Resources to enable access to files.

Terminated files for staff who have left within the previous three months are retained by the HR Officer in order to respond to any immediate queries arising regarding the termination of employment.

Annex 4 - Procedure for Accessing Personal Files

Storage of files

- Complete records are held by Human Resources.
- Managers should hold only relevant information required to effectively manage staff within their teams. Sensitive data is not held by managers.
- Files containing personal data are held in locked drawers/cabinets or on secure IT systems.

Staff access

- Access to all personal information must be requested in writing via email or letter to the HR Officer.
- Requests for access are dealt with as quickly as possible and within a maximum of five working days of receipt of the request.
- Staff are not allowed to remove their personal file from the HR Department.
- Staff are able to take a copy of information held on their files.
- An HR staff member will be present when staff members access their personal files in order to clarify any queries or record amendments/deletions.

Access by line managers

- Access is restricted to information that is required by managers in relation to their duties regarding the management of staff, such as sickness absence records, personal development records and disciplinary records.
- Requests from managers or other sources for access to sensitive data requires the consent of the staff member before the information is produced.

The above guidelines also apply to records held electronically.

Annex 5 - Application for Access to Health Reports

To:

Part A (to be completed by the staff member the record applies to)

I wish/do not wish* to see my Doctor's report before it is sent to the Occupational Health Physician.

I request access to my health report prepared by an Occupational Health Services professional following a medical examination on _____.*

Or

I give permission for _____ to have access to my health Report prepared by an Occupational Health Services professional following a medical examination on _____.*

Name: _____

Date: _____

Address: _____

Signature: _____

Part B (to be completed by the line manager)

I confirm that _____ is the person to whom the medical report applies;*

or

I confirm that _____ (name of applicant) is entitled to see the health report of _____ (name of person the report applies to.)*

Name: _____

Address: _____

Signature: _____

* Delete which does not apply

Annex 6 - Notifiable Changes

Change	Notify Who	Reason
Any personal data including forename or surname, marital status, home address, bank details, emergency contacts, leave pension scheme, etc.	HR Officer	To allow SPSO records to be updated and for the information to be passed onto appropriate contact, for example, payroll and pensions.
Pregnancy or Adoption of children	HR Officer	For health and safety purposes and to arrange leave.

Annex 7 - Personal Information – strictly confidential

Title:

Forenames:

Surname:

Date of Birth:

National Insurance number:

Home Address:

Postcode:

Home Phone number:

Mobile Phone number:

Name of person to contact in an emergency situation:

Contact address for this person:

Contact phone number/s:

Relationship of this person to you:

Name of Bank or Building Society:

Sort Code:

Account number:

This is an accurate record of my personal details.

Signature: Date:

Annex 7a - SPSO Managing Personal Data Policy

In compliance with the Data Protection Code part 2 Employment Records, personal data that may change, for example, home address will be sent annually to each member of staff for verification or amendment. It is the responsibility of individual members of staff to notify such changes to the HR Officer.

Staff are reminded of their right to access their records (subject to certain exceptions as detailed in section 7 of the Data Protection Act 1998) and the SPSO is under an obligation to ensure that the data is accurate. Before releasing such data to a third party the SPSO will seek the permission of the individual concerned.

Permissions

The SPSO uses information reported on sickness absence to monitor sickness absence levels across the office at individual and team level. All staff are asked to give their permission for information on their absence to be held individually by the SPSO, in compliance with the Data Protection Act 1998.

I agree to this information being held for this purpose by the SPSO.

Signature.....Date.....

In exceptional circumstances a member of the HR team may wish to contact you at your home or on your mobile phone.

I agree that the office may contact me using this information.

Signature.....Date.....

