MODEL RECORDS MANAGEMENT PLAN

For Developing Records Management Arrangements Under Section 1 of

The Public Records (Scotland) Act 2011

Contents

Preface

Model Records Management Plan

To assist Scottish Public Authorities to comply with the Public Records (Scotland) Act 2011

The Keeper of the Records of Scotland (the Keeper) is statutorily obliged under the terms of the Public Records (Scotland) Act 2011 (the Act) to publish a Model Records Management Plan (Model Plan) to assist authorities when preparing their own records management plan (RMP) for submission to the Keeper for agreement as required under the Act.

Section 1 of the Act says,

1 Records management plans:

(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.

(2) An authority's records management plan must—

(a) identify—

(i) the individual who is responsible for management of the authority's public records, and

(ii) (if different) the individual who is responsible for ensuring compliance with the plan, and

(b) include, in particular, provision about—

(i) the procedures to be followed in managing the authority's public records,

(ii) maintaining the security of information contained in the authority's public records, and

(iii) the archiving and destruction or other disposal of the authority's public records.

For more information regarding the Act see:
https://www.nrscotland.gov.uk/record-keeping/public-records-scotland-act-2011

For statutory requirements placed on the Keeper, including the preparation of the Model Plan see:
https://www.legislation.gov.uk/asp/2011/12/contents

Introduction

Under the Public Records (Scotland) Act 2011 ("the Act") Scottish public authorities must 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. To assist authorities in this process, the Keeper must publish a model RMP ("Model Plan") that has been produced in consultation with stakeholders. To this end the Keeper established a Public Records Stakeholder Forum ("the Forum")[1] to help develop the Model Plan.

The Model Plan should be read in conjunction with the Guidance to the Form and Content of the Model Plan ("the Guidance"). The Guidance has been produced to comply with section 1(4) of the Act

The Model Plan details 15 elements that the Keeper would expect a Scottish public authority to consider when creating its RMP. It is recognised that all the elements of the Model Plan might not apply to every authority. However, should an authority consider that an element does not apply, the Keeper will expect to see an explanation in support of the omission of that element from its RMP.

Although the Model Plan is published by the Keeper, its content reflects the combined work of the Keeper and the Forum. The Forum membership had representation from a cross section of public authorities and other bodies who are affected, either directly or indirectly, by the Act.

In 2018 the Keeper established a new Stakeholder Forum to develop and produce this revised version of the Model Plan. In response to EU and UK Data Protection legislation the Forum reviewed Element 9, "Data Protection" and concluded only minimal changes were required to the Model Plan. The retention of element nine has been accompanied by the 'seeding' of data protection, where appropriate, throughout other elements in the plan. The most significant change to the plan comes from the Forum recommendation to include an additional element, Element 15, "Public records created by third parties". This element does

[1] *The Forum included representatives from across the public sector and also from relevant professions and other stakeholders. The Forum provided the main mechanism to deliver cross sector agreement on issues relating to the form and content of this Model Plan and the accompanying Guidance Document. Members of the Forum represented the views of their respective sectors, as well as comments on the general principles of good records management. The Guidance Document is drawn from guidance already in existence or in the course of being developed.*

not add to existing requirements of authorities, it merely emphasises the importance of this responsibility through the creation of a separate element.

A glossary of terms used in the Model Plan is included as Appendix A in the Guidance. Reference in this document to an 'authority' should be taken to mean an authority listed in the schedule of the Act. (http://www.legislation.gov.uk/asp/2011/12/schedule/enacted)

The records management practices set out in the Model Plan and supported by the Guidance are essentially a matter of good business administration. Therefore, authorities should already be complying with the bulk of these, including the allocation of adequate resources to support their records management arrangements. Authorities should use the Model Plan and Guidance to assess the effectiveness of their existing records management arrangements. Any deficiencies will need to be addressed including where necessary some consideration of existing resources. In considering what remedial action will be appropriate, authorities should consult the Model Plan and Guidance and take account of the consequences of failing to comply with the Act.

