Scottish Government
Riaghaltas na h-Alba
gov.scot

Scottish Government Records Management Plan

Table of Contents

Records Management Plan 1
About the Public Records (Scotland) Act 2011 1
About the Scottish Government 1
Element 1: Senior management responsibility 3
Element 2: Records manager responsibility: 6
Element 3: Records management policy statement: 7
Element 4: Business classification 9
Element 5: Retention schedules 12
Element 6: Destruction arrangements 14
Element 7: Archiving and transfer arrangements 16
Element 8: Information Security 18
Element 9: Data protection 20
Element 10: Business continuity and vital records 22
Element 11: Audit trail: Tracking and version control 23
Element 12: Records management training for staff 24
Element 13: Assessment and review 26
Element 14: Shared Information 27
Element 15: Public records created or held by third parties 29

Records Management Plan

Summary

The Scottish Government is fully committed to compliance with the requirements of the Public Records (Scotland) Act, which came into force on the 1st January 2013. The Scottish Government will therefore follow procedures that aim to ensure that all employees, contractors, agents, consultants and other trusted third parties who have access to any information held within the Government, are fully aware of and abide by their duties under the Act.

About the Public Records (Scotland) Act 2011

The Public Records (Scotland) Act 2011 (the Act) came into force on the 1st January 2013, and requires the Scottish Government to submit a Records Management Plan (RMP) to be agreed by the Keeper of the Records of Scotland. This document is the Records Management Plan of the Scottish Government and was submitted to the Keeper of the Records of Scotland in February 2021 (our original plan was approved by the Keeper in 2015).

About the Scottish Government

The Scottish Government is the devolved government for Scotland which is responsible for most of the issues of day-to-day concern to the people of Scotland, including health, education, justice, rural affairs, and transport.

The Government's purpose is to focus government and public services on creating a more successful country, with opportunities for all of Scotland to flourish, through increasing sustainable economic growth.

Who is included in the Scottish Government Records Management Plan

The Scottish Government's Records Management Plan includes all Departments covered under the heading of Scottish Ministers. The plan also includes the following Agencies and other bodies who use our Records Management Services:

- Accountant in Bankruptcy
- Chief Dental Officer
- Chief Medical Officer
- Disclosure Scotland
- Drinking Water Quality Regulator for Scotland
- HM Fire Service Inspectorate
- HM Inspectorate of Prisons
- Independent Prison Monitors
- Inspectors of Anatomy
- Mobility and Access Committee for Scotland
- Prison Monitoring Co-ordinators

- Safeguarders Panel
- Scottish Agricultural Wages Board
- Student Awards Agency for Scotland
- Transport Scotland

Review

This plan will be reviewed every year (or sooner if new legislation, codes of practices or national standards are to be introduced) using the Progress Update Review process which was introduced by NRS in 2017.

RMP Element Description

Element 1: Senior management responsibility

An individual senior staff member is identified as holding corporate responsibility for records management.

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.
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.

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).
Best Practice might include:

- Senior management responsibility is recorded in both the RMP and the RM Policy statement (see element 3).
- The post-holder is named in the RMP and confirmed in each report to the Keeper (see element 13).
- The Keeper is promptly advised of any change in post-holder.
- The post-holder should satisfy themselves that they understand their responsibilities.

Read further explanation and guidance about element 1.

Scottish Government Statement

The Director General Corporate Lesley Fraser, has senior responsibility for all aspects of records management, and is the corporate owner of this document.

Lesley Fraser is also the Senior Information Risk Owner (SIRO) for Scottish Government (SG).

The bodies who are named in the act and opted to be included within the Scottish Government plan have all confirmed they use the SG eRDM system for filing information and are happy that our SIRO has signed off the plan.