Please confirm below the number and arrangement of hours that you currently work daily:

	Monday	Tuesday	Wednesday	Thursday	Friday	Total
No. of hours (for example, 3.5)						
Hours worked (for example, 09:00 to 12:30)						

[Back to the main Contents Page](#)

8. SPSO Complying with Information Legislation

Contents

Requests for Information	3
Initial Handling and Recording Information Requests	4
Information Request Flowchart	4
Freedom of Information (Scotland) Act 2002	4
<i>Scottish Information Commissioner</i>	4
<i>Publication Scheme</i>	4
<i>Requests for Information</i>	5
<i>Advice and Assistance</i>	5
<i>Responding to a Request</i>	6
<i>Charging</i>	7
<i>Common Requests for Information</i>	7
<i>Exemptions</i>	8
<i>Formatting Information</i>	10
<i>Rights of Review</i>	10
<i>Rights of Appeal</i>	10
<i>Offences under the FOISA</i>	10
Environmental Information (Scotland) Regulations 2004	11
<i>Charging</i>	11
<i>Rights of Review</i>	11
<i>Rights of Appeal</i>	11
Data Protection Act 1998	11
<i>The Information Commissioner's Office (ICO)</i>	11
<i>Personal Data</i>	12
<i>Data Controller</i>	12
<i>Processing</i>	12
<i>Notification</i>	12
<i>Data Protection Principles</i>	12
<i>Correcting Information</i>	12
<i>Preventing Processing of Information</i>	13
<i>Retention of Data</i>	13
<i>Protecting Personal Data</i>	13
<i>Emergency Protocol for Security and Data Breaches</i>	13
<i>Information Commissioner UK (ICO)</i>	14
<i>Data Protection Audit</i>	14
<i>Offences under the DPA</i>	14
Processing Subject Access Requests.....	14
<i>Subject Access Appeal</i>	16
<i>How to deal with specific types of requests</i>	16
External Guidance.....	17
Annex 1 Information Request Flowchart	18

[Back to the main Contents Page](#)

Requests for Information

The SPSO is considered a Scottish public authority under the Freedom of Information (Scotland) Act 2002 (FOISA), Environmental Information (Scotland) Regulations 2004 (EIR) and the Data Protection Act 1998 (DPA). As such, we must always ensure that we respond to all requests for information in accordance with the statutory requirements of these Acts.

Requests to the SPSO for information held (or believed to be held) by the SPSO must be in writing or some other permanent format. The SPSO have a statutory duty to acknowledge all information requests within three working days, and this acknowledgment must state the Act under which the request will be dealt with. Therefore, to enable the Corporate Information Governance Officer to meet this statutory requirement it is imperative that all Information Requests are passed to the Corporate Information Governance Officer immediately on receipt.

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

Under the SPSOA, Section 12 states that the procedure for conducting the investigation and obtaining information is to be such as the Ombudsman thinks fit. Our legislation states that 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 this information under FOISA is not one of those circumstances. Therefore, this information is exempt from being released under regulation 10(5)(d) of the EIR and section 26 (a) of FOISA, which is an absolute exemption, therefore we do not need to consider the public interest test. However, they have a right to request information that we hold about them under the DPA. In light of our duty to provide requesters with advice and assistance, we will consider the request as a subject access request under the DPA.

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 the DPA; 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.

The Complaints Reviewer should obtain consent from the complainant before any information that the complainant has provided is shared with the listed authority. 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.

For file management see [Section F1](#) of the SPSO Complaints Handling Guidance

Verbal Requests

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, DPA and the EIR will apply. This should certainly be discussed with the requester where there is any doubt whether all the information can be provided.

Initial Handling and Recording Information Requests

Information requests may come in by post, ask@ or by our online request form, via the front office or direct to SPSO staff. All staff should deal with straightforward information requests as far as they can. Where they are unable to deal with the request, they will pass it on to the Corporate Information Governance Officer.

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.

The person dealing with the request for information is responsible for recording the request on Workpro as soon as the request is received.

Setting up a new case:

- Create a new case on WorkPro choosing case type FOI/DP/EIR. The person dealing with the request is the Case Owner.
- All known contact/applicant details should be entered into the record and saved.
- The type of request, i.e. FOI or DP or EIR, should be selected from the dropdown list, and the request receipt date and request details entered. Refresh the target date if necessary.
- 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.
- Link the case to any other related case records.
- 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 be used when dealing with information requests.
- When closing the case, the response date, response details, and exemptions should be entered, along with an estimate of the time taken in minutes.

