GUIDANCE TO THE FORM AND CONTENT OF THE MODEL RECORDS MANAGEMENT PLAN

For Developing Records Management Arrangements Under Section 1 of

The Public Records (Scotland) Act 2011

National Records of Scotland
Model Records Management Plan - **Guidance**
To assist public authorities to comply with the Public Records (Scotland) Act 2011

Links checked by NRS: February 2024

This document last updated: February 2024

Contents

Introduction

This Guidance Document is designed to assist Scottish public authorities create a records management plan (RMP) that is sufficiently robust to receive the agreement of the Keeper of the Records of Scotland (the Keeper). It provides links to published best-practice and sample documents that an authority might adapt for their own purposes. Samples are for 'inspiration' only, and should not be taken to represent the current procedures operational in any authority.

This guidance has been prepared by the National Records of Scotland in consultation with a cross-section of bodies affected by the Public Records (Scotland) Act 2011 (the Act). The guidance is not prescriptive, but is designed to be used in part, or adopted wholesale, as public authorities think appropriate.

As well as PDF samples, this document occasionally provides links to guidance created and published on the websites of other organisations. The National Records of Scotland has no control over this material or when and how often it is amended or updated. You should be aware that, while we will make every effort to keep our Guidance Document up to date, it will not be possible to guarantee that links are to the latest versions of any external document.

The Keeper is committed to helping public authorities comply with the Act. If, having consulted this guidance, an authority is still unsure of what is required, they should contact the Keeper's implementation team at public_records@nrscotland.gov.uk

About the Public Records (Scotland) Act 2011

1. What is meant by the "form" of the Records Management Plan (RMP)?

The Keeper is statutorily obliged to issue guidance on this aspect of the RMP because authorities may wish to use a variety of media when submitting an RMP to the Keeper for consideration and agreement.

While it is expected that most scheduled authorities will chose to support their plan digitally, it may be the case that a paper copy (or in some other format) will be necessary or suitable. The Keeper wishes to be flexible in approach regarding this and will consider all formats on a case-by-case basis.

Similarly, it is expected that most authorities will choose to submit the supporting evidence for their plans, for the Keeper's consideration, in digital format. However, the option to do this by some other means remains open to the Keeper and authorities to mutually agree.

2. What is meant by the "content" of the RMP?

There are certain elements of records management provision that the Keeper will expect authorities to address, and clearly evidence, in their RMP.

These elements are explained in the Keeper's Model RMP. This can be followed by authorities without modification if it fits their circumstances, or by amendment to suit their records and their particular business needs. The Keeper's Model Plan has been issued following extensive consultation with public authorities and others affected by the legislation. The Model Plan can be viewed at http://www.nrscotland.gov.uk/record-keeping/public-records-scotland-act-2011/resources/model-records-management-plan.

Under the terms of the Public Records (Scotland) Act 2011, the Keeper is required to publish guidance so that the individual elements of the Model Plan can be readily understood by all who are obliged to produce a RMP, and to help authorities make accurate and sensible decisions on what their own RMP should contain. It is also vital that authorities understand what is expected of them under each element of the RMP. This is of critical importance because it may be that for some bodies not all the elements of the model RMP will be relevant.

Evidence

In order to agree the records management plan (RMP) of a public authority, the Keeper must be satisfied that the policies and procedures explained in the plan are in fact operational throughout an authority. To do this, the Keeper will ask that an authority submits evidence that supports the claims made in their RMP.

The nature of this evidence will depend on the individual authority. The 'evidence' section under each element in this guidance is not prescriptive nor is it comprehensive.

There are, however, some points that scheduled authorities should consider before submitting evidence to the Keeper:

1. The single most important piece of evidence that the Keeper would expect to see with each RMP is the sign-off of a senior accountable officer from the authority. This aspect of the RMP (Element 1 in the Model Plan) is mentioned specifically in the Act (1 2(a)i) and is therefore compulsory for its agreement.

2. If an authority's RMP refers to a formal policy document, the Keeper would expect to see a copy of that document and expect to see evidence that the policy is approved by a relevant accountable officer. It is accepted that, in some specific cases, access to documents by the Keeper's assessment team might be restricted. An explanation of this, again approved by the senior accountable officer, would suffice.

3. Submitted evidence should not be created solely to comply with the Public Records (Scotland) Act 2011 (the Act), but should be drawn from current records management policies and procedures.