Evidence	Further Development
E01: SG Records Management policy E02: Data handling -Roles and responsibilities - SIRO E59: Scottish Government Records Management Plan Submission - Chief Medical Officer - Confirmation response E60: Scottish Government Records Management Plan Submission - HM Chief Inspector of Fire and Rescue Authorities and Assistant Inspectors of Fire and Rescue Authorities - Confirmation response E61: Scottish Government Records Management Plan Submission - HM Chief Inspector of Prisons for Scotland - Confirmation response E62: Scottish Government Records Management Plan Submission - HM Inspectorate of Constabulary - Confirmation response E63: Scottish Government Records Management Plan Submission - Scottish Agricultural Wages Board - Confirmation response E64: Scottish Government Records Management Plan Submission - Chief Dental Officer - Confirmation response E67: Scottish Government Records Management Plan Submission - Her Majesty's Inspector of Anatomy for Scotland – Confirmation response E70: Scottish Government Records Management Plan Submission – Safeguarders Panel – Confirmation response	No additional actions have been identified in relation to the Senior management responsibility.

E71: Scottish Government Records Management Plan Submission – Drinking Water Quality Regulator for Scotland – Confirmation response E73: Scottish Government Records Management Plan Submission - Independent Prison Monitors and Prison Monitoring Co-Ordinators – Confirmation response E74: Scottish Government Records Management Plan Submission - Mobility and Access Committee for Scotland - Confirmation response E76: Scottish Government Records Management Plan Submission - Accountant in Bankruptcy – Confirmation response E77: Scottish Government Records Management Plan Submission - Disclosure Scotland - Confirmation response E78: Scottish Government Records Management Plan Submission - Transport Scotland - Confirmation response E79: Scottish Government Records Management Plan Submission – Student Awards Agency for Scotland - Confirmation response	

Element 2: Records manager responsibility:

An individual staff member is identified as holding operational responsibility for records management and has appropriate corporate responsibility, access to resources and skills.

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.

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 a non-records professional member of staff to undertake this task, a framework which allows the authority to develop a training programme for that person will be essential.

It should be noted that staff changes will not invalidate any submitted plan provided that 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.

Best Practice might include:

- Records manager responsibility is recorded in both the RMP and the RM Policy statement (see element 3).

- Evidence can be supplied that the individual identified as having responsibility for the implementation of the RMP can access the relevant training as appropriate. This may take the form of an agreed Personal Development Plan.

- The post-holder is named in the RMP and confirmed in each report to the Keeper (see element 13).
- The Keeper is promptly advised of any change in post-holder.
- The post-holder should satisfy themselves that they understand their responsibilities (see element 12).

Read further explanation and guidance about element 2.

Scottish Government Statement

Our existing records management policies have Craig Sclater (Scottish Government Corporate Records Manager) as having day to day operational responsibility for records management. Craig reports to Pauline Travers, Head of Information Services Operations.

Overall responsibility for Records Management sits with our Senior Information Risk Officer (SIRO) Lesley Fraser.

Evidence	Further Development
E01: Records Management Policy	No additional actions have been identified in relation to Records Manager responsibility.

Element 3: Records management policy statement:

The authority has an appropriate policy statement on records management.

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. 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 appropriate safe and secure storage of digital records and for any migration or transformation of digital records if they are moved from one system to another.

The records management statement should include a description of the mechanism for records management issues being disseminated through the authority and confirmation that regular reporting on these issues is made to the main governance bodies.

The statement should have senior management approval and evidence, such as a minute of the management board recording its approval, submitted to the Keeper.

The other elements in the RMP, listed below, will help provide the Keeper with evidence that the authority is fulfilling its policy.

Best Practice might include:

- The Policy Statement (Policy) sets out how the authority will manage its records in accordance with its Records Management Plan.
- The Policy includes provision for the lawful management of records that include personal data.
- The Policy includes a statement of the named posts that hold corporate and operational responsibility for records management (see element 1 and element 2).
- The Policy is regularly reviewed.

Read further explanation and guidance about element 3.

Scottish Government Statement

We have a strong Records Management policy in place which details the record keeping arrangements for Scottish Government.

Scottish Government is committed to a systematic and planned approach to the management of records within the organisation, from their creation to their ultimate disposal or archive. This approach ensures that Scottish Government can:

- control the quality, quantity and security of the information that it generates;
- maintain the information in an effective manner whilst ensuring compliance with our legislative requirements.