Information Request Flowchart

See flowchart at the end of this [section](#).

Freedom of Information (Scotland) Act 2002

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

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

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:

- Class 1: About us
- Class 2: How we deliver our functions and services
- Class 3: How we take decisions and what we have decided
- Class 4: What we spend and how we spend it
- Class 5: How we manage our human, physical and information resources
- Class 6: How we procure goods and services from external providers
- Class 7: How we are performing
- Class 8: Our commercial publications

Requests for Information

Identity of the Requester

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.

Section 8 of the Freedom of Information (Scotland) Act 2002 requires that when making a request for information an applicant must provide his or her name, together with an address for correspondence. While the Scottish Information Commissioner deems that an email address is sufficient for the purposes of the FOISA, the Commissioner has issued guidance which states that an applicant must provide his or her own name and address when making a request. 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

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

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

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

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

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

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.

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:

- do not hold the information requested (section 17 of the FOISA)
- information is covered by an exemption
- excessive cost of compliance exceeds £600 (section 12 of the FOISA)
- vexatious or repeated request (section 14 of the FOISA)

Information Not Held

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 Director.

Information Held

If the information cannot be supplied straight away, an acknowledgement should be sent to the requester within three working days.

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, H and G drives, individual outlook boxes, 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.

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.

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.

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.

If a request is being dealt with by somebody other than the Corporate Information Governance Officer, draft refusal responses should be forwarded, along with the information that is to be withheld or redacted, to the Corporate Information Governance Officer for approval 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.

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 Director at the SPSO.

Charging

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](#).

We cannot take account of costs incurred in determining whether information is held, or whether the requester is entitled to receive it.

- The estimate of staff costs cannot exceed £15 per hour.
- 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).
- 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.
- In all cases where fees are applied, a fees notice must be issued and must detail how projected costs were calculated.
- 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.

Common Requests for Information

Requests for Qualifications and Experience

The SPSO Job Descriptions and Person Specifications contain this information.

Requests for Names and Qualifications of Advisers

Normally we will 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. All SPSO advisers should be made aware of our position on release of this information. PHSO adviser biographical information should be edited down to clinical qualifications etc. PHSO advisers are aware that they will be named in reports and are used to their details being requested. It is good practice to contact the adviser before releasing the information.

Requests for SPSO Processes or Policies

If someone requests information which we already have in printed form, or available on our website, this can be sent directly. This does not need to be dealt with under the FOISA, although we should try to respond within 20 working days in case of appeal to the SIC.

Requests for Statistics

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 Information Analyst will collect the relevant information and the Corporate Information Governance Officer will respond to the request.

Requests for Legal Advice

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.

Exemptions

Absolute Exemptions

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 the DPA.

Qualified Exemptions

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

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'

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' (absolute)

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

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

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 the DPA (subject access request – deal with under the DPA); or (b) it constitutes 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; or

the requester is the data subject but the information is exempt from release to them under Part IV of the DPA.

Key Exemptions - qualified

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

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'

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'

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'

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

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

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 the DPA. 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.

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.

There are a number of ways in which it may be possible to identify individual requests as being vexatious, notably:

- 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.
- 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.
- 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.

- 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.

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.

Formatting Information

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.

Rights of Review

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).

Requesters must be advised to:

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

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.

Rights of Appeal

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.

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

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

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

The SPSO can charge a 'reasonable amount' under the EIR for environmental information.

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.

Rights of Review

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).

Requesters must be advised to:

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

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.

Rights of Appeal

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.

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.

Data Protection Act 1998

Access to personal information is governed by the Data Protection Act 1998 (DPA), which is enforced and promoted by the UK Information Commissioner.

The Information Commissioner's Office (ICO)

The SPSO is legally obliged to protect any personal information that we hold, and we are required to register 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 the DPA and our responsibilities can be found on the ICO website at www.ico.gov.uk, which should be the main point of reference. This SPSO document is not intended to be used in place of the ICO guidance, and will not repeat that guidance in detail.