4. A records management self-assessment exercise, as advocated by the Keeper, would generate evidence that might be submitted in support of an authority's RMP (see below). The self-assessment programme is not however, in itself, a substitute for a RMP.

5. The Keeper does not require multiple copies of similar evidential documents. One robust piece of evidence should suffice. For example, a single sample contract, might be used as evidence of the type of arrangement that would apply to all comparable contracts.

6. Please do not send the Keeper, as evidence, documents labelled ‘draft’, ‘business case’ or similar. The Keeper can only consider documents that appear to be final and approved.

General Guidance

The Keeper of the Records of Scotland (the Keeper) is required, under section 1.4 of the Act, to issue guidance to 'the form and content' of the Model Records Management Plan.

Section 9 of the Act permits the Keeper to offer guidance beyond the form and content of the Model Plan. The Keeper considers that, further to fulfilling a statutory requirement, this Guidance Document should provide links to other guidance on records management. It is hoped that this will encourage best practice generally and to further a culture of improvement in Scottish public sector records management.

1. General Records Management Guidance

National Records of Scotland

The National Records of Scotland offer guidance and advice for organisations considering implementing or expanding a records management programme. Link: http://www.nrscotland.gov.uk/record-keeping/records-management

Scottish Ministers' Code of Practice on records management by Scottish public authorities under the Freedom of Information (Scotland) Act 2002 - 'Section 61' - Records Management Code of Practice.

Many of the authorities scheduled under the Public Records (Scotland) Act 2011 will also have been scheduled under the Freedom of Information (Scotland) Act 2002 (FOI(S)A). The records management code, issued to set out practices authorities should follow to comply with FOI(S)A, was prepared in consultation with the Scottish Information Commissioner and the Keeper of the Records of Scotland. The updated version of the code was officially launched in December 2011 and, although the two pieces of primary legislation are entirely separate, the FOI(S)A code and the PR(S)A guidance are complementary.

Link: https://www.gov.scot/publications/code-of-practice-on-records-management/

Model Action Plan

The Keeper of the Records of Scotland has produced a generic Model Action Plan to assist Scottish public authorities in the development of records management arrangements which comply with the Freedom of Information (Scotland) Act 2002 section 61 Code of Practice on Records Management. The generic Model Action Plan should be read in conjunction with the section 61 code. It can be used by individual organisations as a guide, and can also be used as the basis for the development of sector-specific plans tailored to the needs and business practices of particular types of public authority.

Link: https://www.nrscotland.gov.uk/record-keeping/public-records-scotland-act-2011/resources/model-records-management-plan

ISO ISO 15489-1:2016 Records Management

ISO 15489-1 (last reviewed in 2021) provides guidance on managing records in organisations, public or private, for internal and external clients. However, unlike other guidance offered here, the ISO document is not free. The link is to the 'shop' where it can be purchased. Appendix 2 of this Guidance Document lists other formal standards that refer to records management.

Link: https://www.iso.org/standard/62542.html

Office of the Scottish Information Commissioner (OSIC)

Although it is clearly designed for OSIC staff, their Information and Records Management Handbook offers best practice guidance generally and is a high-quality example of how staff guidance might be arranged.

Link: https://www.itspublicknowledge.info/sites/default/files/2022-04/InformationandRecordsManagementHandbook.pdf

University of Edinburgh

Also principally designed for use by their own staff, a large suite of guidance is freely available on the Edinburgh University website and features information that could, with a little adaptation, be of benefit for all organisations instigating a records management programme. For example, guidance on how to set up records management systems are available to download.

Link: https://www.ed.ac.uk/records-management

The UK Information Commissioner

To assist with data protection compliance, the Information Commissioner's Office has developed several records management guidance documents. Although focused on the secure handling of personal information, many of the principles are 'content-neutral' and may represent a valuable addition to a records manager's guidance suite.

Link: https://ico.org.uk/media/for-organisations/documents/1624142/section-46-code-of-practice-records-management-foia-and-eir.pdf

The National Archives UK (TNA) records management guidance

TNA offers a series of guides and standards for information management professionals including a large section on records management (click on 'R' under A-Z for 'Records Management' but be aware that other guidance may be of interest such as appraisal under 'A').