It has been approved by the SG Senior Information Risk Owner.

Evidence	Further Development
E01: Records Management Policy	We are in the process of developing an Information Management strategy which will complement the information provided in our Records Management policy. We plan to finalise this strategy in 2021. Other than that we will continue to review our Records Management policy regularly in order to ensure that it continues to reflect the organisational position in relation to record keeping.

Element 4: Business classification

Records are known and are identified within a structure, ideally founded on function.

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, information asset register or similar.

This should record, at a given point in time, the information assets the business creates and maintains, and in which function or service area they are held. As authorities change, the structure should be regularly reviewed and updated.

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

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

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

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

An authority will need to demonstrate that its chosen structure can be applied to the record systems which it operates.

Best Practice might include:

- Business classification is recorded within a business classification scheme, a file plan or an information asset register.
- The structure includes all records and information held by the authority regardless of format (physical or digital).
- In particular, the structure should identify the systems and records that contain personal data.
- The structure also covers any functions which are contracted to third parties and the authority recognises its responsibility to satisfy itself that the records produced by these functions are robustly managed and revert to the authority at the end of the contract (see element 15).
- The arrangement is periodically reviewed (see element 13).

Read further explanation and guidance about element 4.

Scottish Government Statement

Our Business Classification Scheme is the keystone of the records management function within Scottish Government. The Business Classification Scheme aims to provide the framework for managing the records and information.

The Business Classification Scheme has been adapted from the Integrated Public Sector Vocabulary (IPSV) and Government Category List. The scheme has four levels of classification, the first three levels are subject based and the fourth level describes the activity undertaken.

Every file that is created has a file type attached to it. The file type determines when the file will be closed and the action that will be taken on the file following closure.

Extracts of eRDM files created for those bodies who have elected to be part of the SG file plan have been provided to show where they sit in the structure.

Evidence	Further Development
E03: SG Business Classification E04: Scottish Government File type guidance E05: Scottish Government Casework File type guidance	No changes will be made to our Business Classification Scheme at the current time but we will continue to review it on an annual basis.

E48: Extract of Chief Dental Officer file in eRDM E49: Extract of Chief Medical Officer file in eRDM E50: Extract of Scottish Agricultural Wages Board file in eRDM E51: Extract of Transport Scotland file in eRDM E52: Extract of Student Awards Agency for Scotland file in eRDM E53: Extract of a Legal Secretariat for the Advocate General file in eRDM E54: Extract of HM Inspectorate of Anatomy file in eRDM E55: Extract of a HM Inspectorate of Constabulary file in eRDM E56: Extract of a Legal Secretariat of the Lord Advocate in eRDM E65: Scottish Government Fileplan Level 1 to 3 E68: Extract of a Safeguarders Panel file in eRDM E69: Extract of a Drinking Water Quality Regulator for Scotland file in eRDM	

Element 5: Retention schedules

Records are retained and disposed of in accordance with the Retention Schedule.

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

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

The principal reasons for creating retention schedules are:

- to ensure records are kept for as long as they are needed and then disposed of appropriately.
- to ensure all legitimate considerations and future uses are considered in reaching the final decision.
- to provide clarity as to which records are currently held by an authority and which have been disposed of.

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

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

An authority's RMP must demonstrate the principle that retention rules are consistently applied across all of an authority's record systems. Best Practice might include:

- The Retention Schedule is arranged in accordance with business classification (see element 4).
- The Schedule is developed to comply with relevant legislation and statutory regulation.
- The Schedule identifies records of enduring value following professional archival advice and enables these to be selected in collaboration with the authority's archive provider.

- The Schedule identifies how long records are to be retained, which records require review for business and/or archival purposes and what their eventual disposition is to be.
- The Schedule is developed and reviewed to ensure compliance with data protection principles, and in particular the storage limitation principle.
- Business requirement is determined by the relevant business area.
- The Schedule is reviewed periodically (see element 13).

Read further explanation and guidance about element 5.

Scottish Government Statement

Scottish Government has a detailed retention and disposal policy. This is based on the key record types held by the organisation and their required retention periods which are in line with statutory and legislative obligations and business needs.