Personal Data

Section 1 of the Data Protection Act 1998 (DPA) defines personal data as information relating to a living individual who can be identified either from the data or from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

Data Controller

Section 1(1) of the DPA defines a data controller as 'a person who (either alone or jointly or in common with other persons) determines the purpose for which and the manner in which any personal data are, or are to be, processed'.

Processing

Section 1(1) of the DPA defines processing, which means obtaining, recording, or holding the information or carrying out any operation or set of operations on it, including:

- Organisation, adaptation or alteration
- Retrieval, consultation or use
- Disclosure by transmission, dissemination or otherwise making available
- Alignment, combination, blocking, erasure or destruction

Notification

The ICO maintains a public register of data controllers. Notification is the process by which a data controller's details are added to the register.

Data Protection Principles

The DPA 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 eight principles, which make sure that it is:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate and up to date
- not kept for longer than is necessary
- processed in line with individuals' rights
- secure
- not transferred to other countries without adequate protection

The second area covered by the DPA gives individuals important rights, including the right to know what information is held about them and the right to correct information that is wrong.

Correcting Information

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.

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.

Information standards, principle 4 covers the accuracy of personal data. The Data Protection Act 1998 imposes obligations on us to ensure the accuracy of the personal data we process.

We must comply with these provisions by:

- Taking reasonable steps to ensure the accuracy of any personal data we obtain
- Ensure that the source of any personal data is clear
- Carefully consider any challenges to the accuracy of information
- Consider whether it is necessary to update the information

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

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 21 days. The SPSO is not always bound to act on the request.

Retention of Data

The fifth data protection principle states that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. Please refer to the SPSO [Retention and Disposal Policy](#).

Protecting Personal Data

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

- do not share passwords
- encrypt any personal information held electronically if it will cause damage or distress if it is lost or stolen
- shred all confidential paper waste
- be wary of people who may try and trick you into giving out personal details; especially be aware of media requests
- carry out any appropriate identity checks before giving out personal details
- be aware that you can be prosecuted if you deliberately give out personal details without permission
- consider whether it is appropriate to leave a message on an answering machine
- only include necessary information in telephone messages
- use a strong password (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
- do not send offensive emails about other people, their private lives or anything else that could bring the SPSO into disrepute
- 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)
- do not open spam, not even to ask for no more mailings. Delete the email
- consider whether the content of emails should be encrypted or password protected
- only include necessary information in emails as they can be released under subject access requests
- make sure you choose the right email address before you press send
- consider asking email recipients to acknowledge receipt of emails
- make sure you use bcc if you do not want to reveal recipients in emails
- be careful; when using group email addresses
- if you send a sensitive email from a secure server (GSI) to an insecure recipient, security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending.

Further guidance on out of office records management and security is at [Section F2](#) of the SPSO Handbook - Complaints Handling Guidance. Please also refer to the [SPSO Clear Desk and Screen Policy](#).

Emergency Protocol for Security and Data Breaches

In the event of an SPSO information security breach and/or files being misplaced or stolen, 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 should be taken:

- the staff member should report the loss to their line manager and the Corporate Information Governance Officer within 24 hours or as soon as is practicably possible thereafter;
- the Corporate Information Governance Officer, or, in their absence, the relevant manager, should record the breach in a central database and is responsible for recording all the actions taken by the SPSO to investigate and conclude the matter; and
- it is good practice to report the breach to the ICO within 24 hours, and thereafter provide a response within 72 hours detailing the steps we have taken.

We will need a strategy for dealing with the breach, including:

- a recovery plan, including damage limitation
- assessing the risks associated with the breach
- informing the appropriate people and organisations that the breach has occurred
- reviewing our response and updating our information security

Important guidance on [data security breach management](#) and [reporting breaches](#) is available on the ICO website.

Information Commissioner UK (ICO)

If an individual believes there has been a breach of the Act they can ask the ICO to assess whether our processing of personal data complies with the Act. The ICO can ask us to take steps to comply with the Act, issue enforcement notices and even impose financial penalties in respect of deliberate or reckless handling of personal data which seriously breaches the Act. The ICO cannot award compensation, only the courts can do this. See also [external guidance](#)

Data Protection Audit

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.