Link: http://www.nationalarchives.gov.uk/help/a-to-z/

Scottish Public Services Ombudsman (SPSO)

SPSO have taken the opportunity to unify records management guidance into a single published document, *The Information Governance Handbook*. This document includes the Records Management Plan in section 1 and the Records Management Policy

in Section 2. Many of the security principles are also explained in the *Handbook*, including a section on 'Managing Personal Data'. As a single point of reference, the Handbook appears to be a useful tool for SPSO staff. It is published on the SPSO website.

Link:
http://www.spso.org.uk/sites/spso/files/communications_material/foi/corporate_documents/InformationGovernance(R.2017.04)W.pdf

Information and Records Management Society

IRMS is a membership organisation that is an association for information professionals and students. It provides support and brings together all those working in information governance, records management, data protection, information security and more, across all industry sectors, in the UK and beyond.

Link: https://irms.org.uk

Other Publications: Users of this guidance should be aware that there are several published works on records management which may prove useful when creating a RMP. You may be able to consult copies of these publications in larger libraries.

2. Self-assessment:

Section 1(5)(i)(a) of the Act says that an authority must keep its RMP under review. One of the ways to comply with this requirement is to undertake a regular self-assessment exercise and to provide details of this to the Keeper (see element 13 below).

There are several records management self-assessment tools available that an authority might utilise. The following offers a few examples.

ARMS

The Scottish Council on Archives has developed a self-assessment tool called ARMS (Archives and Records Management Services). The Keeper of the Records of Scotland has endorsed ARMS as being entirely complimentary to their Model Plan and the aims of the Act. The Keeper considers the ARMS self-assessment tool may be instrumental in helping further a culture of good records management in Scotland as it was commissioned in Scotland by Scottish archive and records management professionals and designed specifically to assist Scottish authorities assess their own records management performance,

ARMS is described as '*A quality improvement framework to improve the consistency and transparency of quality and performance measurement across archives and records management in Scotland'.*

Although developed separately from the Public Records Act, ARMS is entirely complementary to the 'improving' spirit of that Act, and it is therefore a key piece of guidance in this document.

ARMS is primarily designed to be a flexible self-assessment tool that allows organisations undertaking a records management review to create an improvement plan. This is designed to be a self-development exercise rather than a formal systems audit. However, it is hoped that the project will lead to the identification of positives and negatives in current practice, and allow an organisation to target areas for improvement.

Link: http://www.scottisharchives.org.uk/arms

National Records of Scotland - Records Management Workbook

In 2006 the National Archives of Scotland (now part of the National Records of Scotland) made available a *Records Management Workbook* to permit organisations or auditors to check their records management procedures against the section 61 Code of Practice (issued under the Freedom of Information (Scotland) Act 2002). This tool can be adapted by public authorities intending to assess their records management provision in light of the Public Records (Scotland) Act 2011.

Link: http://www.nrscotland.gov.uk/files//about-us/complying-with-records-management-code-evaluation-workbook.pdf

The National Archives

The National Archives has developed an automated support tool to help public authorities to evaluate and assess the performance of their records management systems.

Link: http://www.nationalarchives.gov.uk/information-management/manage-information/ima/

The UK Information Commissioner

To assist with data protection compliance, the Information Commissioner's Office has developed a self-assessment Toolkit. Although focused on the secure handling of personal information, it may represent a useful starting point for an authority considering developing their own assessment process.

Link: https://ico.org.uk/for-organisations/sme-web-hub/checklists/data-protection-self-assessment/

It is worth remembering that many records management principles are relevant wherever in the world an organisation is based. There are several self-assessment toolkits developed for the public sector outside the UK that could be considered:

US: Records Management Self-Assessment (RMSA): https://www.archives.gov/records-mgmt/resources/self-assessment.html**.**

Australia: Information Governance Agency Self-assessment Tools: https://www.ipc.nsw.gov.au/information-governance-agency-self-assessment-tools-privacy.

New Zealand: Information Management Maturity Assessment: https://www.archives.govt.nz/manage-information/how-we-regulate/monitoring-and-audit/information-management-maturity-assessment.

See guidance under element 13 for the Keeper's expectations around reviewing records management provision under the Act.

Please note that any samples provided in this Guidance should not be taken to represent the current procedures operational in the authority that provided the sample; they are for 'inspiration' only.

If you encounter difficulties opening linked websites or PDF documents provided or if you have any uncertainties around the application of this guidance, or any other queries regarding compliance with the Act, please contact the Public Records (Scotland) Act Team at the National Records of Scotland: public_records@nrscotland.gov.uk.