The retention and disposal schedules have been mapped to file types which are then used against the files created within eRDM. These are the standard retention schedules that all bodies covered by the SG plan use.

A standard records schedule is used for the retention and disposal of our legacy paper files.

Before the introduction of eRDM Divisions and Branches in SG could also draw up their own Branch/Divisional specific retention schedule to help the SG review team. These are still used to review pre-eRDM records.

At the moment we do not use retention and disposal schedules on shared drives, pst files and public folders. We plan to re-commence our project to review material in these locations and arrange for the material to be disposed of/added to eRDM in line with agreed retention schedules. A copy of the original policy document relating to the SG archival policy for shared drives is attached.

Evidence	Further Development
E04: Scottish Government File type guidance E05: Scottish Government Casework File type guidance E06: Scottish Government Paper Records Retention Schedule pre-eRDM	We will continue to review our retention and disposal schedules to make sure they continue to meet business needs.

E07: Example of branch own retention schedule E36: Scottish Government Archival Project – Analysis and Interim Progress Report E37: Scottish Government Archival Project – Project Mandate/PID E57: Scottish Government Archival Policy for Shared Drives	

Element 6: Destruction arrangements

Records are destroyed in a timely and appropriate manner and records of their destruction are maintained.

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.

An authority's RMP must demonstrate that proper destruction arrangements are in place.

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.

In particular an authority should be confident that it maintains controlled destruction, when appropriate, of digital records held on remote or standalone systems and mobile devices. Furthermore, an authority must understand the availability and accessibility of digital records held as continuity backups and the destruction cycles of such backups.

Best Practice might include:

- Destruction is in accordance with the retention schedule.
- Destruction is systematic.
- Records of destruction are created and retained in accordance with the authority's retention schedule.
- Special provision is made for confidential paper waste.

- Special provision is made for the assured destruction of sensitive digital records.
- Arrangements cover the assured secure destruction of hardware and back-up media used to store digital records.
- Arrangements are reviewed periodically (see element 13).The destruction of personal data is in accordance with data protection law.

Read further explanation and guidance about element 6.

Scottish Government Statement

All paper records are subject to secure disposal under contract to Shred-It:

- The contract details ISO accreditation, insurance certificate and employer's liability.
- Shred-It dispose of confidential documents directly from offices.

  Click to go to the Shred-It site
- Scottish Government has implemented retention schedules on all electronic records and regularly review these.
- When an electronic file is destroyed or transferred to National Records of Scotland in line with its retention schedule stubs remain on the system confirming the name of the file and all documents that were held within it.

Computer media is disposed of securely and through approved procedures.

Evidence	Further Development
E04: Scottish Government File type guidance E05: Scottish Government Casework File type guidance E08: Shredit Certificate of destruction E09: Screenshot of a destroyed file on eRDM E39: SCOTS Back up and Destruction procedures E47: Certificate of Destruction Saughton House	No further development is required at the moment but we will keep this under review.

Element 7: Archiving and transfer arrangements

Records that have enduring value are permanently retained and made accessible in accordance with the Keeper's 'Supplementary Guidance on Proper Arrangements for Archiving Public Documents'.

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.

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 service responsible for the archive should be cited.

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.

Best Practice might include:

- The authority has access to professional archival advice in identifying records of enduring value.
- Archive selection is in accordance with the retention schedule and is format neutral.
- Selection is systematic.
- The authority is satisfied that the process of transfer ensures the security of the records, that the records are not corrupted in transit (especially in the case of digital records), and the correct records are transferred and received.
- The authority can confirm that the archives repository has appropriate staff, security and storage to meet the Keeper's requirement.
- The authority is satisfied that the arrangements for public access to their records is in accordance with access to information legislation and regulation.
- The authority is satisfied that access to archive records that include personal data (data relating to living individuals) is in accordance with data protection law.

Read further explanation and guidance about element 7.

Scottish Government Statement

Scottish Government records which are identified as being of historical interest are transferred to the National Records of Scotland for permanent preservation.