Offences under the DPA

- unlawfully obtaining, disclosing, or procuring the disclosure of personal data;
- selling, or offering to sell, personal data which has been unlawfully obtained;
- processing personal data without notifying the Information Commissioner (and other offences related to notification);
- failing to comply with an enforcement notice or an information notice, or knowingly or recklessly making a false statement in compliance with an information notice;
- obstructing, or failing to give reasonable assistance in, the execution of a search warrant;
- requiring someone, for example during the recruitment process, to exercise their subject access rights to supply certain information (such as records of their criminal convictions), which the person wanting it would not otherwise be entitled to. This offence, known as 'enforced subject access', is not yet in force; and
- the unlawful disclosure of certain information by the Information Commissioner, his staff or agents.

Failure to comply with the data protection principles is not, on its own, a criminal offence.

Processing Subject Access Requests

One of the main rights which the DPA gives to individuals is the right of access to their personal information (section 7 of the DPA). As a data controller, the SPSO is required to respond to Subject Access Request (SAR)'s under the DPA.

Receipt

The request must be in writing. The request does not have to mention the DPA. The requester might just ask for access to personal data/information/files/records. On receipt of the SAR, the

Corporate Information Governance Officer must be advised that it has been received. The Corporate Information Governance Officer will give advice on processing the SAR.

Third Party Consultation

If a request includes information about third parties, public authorities or suppliers to the SPSO, it may be appropriate to seek their comments on disclosure. 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.

Charges

The data controller may charge a fee of £10, unless the information is held in an unstructured filing system, in which case we can charge in line with the [Freedom of Information and Data Protection \(Appropriate Limit and Fees\) Regulations 2004](#). These say, amongst other things, that if the cost of providing the information exceeds £600, we are under no obligation to comply with the request.

Process the Request

The person dealing with the request should check the request to ensure that all of the necessary information has been provided. If all the necessary information is there, an acknowledgement is issued. Where further information is required (such as proof of identity or more details about the information requested), this should be requested straight away.

Verify the Identity of the Requester

The data controller should satisfy himself or herself as to the identity of the person. Where we reasonably require further information in order to confirm the identity of the requester and to locate the information, and we have informed the requester of that requirement, we are not obliged to reply to the request unless we have received that further information. Where requests are made by a third party, we must be satisfied that they are authorised to act on behalf of the individual. It is the third party's responsibility to provide evidence of this entitlement.

Repeat Requests

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.

Start the 40 day count

The data controller has up to 40 calendar days to respond, from the date of receipt of the request, or from receipt of the further information to identify the requester and to locate the requested data (and following receipt of fee if appropriate).

Gather the Information

The Corporate Information Governance Officer dealing with the request will contact any SPSO staff who are likely to hold the personal data and request a full copy.

Ask for Comments

Relevant SPSO staff should be asked for any comments they may have about the 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, but it is for the SPSO to decide what information to release. In the case of medical records, comments must be obtained from the relevant health professionals as soon as possible.

Conjoined Data

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. Information does not have to be released unless it is reasonable to release it, taking into account the tests in section 7(6) of the DPA. 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

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 Corporate Information Governance Officer.

Exemptions

Part IV of the DPA sets out the exemptions which may be used to withhold information from data subjects. Some exemptions to the subject access provisions include:

- confidential references given by the data controller
- information relating to negotiations with the data subject
- legal professional privilege – where confidentiality of information between client and professional legal adviser could be maintained in legal proceedings
- self-incrimination

Respond to the Request

Unless it is clear from the letter of request, the person dealing with the request should establish the preferred method of providing the information. Depending on the sensitivity of the information, it may have to be sent out by courier.

Subject Access Appeal

Individuals can appeal to the ICO if they consider the SPSO has not complied with section 7 of the DPA. If an individual is unhappy with the SPSO response, or the way in which their request has been handled, the matter should firstly be referred to the SPSO Director for further investigation, although the requester does not have to accept this route and may go straight to the ICO. In case of appeal to the ICO, it is SPSO practice to retain all relevant information for six months.