Section 8(3) of the Act states that authorities must have regard to the Model Plan, but it is not compulsory for an authority to copy the format of the Model Plan in developing their RMP. Where an authority has already developed a robust records management system the Keeper would not expect that authority to expend additional resources rewriting it in line with the Model Plan.

It is important to note that establishing effective records management arrangements will deliver significant benefits for authorities – for example it will help to:

- **Increase efficiency and effectiveness, delivering savings in administration costs**
- **Improve and develop service delivery**
- **Achieve business objectives and targets**
- **Ensure compliance with the Public Records (Scotland) Act 2011 and other legislative requirements, standards and codes of conduct**
- **Support transparency and open government**
- **Underpin business resilience**

The scope of the Model Plan applies to all records irrespective of the technology used to create and store them or the type of information they contain.

Model Records Management Plan

This Model Plan has 15 elements. The Keeper expects each of these elements to be addressed in a RMP submitted by an authority.

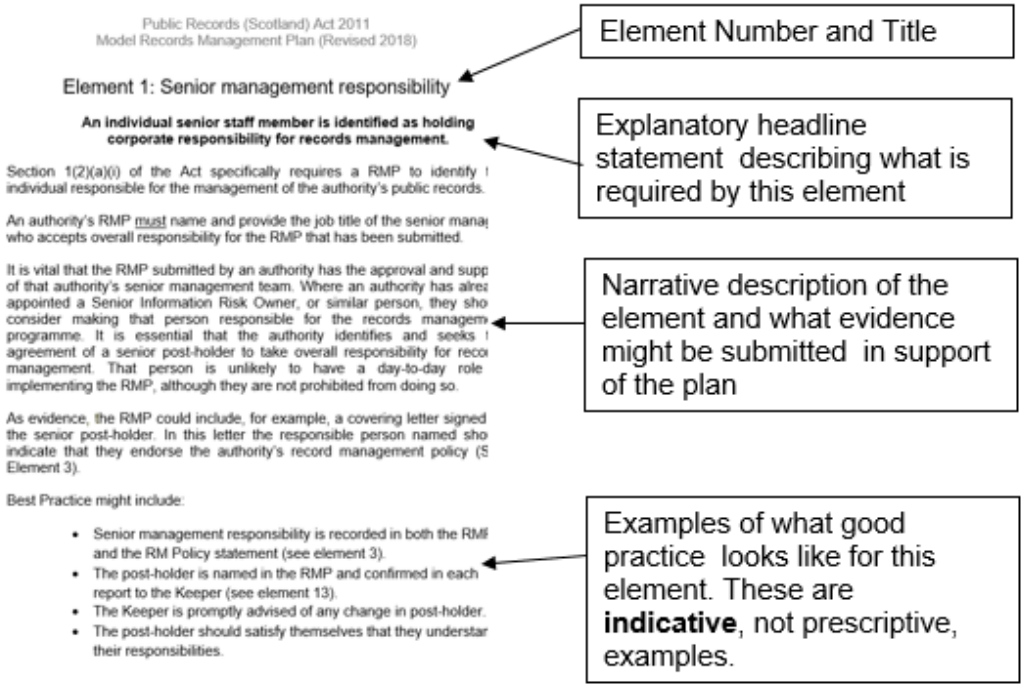
The order in which these elements appear is not prescriptive, nor does a RMP have to use the Model Plan numbering sequence. However, an authority must have regard to the Model Plan in preparing its own plan for submission to the Keeper.

The 15 elements 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. **Records management training for staff**
13. **Assessment and review**
14. **Shared information**
15. **Public records created by third parties**

Whilst it is not compulsory for authorities to directly copy the Model Plan they are required to have regard to it when preparing their own plans. It is also important to remember that certain elements of it are specifically required under the Act.

Within the Model Plan each of the 15 elements is addressed and within each element the following layout is always applied.



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.

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).

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 elements 1 and 2).
- The Policy is regularly reviewed.

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).

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).

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.