There is a formal Service Level Agreement between Scottish Government and the National Records of Scotland which covers the transfer of all records.

Scottish Government use Enterprise Vault to archive emails from all employees mailboxes.

We plan to re-commence our project to review material in shared drives, pst files and public folders and will arrange for the material to be disposed/added to eRDM in line with agreed retention schedules. A copy of the original policy document relating to the SG archival policy for shared drives is attached.

We are progressing the digitising of our legacy paper files in line with the Digital First Agenda.

Evidence	Further Development
E10: NRS selection policy E11: SG iTECS-NRS Service Level Agreement E27: NRS Depositor Guidance for the Transfer of Archival Born Digital Records E35: Scottish Government Email Archiving E36: Scottish Government Archival Project - Analysis and Interim Progress Report E37: Scottish Government Archival Project - Project Mandate/PID E57: Scottish Government Archival Policy for Shared Drives E72: Digitisation of Legacy Paper Files	We will maintain regular contact with NRS with regards to record transfers. We will adhere to any updates to the NRS Depositor Guidance for the Transfer of Archival Born Digital Records when transferring electronic records to NRS. The NRS selection policy and SG iTECS-NRS Service Level Agreement will be reviewed and updated in 2021 in conjunction with NRS. The Scottish Government Archival project has been on hold for a period of time but will be progressed again in 2021. We will continue to digitise our legacy paper records in order to meet with our "digital first" policy.

Element 8: Information Security

Records are held in accordance with information security compliance requirements.

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

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

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

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 physical records should not allow large changes in temperature or excess humidity (as increased high temperatures and humidity are more likely to cause mould). If physical 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.

Best Practice might include:

- Information security provision is adequate to meet all relevant information security compliance requirements.
- Appropriate security measures are in place to protect records involving personal data and ensure compliance with the integrity and confidentiality principle.

Read further explanation and guidance about element 8.

Scottish Government Statement

Scottish Government has a number of well-established information security policies and procedures which all staff are required to comply with. The policies are approved and reviewed on a regular basis.

Scottish Government is pro-active in its approach to information risk through the corporate risk register.

All Information Asset Owners (IAOs) are briefed and provided with guidance on their role.

All staff are required to complete "Responsible for Information – General User'" and "Data Protection" e-learning training on an annual basis. This annual awareness training reminds employees of the importance of data security and associated risks.

Scottish Government ensure that adequate physical controls are put in place to maintain the security and confidentiality of all business sensitive data whether held manually or electronically.

Evidence	Further Development
E12: SG Information Security Policy Statement E13: SG Data Handling Standard E14: SG Clear Desk Policy E15: SG Risk Management Guide E16: SG Risk Strategy and Policy E17: Information Asset Owner Handbook E18: Scottish Government IT Security Policy E19: Scottish Government Information Risk Management Appetite Statement E20: Restricting files and documents in eRDM – use of security groups	These policies will continue to be reviewed regularly and updated as required.

E33: Scottish Government eRDM Document Restrictions E38: Scottish Government IT Code of Conduct	

Element 9: Data protection

Records involving personal data are managed in compliance with data protection law.

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

If an authority holds and processes personal data about stakeholders, clients, employees or suppliers, it is legally obliged to protect that information. Under data protection law 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, historical or research purposes and only for as long as is set out on an agreed retention schedule. The person who is the subject of the information must be afforded access to it on request, unless an exemption applies.

Best Practice might include:

- The authority has appointed a Data Protection Officer.
- The authority demonstrates compliance with the accountability principle.
- The authority maintains records of processing activities appropriate to the authority's size.
- The authority has put in place appropriate technical and organisational measures to meet accountability requirements - for example, a data protection policy has been implemented, a data protection officer has been appointed, data breaches are recorded, data protection impact assessments are carried out.
- The authority is transparent about processing of personal data and enables individuals to determine what information the authority holds about them, how it is used, how long it is held and how they can exercise their rights.

Read further explanation and guidance about element 9.

Scottish Government Statement

Scottish Government has wide ranging data protection controls in place including high-level procedures, mandatory staff data protection e-learning training and guidance for specific activities.