How to deal with specific types of requests

Requests for copies of documents originally sent to us

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 their own information should be handled the same way, we do not need to handle this as a Corporate Information Governance 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

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 consent from the data subject (if possible).

Requests for copies of deceased person's medical records

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

Normally we will release copies of the advice we receive from the advisers when requested, along with the name of the adviser. This should always be referred to the Corporate Information Governance Officer in the first instance.

Requests after a report is laid

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

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 Complaint Reviewers 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 therefore maintain that paragraph (f) of section 5.2.5 of the OA guidance on data protection is relevant here, and consequently, Section 31 of the DPA, and thus 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.

External Guidance

The ICO Guidance

The ICO has developed guidance in conjunction with data protection to assist in complying with their obligations under the DPA. This very useful guidance can be found at:

https://ico.org.uk/media/for-organisations/documents/1607/the_guide_to_data_protection.pdf

The Ombudsman Association Guidance

The Ombudsman Association (OA) has developed guidance in conjunction with complaints handling to assist OA members in complying with their obligations. This very useful guidance can be found at

<http://www.ombudsmanassociation.org/docs/BIOAGoodComplaintHandling.pdf>

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

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

<http://www.gov.scot/About/Information/FOI/Section60Code>.

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

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:

<http://www.gov.scot/About/Information/FOI/Section60Code/s61codeofpractice>

Annex 1 Information Request Flowchart

Request for information received

- Where information can easily be provided these can be dealt with by all staff
- Advice from Corporate Information Governance Officer is available if required
- Regard should be taken of timescales (DPA 40 calendar days, FOISA and EIR 20 working days)
- Complex requests to be passed immediately on receipt to the Corporate Information Governance Officer (to allow an acknowledgement letter to be issued within three working days of request received in line with statutory obligation)

- Requests must be received in writing and provide name and contact address details
- The date requests received, including emails, is the actual date received, even if it is out-with office hours
- If the request is unclear, we must get clarification ASAP (clock starts once clarification received as long as we have not delayed in getting the clarification)
- Bear in mind our duty to advise and assist under section 15 of FOISA and Regulation 9 of the EIR

- If the requestor is clearly making a SAR for personal information log on Workpro as DP request
- mark as 'casework involved'
- link cases with complaint ref number

- If requestor quotes FOI for information from our complaint files, log on Workpro as FOI
- mark as 'casework involved'
- create a SAR IR case
- link cases
- Regards should be taken of who the complainant actually is

- Log as FOI requests on Workpro
- link cases if appropriate

- Acknowledge within three working days as a SAR
- Create file note for complaint file with IR reference number
- Health or social work cases write to Health Board ASAP for comments on release of information to ensure no harm
- Seek advice from appropriate IPA and CR for comments or concerns when considering releasing a copy of an IPA Report
- Copy and check file to remove any conjoined or confidential information etc. and consider DPA exemptions
- Respond (by courier) under DPA within 40 calendar days
- advise of right to request the Director look at the request again
- advise of right to appeal to ICO

- Acknowledge as a SAR
- close the FOI case, explaining s26(a) FOISA (s12 and s19 SPSOA and s38(1)(a) FOISA & advise more beneficial to consider under DPA
- provide details of right to request a review under FOISA
- provide details of right to request an appeal to SIC

- Acknowledge within three working days as a FOI case
- Respond within 20 working days
- provide details of right to request a review
- provide details of right to request an appeal to SIC

Request for review received
(must be made in writing within 40th working day after IR response has been issued)

- DPA**
- Log on Workpro as DP review for the Director
 - Acknowledge (within three working days)
 - Respond within 20 working days
 - provide details of appeal to ICO
 - retain information for six months from date of final decision in case of appeal
 - Log any appeals made to ICO on Workpro

- FOI**
- Log on Workpro as FOI review for the Director
 - Acknowledge (within three working days)
 - Respond within 20 working days
 - provide details of appeal to SIC
 - retain information for six months from date of final decision in case of appeal
 - Log any appeals made to SIC on Workpro

[Back to the main Contents Page](#)

9. SPSO Out-of-Office Records Management and Security Guidance

Contents

For whom is this guidance intended?	2
What is the purpose of this guidance?	2
Why do freedom of information and data protection affect me when I work out of office?	2
How does this affect how I work out of office?	2
How do I decide what security measures I need to take for information I use out of office?	3
Working Out Of Office: Dos and Don'ts	3
Further Guidance	4
Emergency Procedures	5
Reminder Checklist:	5

[Back to the main Contents Page](#)

For whom is this guidance intended?