Guidance to Element 1

Senior management responsibility

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

It is vital that the RMP has endorsement at the highest levels in an authority.

A RMP will require resources to implement and maintain, and therefore the Keeper, in agreeing an authority's RMP, will need to be assured that it is supported by a commitment at a senior level.

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. It is, therefore, essential that the authority identifies 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.

The identification of an individual is specifically mentioned in the Act (1 2(a)i) and a name must be supplied. Neither a job title (i.e. 'CEO') nor a collective body (i.e. 'XXX City Council') is acceptable under the terms of the Act.

Current best practice guidance advises senior management to:

- Recognise records management as an important corporate responsibility and give it the appropriate level of priority and authority
- Assign overall line management responsibility for records management to a senior member of the management team. Where an authority has already appointed a Senior Information Risk Owner (SIRO) or similar person, they should consider making that person responsible for the records management programme.

If all information functions are not part of the same command, it is important that the Keeper can be confident that there are close working relationships between them.

Evidence

The Keeper will require evidence to be submitted, confirming the name and job title of the senior responsible officer with overall responsibility for the RMP, which has been submitted for agreement.

The Keeper will write to the CEO (or equivalent) of an authority inviting them to submit the RMP. It would be beneficial if the CEO could respond to the Keeper indicating who the individual at element 1 in the plan ought to be and providing their contact details. In some cases this will be the CEO themselves. In other cases this will be delegated. The CEO should make any delegation clear in a covering letter or a foreword to the RMP.

If it is not possible for the CEO to produce such a covering letter, the individual identified at element 1, who must still hold a senior position in the authority, should provide one. Again, this does not have to be a separate document and may take the form of a foreword to the RMP.

It would also be useful if the covering letter identifies the individual at element 2 and endorses the Records Management Policy statement (see element 3).

If the authority has a Records Management Policy and if that Policy has a ‘roles’ section, the responsibility of the senior officer named at element 1 should be supported.

If the authority has formally allocated responsibilities to each of the elements in their RMP (many have done this, but it is not compulsory) then the Keeper would expect the senior officer to be directly responsible for, at least, element 2. The individual identified at Element 1 retains overall responsibility for records management in an authority, but the individual at element 2 may have delegated responsibility for elements 3 – 15.

Examples

It is possible that the records manager will be required to write the Covering Letter for the CEO or senior officer to sign:

PDF 01. A sample of a Covering Letter (from the NRS) that identifies a senior officer, the person at element 2 and endorses the Records Management Policy

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/covering-letter-from-nrs.pdf

PDF 02. A sample of how a senior officer can support records management in a public authority by providing a foreword to the RMP itself (Example from Ayrshire Valuation Joint Board):

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/covering-statement-from-ayrshire-valuation-joint-board.pdf

PDF 03. A sample of how 'roles' might appear in a Records Management Policy supporting the identification of the senior officer to element 1. (Example from Scottish Fire and Rescue Service):

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/roles-in-records-management-policy-from-sfrs.pdf

Guidance to 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.

The Act specifically requires an authority to identify the name and job title of the individual in their authority, who is charged with overseeing the implementation of the plan on a day-to-day basis. Normally, this will be the Corporate Records Manager or similar, rather than a director or other senior manager.

This individual will normally be the Key Contact for the PRSA Team for purposes relating to the agreement and implementation of the RMP. For example, any engagement around the development of the RMP is likely to be with this individual.

The Keeper will, therefore, require evidence to be submitted confirming the name and job title of the person responsible for the day-to-day operation of the authority's RMP, as part of that RMP. The Keeper will expect an authority to name an individual, rather than simply a job title.

All staff members who create records should be made aware of the organisation's records management programme. However, in this element, the Keeper requires the name of the individual, who has the operation of the records management programme, as a specific objective in their work plan.

The Act indicates that a single individual should be identified. However, in some cases an authority may have more than one records manager, for example, in the case of a job-share or Corporate/Clinical administrative division. In these circumstances, references in this guidance to 'the individual' can be taken to read 'the individuals'.

Evidence

The RMP must supply a name. Neither a job title alone (i.e. 'Records Manager') nor a collective body (i.e. 'Finance Department') is acceptable under the terms of the Act.