Our Data Protection Policy is a statement of public responsibility and demonstrates our commitment to compliance with the Act and the safeguarding and fair processing of all personal data held by SG.

All staff of organisations who are part of the SG file plan are required to complete the "Responsible for Information – General User'" and "Data Protection" e-learning courses on an annual basis and obtain a pass mark.

All the non-ministerial bodies covered by the SG file plan fall under the SG Data Protection registration under their Director General name. Screenshots have been provided to show which Director General (DG) they fall under.

Evidence	Further Development
E21: SG Data Protection ICO notification E22: SG Data Protection Policy E23: SG Data Sharing Template and Guidance – Non-Personal data E24: SG Data Sharing Template and Guidance – Personal data E25: Managing Information E26: SG Subject Access – Guidance E58: Director General Screen Shots for Data Protection Registration	Staff will continue to undertake the "Responsible for Information – General User'" and "Data Protection" e-learning courses on an annual basis and be required to obtain a pass mark.

Element 10: Business continuity and vital records

Record recovery, prioritising vital records, is an integral part of the authority's business continuity planning.

An authority's business continuity arrangements should include the recovery of records made temporarily unavailable due to an unexpected event.

Current data protection law emphasises that the loss of personal data may constitute a breach.

In particular, the Keeper will expect an authority's RMP to indicate arrangements in support of records vital to core business activities. 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.

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.

Best Practice might include:

- An authority's business continuity arrangements should recognise the importance of the recovery of records.
- Vital records are identified, perhaps as part of an Information Asset Register (see element 4), and the mechanisms for their protection and recovery included within the authority's Business Continuity Planning.
- Arrangements are in place within the Plan that ensures that copies of vital records will both survive envisaged incidents and be available thereafter in accordance with defined criteria.
- Arrangements are in place to ensure the ongoing confidentiality, integrity, availability and resilience of records involving personal data.
- The authority's business continuity arrangements are reviewed regularly.

Read further explanation and guidance about element 10.

Scottish Government Statement

Scottish Government has a number of Business Continuity and disaster recovery plans in place.

All records and data held on the Scottish Government network are subject to regular back up and associated recovery procedures.

Evidence	Further Development
E28: eRDM Business Continuity Plan E39: SCOTS Back up and Destruction procedures	Business Continuity Plans will continue to be reviewed regularly.

Element 11: Audit trail: Tracking and version control

The location of records is known and changes recorded.

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.

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.

Best Practice might include:

- When a physical record is removed from storage, its location is known.
- Records of physical record movements are made and retained.
- Version control is in place.
- Logs of digital record movements and amendments are maintained and are available.

Read further explanation and guidance about element 11.

Scottish Government Statement

The eRDM system provides an audit trail which evidences when a specific user has viewed, modified or deleted any information held in eRDM.

Paper records are identified within the Legacy Paper File database. The database tracks the movement (including those passed to NRS for permanent preservation) and destruction of files. As mentioned previously we are in the progress of digitising our legacy paper records which will allow us to capture them in eRDM. This will ease access to files and vastly reduce the storage space required to hold our legacy material prior to its destruction/transfer to National Records of Scotland in line with the arrangements in our Records Management Plan.

Evidence	Further Development
E11: SG iTECS-NRS Service Level Agreement E29: SG Audit Trail E34: Extract from Legacy Paper Filing system	No further development is required at the moment but we will keep this under review.

Element 12: Records management training for staff

Staff creating, or otherwise processing records, are appropriately trained and supported.

The RMP must be adhered to by all staff in an authority. The Keeper will expect an authority's RMP to detail how the day-to-day operation of activities described in the elements in the authority's RMP are explained to the staff who will be required to carry them out. It is important that authorities recognise that records management processes are likely to be implemented by staff in various roles and business areas out-with the immediate information governance officers. These staff members must be trained and supported accordingly. Guidance should be made available.

The level of training required by staff will vary considerably depending on their role.

Staff processing personal data will require particular training in the handling of those categories of record.