This guidance is intended for all SPSO staff (and those contracted to provide services to the SPSO) that work out of office, either on an occasional or a regular basis.

What is the purpose of this 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.

Addressing these issues will also help you to comply with the Data Protection Act 1998, the Freedom of Information (Scotland) Act 2002 and the Scottish Public Services Act 2002 confidentiality provisions.

Why do freedom of information and data protection affect me when I work out of office?

The Data Protection Act 1998 and the Freedom of Information (Scotland) Act 2002 apply to all the paper and electronic information that you receive and create as part of your employment/contract with the SPSO, regardless of where you work or store that information.

The Data Protection Act permits people to see information that the SPSO holds about them while the Freedom of Information (Scotland) Act gives people the right to access any other recorded information that the SPSO holds. The Data Protection Act also requires us to hold information about living identifiable individuals for no longer than is necessary, to ensure that information is accurate, and to adopt appropriate security measures for this information to protect it from unauthorised access, amendment or deletion.

We have 40 calendar days to respond to a data protection request and 20 working days for freedom of information request. These deadlines mean that the SPSO must know what information it holds, and must be able to retrieve that information even if key staff are away from the office. The Freedom of Information (Scotland) Act even includes 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.

How does this affect how I work out of office?

The primary copy of SPSO information should not be stored out of office, so SPSO records should be updated as soon as possible with copies of any work that you do out of office. This means that anyone who needs to refer to the records in your absence will be able to access the most up-to-date information. It will also enable the SPSO to respond to any freedom of information or data protection requests for that information without having to ask you to search information you have out of office.

You also need to take reasonable measures to protect the information you take out of office from unauthorised loss, access or amendment. This will enable us to comply with our Data Protection Act obligations and is also in the SPSO's business interests: depending on the nature of the information involved, if someone gained unauthorised access to SPSO information it could cause reputational, commercial or competitive damage to the SPSO. For example, sensitive information about a case might be disclosed inappropriately, causing the complainant distress and in breach of our Act.

A number of secure laptops are available to SPSO staff to enable use of a Broadband connection to work directly from/to the appropriate SPSO server via a Virtual Private Network. This removes the need to take home electronic information or to store it there.

How do I decide what security measures I need to take for information I use out of office?

The paper information you use out of office is most vulnerable to loss or unauthorised access in the following ways:

- as a result of leaving papers in household 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
- as a result of crime, for example, theft of a briefcase
- as a result of loss, particularly on the journey to and from work

The electronic information you work on out of office is vulnerable to loss or unauthorised access or amendment in two ways:

- physically, through the loss, damage or access to the storage medium on which the record is held. This is most likely to happen on the journey to and from work, or as a result of a theft from your home. However, a member of your household might also access information accidentally, for example, if information is stored on a household PC
- remotely, through someone accessing your computer while it is connected to the Internet or through a virus. If you use a broadband connection, whenever your computer is switched on and not only when in use, it is possible for someone to access your computer

When deciding what reasonable security precautions you need to take against these vulnerabilities, it is necessary to balance their financial cost, time and practical implications against the seriousness of the damage that would result if someone did see the information or made unauthorised alterations to it. Depending on the nature of the information, this damage could entail legal action against you or the SPSO; damage to the SPSO's reputation; or damage to collaborative relationships caused by the inappropriate release of information.

For information that is in the public domain or that we would release in its entirety if we were asked for it under a freedom of information request, the risks are low, and so little or no security measures are required. 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. For some information the risks may be so high that it should never be taken out of office. This might include medical information about identifiable patients (where a strong duty of confidentiality applies), or information whose disclosure is forbidden by law.