Evidence of compliance may take the form of covering letter carrying the senior accountable officer's signature, and identifying the person responsible for implementing the RMP (see under guidance for element 1).

Evidence of compliance might also take the form of the formal job description of the role, showing clear responsibility for day-to-day records management in the authority.

If the individual has annual objectives relevant to the implementation of the RMP, or of information governance generally, please supply these (redacted as appropriate).

The Keeper will require evidence that the individual identified at element 2 has access to relevant training opportunities.

If the individual identified at element 2 is a professionally qualified records manager, and/or is a member of a relevant professional body, this should be included under this element.

If the authority has a Records Management Policy, and if that Policy has a 'roles' section, the responsibility of the individual named at element 2 should be supported.

If the authority has formally allocated responsibilities to each of the elements in their RMP (many have done this, but it is not compulsory), then the Keeper would expect this individual to be responsible for various elements, such as instigating the review of the RMP (element 13).

Examples

PDF 01. A sample of how the implementation of the RMP might appear in the 'Records Manager's' job description (Example from Aberdeen City Council):

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/demonstrating-implementation-of-rmp-in-rm-job-description-from-aberdeen-city-council.pdf

PDF 02. A sample of relevant entries from a Records Manager's annual objectives (Example from Loch Lomond and Trossachs National Park Authority):

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/example-of-entries-from-rm-annual-objectives-from-loch-lomond-and-trossachs-national-park.pdf

PDF 03. A sample of how training opportunities might be evidenced (Example from Historical Environment Scotland):

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/how-training-opportunities-may-be-evidenced-from-historic-environment-scotland.pdf

PDF 04. A sample of how training opportunities for the records manager may be evidenced by their personal development plan (PDP) (Example from NHS Dumfries and Galloway):

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/training-opportunities-for-rm-evidenced-by-pdp-from-nhs-dumfries-and-galloway.pdf

PDF 05. A sample of how the records manager can be supported in a Records Management Policy (Example from Renfrewshire Council):

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/how-rm-can-be-supported-in-rm-policy-from-renfrewshire-council.pdf

Guidance to Element 3

Records management policy statement

The authority has an appropriate policy statement on records management.

The Act specifically requires authorities to have a 'records management policy statement'. This is probably best achieved by developing a formal records management policy which can be published, at least to staff, and probably online. There are several examples of what a records management policy might look like below.

The policy should be used in an authority to govern the creation and management of authentic, reliable and useable records, capable of supporting business functions and activities, for as long as they are required.

The policy should be a key component of an authority's corporate governance. It will help foster an appropriate culture within the authority, and it will help demonstrate to stakeholders that it is committed to undertaking its business activities in a diligent and accountable manner.

The policy should reflect the size and complexity of the authority, and confirm that the policy is owned by senior management. Authorities with a wide range of functions, operating in a complex legislative environment, will require a fuller policy document than a smaller authority.

The policy should define the legislative, regulatory and best practice framework within which the authority operates, and demonstrate how the authority aims to ensure that its records remain accessible, authentic, reliable and useable through any organisational or system change. A good records management policy should make records management roles clear and commit the authority to appropriate training.

A good records management policy should also include a description of the mechanism for records management issues being disseminated through the organisation, and confirmation that regular reporting on these issues is made to the main governance bodies.

Although the Public Records (Scotland) Act 2011 is 'technology blind' and refers to records created in any format, an authority's formal policy may, if appropriate, differentiate between the processes in place for paper records, and for those held electronically.

The policy must be approved by senior management and should be made available to all staff at all levels in the organisation.

The policy statement is a compulsory element of a RMP according to the Act (1 2(b)(i). It must be approved by a senior accountable officer in the authority and submitted to the Keeper.

Evidence

The Keeper will expect to be provided with a copy of the records management policy and of any supplementary guidance that accompanies it. If the authority has other high level documents, such as an information governance strategy, these should also be submitted under element 3. It would be useful if the Chief Executive, or the person named at element 1, could provide endorsement of the records management policy in a covering letter. The Keeper will be looking for evidence that the policy is understood at the highest levels of an authority.

Examples

PDF 01. A sample Records Management Policy (Example from Dumfries and Galloway Council):

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/records-management-policy-example-from-dumfries-and-galloway-council.pdf

Many authorities have used element 3 in their RMP to submit other information governance documents that support and provide guidance to the policy. This is not a requirement, but is likely to be acknowledged and welcomed by the Keeper.