It is important that there is a mechanism in an authority that will allow staff to be alerted to changes in records management procedure.

Best Practice might include:

- The authority is responsible for identifying the skills and training required for staff engaged in records processing.
- Staff across the authority engaged in records processing activities are given regular training and development so that they understand their records management responsibilities.
- The operation of the authority's records management processes should be included at induction.
- Staff engaged in activities that include records with personal data are trained so that they understand their responsibilities under data protection law.
- Any professional record-keeping staff are supported to maintain involvement in Continuous Professional Development schemes.

- Training for staff who use records is refreshed periodically.
- A record is made of staff who have completed records management training.

Read further explanation and guidance about element 12.

Scottish Government Statement

Core competencies, key knowledge and skills required by staff with responsibilities for Records Management have been clearly defined within the Records Management Competency Framework. This ensures that staff understand their roles and responsibilities and can offer expert advice and guidance. The framework has identified that the Corporate Records Manager will be professionally qualified in information/records management or working towards such a professional qualification. We will also endeavour to have all staff in our Records Management team undertake appropriate records management courses to enhance their knowledge and understanding of the subject.

On an annual basis staff must complete the "Responsible for Information – General User'" and "Data Protection" e-learning courses and obtain a pass mark.

eRDM Training is mandatory for all staff before they get access to the system. Non completion of training means no access to the system.

E25: Managing Information E30: Records Management Competency Framework E32: eRDM Browser - Functionality handbook	Identify appropriate training for all members of the Records Management team and arrange attendance at training courses. We have introduced more content relating to the Public Records (Scotland) Act into the training and guidance we supply to SG colleagues. We will look to continue to develop this material going forward.

Element 13: Assessment and review

Records Management arrangements are regularly and systematically reviewed with actions taken when required.

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.

It is important that an authority's RMP is 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.

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.

Best Practice might include:

- The authority's procedure for assessing and reviewing its records management plan are recorded within the RMP.
- Timely and effective actions are taken to address issues raised by the review.
- The authority reports regularly to the person named at element 1 on progress/review of its RMP.
- The authority can explain the following to the Keeper: When the review is scheduled, who is responsible for carrying out the review, the methodology that will be used and how the results of the review will be reported up through the authority's governance structure.

Read further explanation and guidance about element 13.

Scottish Government Statement

Each of the policies and procedures produced in line with the requirements of the Public Records (Scotland) Act 2011 have been created in consultation with colleagues across the organisation.

Each policy has been reviewed in detail in order to ensure compliance with all business and legal obligations.

The Corporate Records Manager will be responsible for overseeing the Records Management Plan and making sure that the supporting documentation is kept up to date. They will update content that falls under their responsibility or ask the relevant business area to update content owned by other business areas.

We are committed to completing the Records Management Plan Progress Update Review on an annual basis (excluding years we are required to re-submit our Records Management Plan to the Keeper of the Records for approval). The outcome of these reviews will be reported to the iTECS Senior Leadership Team and the Senior Information Risk Owner in order that they are aware of progress which has been made and weaknesses that require to be addressed.

Evidence	Further Development
E66: Scottish Government Assessment and Review Process E75: Progress Update Review 2019	All policies and procedures will be reviewed annually to ensure the Records Management Plan is kept up to date. The Records Management Plan will also be reviewed if we replace or upgrade the eRDM system which has been installed within Scottish Government.

Element 14: Shared Information

Information sharing, both within the Authority and with other bodies or individuals, is necessary, lawful and controlled.

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. An authority's arrangements must, for example, take data protection into account and demonstrate robust arrangements for the safe and secure sharing of personal sensitive data.

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

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

Issues critical to the good governance of shared information should be clearly set out among parties at the earliest practical stage of the information sharing process. This governance should address accuracy, retention and ownership. The data sharing

element of an authority's RMP should explain review procedures, particularly as a response to new legislation.

Best Practice might include:

- The need for, and lawfulness of proposed information sharing, is established before the information is shared.
- Information sharing is documented. This can be by means of an information sharing agreement (ISP) or on an instance by instance basis as appropriate.
- A log of information sharing is retained.
- Information sharing is secure.
- Where personal data is shared, consideration is given to the need for a data protection impact assessment, and any transparency requirements for data subjects.