Thus, there is a risk assessment involved in deciding what measures are required. These considerations can be represented in the following matrix:

<i>High</i>	<i>Medium</i>	<i>Low</i>	<i>Very low</i>
How serious would the consequences be if someone gained unauthorised access to this information?			
How likely is it that someone could gain access to this information?			
What is the cost of the security precautions?			

Working Out Of Office: Dos and Do nots

Extract from the Working at Home Policy:

6. Confidentiality and Security

6.1 Confidentiality and security rules continue to apply to all business conducted on behalf of the SPSO when a staff member is working at home. Official information must not be disclosed to those unauthorised to receive it. As with work in the office, breaches will be dealt with under the SPSO Disciplinary Procedure.

6.3 Staff members are responsible for ensuring the security of the papers and equipment, and that basic levels of security are in place, such as locked windows and doors. Particular care must be taken when confidential papers are being transported to and from home.

DO:

- remember that all work-related documents are SPSO records irrespective of where they are physically stored
- make full use of security features such as encryption and passwords for information stored on removable storage devices such as memory sticks, floppy disks etc.
- notify your team assistant 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
- take a copy of paper files or electronic documents out of office where possible, not the original documents, and only take what is necessary
- in circumstances when it is not possible to take copy documents, discuss additional precautions and risk prevention methods with your line manager. This will include changing the location on WorkPro to 'Home Working' and the dates that the file will not be in the office. If you are not the designated officer, include your name in the additional field
- transport copy paper files and electronic data in an SPSO authorised locked bag to and from the office. Transport any original documents in a fireproof lockable bag. When the documents are not in use, store them in the locked bag until returned to the office
- go directly home and to the office without putting the bag down in any public place. Take extreme care not to misplace SPSO information on the journey to and from work
- take security precautions when working on your private PC, for example, ensure your PC is password protected and work off-line at all times to reduce risk. Save and store work-related information to a removable encrypted storage device such as memory stick, floppy disk etc.
- save any electronic documents produced out of office into the SPSO WorkPro database or common drive as soon as possible
- destroy any SPSO information on removable storage devices once successfully transferred to the office files
- use only your SPSO email accounts for any complaint related business
- copy any other work-related emails sent to or from a personal email account to your SPSO email accounts; then delete from your personal account
- consider whether the content of emails should be encrypted or password protected. If you send a sensitive email from a secure server to an insecure recipient, security will be threatened
- dispose of all confidential paper waste in the confidential waste bins provided in the SPSO office
- keep up-to-date with security patches for your private computer system and applications
- when possible, work directly from/to the appropriate SPSO server via a Virtual Private Network and Broadband or dial in connection

Do not:

- take medical records out of the office
- use your private computer, a moveable storage device or a laptop to store SPSO information
- store SPSO documents at home
- remove documents unless you are sure you can keep them secure
- leave paper or electronic files where they could be accidentally viewed by visitors or family members
- use a personal email account for SPSO complaint business
- take SPSO information with you when visiting public places such as shops, gym, or bar

Further Guidance

It is important to take time to familiarise yourself with the Information Commissioner's guidance for organisations on security measures to protect the personal data you hold, which provides further links to the Commissioner's topic page on encryption and his Good Practice Note on Security of personal information. [Link](#)

Emergency Procedures

In the event of SPSO information being misplaced, take the following action:

- immediately retrace your movements and take all actions possible to retrieve the information
- as soon as possible, call your manager and the FOI/DP Officer and report exactly which information has been misplaced and under what circumstances this came about
- if there has been a theft, notify the police immediately
- it is good practice to notify the body and report the loss to the ICO within 24 hours

Your manager will inform the Ombudsman and Communications Manager who will decide what further appropriate action to take. See Section G for further guidance

Reminder Checklist:

- Copy document where possible
- Lockable bag (fireproof for original docs)
- Password protection
- Notified TA, changed location on WorkPro
- Travel arrangements
- Home storage arrangements

Also, look at the Scottish Government document on keeping information secure.
<http://intranet/InExec/News/Releases/2013/05/29163703>

[Back to the main Contents Page](#)