Read further explanation and guidance about element 14.

Scottish Government Statement

Scottish Government shares data in accordance with Data Protection regulations and the Freedom of Information (Scotland) Act. The organisation has a guide to information approved by the Scottish Information Commissioner. This outlines and links to the information the organisation will routinely publish and make available.

In addition to completing the "Responsible for Information – General User" e-learning course on an annual basis, all staff are provided with guidance concerning the procedures and considerations for electronic and hard copy distribution of information.

Standard data sharing templates are available for staff to use in order to reflect the specific requirements and circumstances for sharing information.

Evidence	Further Development
E20: Restricting files and documents in eRDM – use of security groups E23: SG Data Sharing Template and Guidance – Non-Personal data E24: SG Data Sharing Template and Guidance – Personal data	No further development at this time.

E31: Security Classifications E46: Data Sharing Agreement - Between Scottish Government and Fire and Rescue Service	

Element 15: Public records created or held by third parties

Adequate arrangements must be in place for the management of records created and held by third parties who carry out any functions of the authority.

Section 3 of the Act describes the meaning of 'public records' for the purposes of the Act. It says that public records in relation to a named authority means records created by or on behalf of the authority in carrying out its functions. This is extended to records created by or on behalf of a contractor carrying out the authority's functions and includes records that have come into the possession of the authority or contractor in carrying out the authority's functions. Records created or held by a third party contractor that are not done so in relation to that contractor carrying out the function of the public authority are not public records under the Act.

An authority's plan must include reference as to what public records are being created and held by a third party carrying out a function of the authority and how these are being managed to the satisfaction of the authority. This does not mean the authority must impose its own arrangements on the third party.

Authorities should take a risk-based approach to the arrangements it puts in place with third parties to ensure that these are relevant and proportionate to the public records that fall within the scope of each contract type. Records management requirements, and evidence of assurance that prospective contractors will be able to meet these, should be included in the procurement exercise.

An authority will wish to ensure the scope of its proposed arrangements include sub-contractors. It will further wish to ensure that arrangements are in place to allow it to meet statutory obligations under other information legislation, for example, to FOI(S)A and data protection legislation (see Element 9). There may be other regulatory obligations that an authority will wish to consider in relation to the function being carried out by the third party.

Best practice might include:

- An authority will set out arrangements for managing public records created and maintained by a third party provider through the provision of adequate records management contractual clauses and monitoring procedures.

- Arrangements under procurement documentation and contractual clauses will reference contract monitoring and "end-of-contract" procedures for public records being created and maintained by third parties.
- Arrangements will provide for proper retention and disposal of public records throughout the duration of the contract.
- The authority and the third party will have a clear understanding of the public records that fall within the scope of the contract.
- An authority will be able to demonstrate its satisfaction to the Keeper that corporate and operational responsibility for records management within the third party is robust.
- Arrangements will provide for public records of enduring value and public records with on-going business value reverting to the authority on conclusion of the contract or where the third party falls.
- An authority will be satisfied that the third party keeps its records management arrangements under review.
- A public authority can demonstrate that contractors have had regard to the Guidelines for Contractors as part of the procurement exercise.

Read further explanation and guidance about element 15

Scottish Government Statement

The Scottish Government contract some of their functions to third parties. Contracts which contain details of what should happen to information that they produce are provided on the SG website.

Evidence	Further Development
E40: Scottish Government Model Framework Agreement Terms and Conditions E41: Scottish Government Terms and Conditions 1 - conditions of contract for the purchase of goods E42: Scottish Government Terms and Conditions 2 (SGTC2) E43: Scottish Government Terms and Conditions 3 - conditions of contract for consultancy services (other than works consultancies)	No further development is required at the moment but we will keep this under review.

E44: Scottish Government Terms and Conditions 4 - conditions of contract for the supply of goods (and any related services) E45: Scottish Government Terms and Conditions 5 - conditions of contract for the sale of goods	