Below are some examples of supplementary documents that were provided to the Keeper alongside a Records Management Policy:

PDF 02. This is an example of an overarching Information Governance Strategy (Example from Strathclyde Partnership for Transport):

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/overarching-ig-strategy-example-from-strathclyde-partnership-for-transport.pdf

Below is an example of Records Management Guidance for staff. Again, Element 3 would seem the most appropriate place to include a general guidance document like this:

PDF 03. A sample Records Management staff guidance manual (Example from Police Scotland is called 'standard operating procedure'):

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/records-management-staff-guidance-manual-example-from-police-scotland.pdf

Guidance to Element 4

Business classification

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

In line with the Keeper of the Records of Scotland's (The Keeper's) obligations under the Public Records (Scotland) Act 2011 (the Act), the following guidance is issued about an authority's Business Classification Scheme:

It is expected that an authority's *Records Management Plan* (RMP) submitted for agreement with the Keeper, confirms that the authority has developed, or is in the process of developing, a business classification scheme or similar.

We are using the term 'business classification' to refer to a representation of an authority's functions, and the records created pursuing those functions. For some authorities, this may appear in the form of a simple File Plan; for other, more complex organisations, as a full Information Asset Register. As long as all public records, in all formats, are considered under this element, the Keeper should be able to agree it is compliant.

The purpose of this element is to demonstrate, in the RMP, that the authority takes account of all the records created by the entire organisation and all its various business activities.

Having a structured business classification scheme at the outset will assist an authority in the application of retention and disposal decisions under each of these business functions. It is also likely that a robust business classification scheme structure will assist staff to save, locate and recover records efficiently.

To properly fulfil this element, an authority will need to demonstrate that its business classification scheme can be applied to all the records management systems which it operates.

Element 4 is, therefore, the ideal section of an authority's RMP for them to explain to the Keeper the different systems and formats in which their public records are kept. For some authorities, all records will be held digitally in an electronic records management system. However, the majority of Scottish public authorities operate multiple record keeping systems simultaneously. The Keeper will need to be satisfied that the authority has considered all these structures under their Business Classification Scheme. For example, the Keeper would expect to see reference to all of the following:

- Records held digitally on an electronic records management system
- Records held digitally on network/shared drives
- Records held hard-copy in a corporate records store or in offices (including legacy records)
- Records held hard-copy in an external store operated under contract by a third party (the Keeper would expect to see evidence that this arrangement is operational – such as a copy of the contract, redacted as appropriate)
- 'Line of Business' systems (see below)

Once the different formats and record keeping systems are explained in element 4, this should provide a structure for other elements where procedures vary depending on format or location (such as the destruction procedures detailed in element 6).

A clear and robust business classification scheme is a strong business tool for any organisation. Its utility for the authority must be the primary consideration when the scheme is being developed and implemented.

However, this is also a very important element for the purposes of achieving the Keeper's agreement upon which much of the rest of the plan will be built. It is also subject to change as new systems and procedures are implemented in an authority. It is approached in different ways by different organisations as best suits their business need. The Keeper is open to receiving schemes based on different methodologies, whether complete or in development. Any proposed scheme should aim to better allow an authority to document its activities, identify records, retrieve records, apply disposal markings, and meet statutory and regulatory requirements.

It is understood that to encompass an authority in its entirety, the expansion of the formal business classification scheme, may take many years – particularly for more complex organisations. If an authority is not able to fully satisfy this element when submitting their RMP for agreement, then

a) The Keeper will expect to see evidence that senior management acknowledge the importance of expanding the business classification scheme throughout the organisation, and

b) The Keeper's agreement is likely to be conditional on receiving regular updates as the roll-out progresses.

To this end, it is suggested that authorities should schedule their own review of progress (see element 13) and report this to the Keeper.

A note regarding ‘Line of Business Systems’

We use the term ‘line of business system’ to cover the huge range of information systems that sit outside the main records management provisions in public authorities.

These may be case management or HR systems, scientific databases, paper checklists, or any number of other similar arrangements. These may be peculiar to one area of the authority’s business.

In some cases, the output from these records may be collated into a document that is later stored in an electronic records system or similar. In some cases, line of business systems lie entirely and permanently outwith the standard records management structure of an authority.

Either way, the records held in line of business systems remain public records under the Act and should be accounted for under a RMP. As many of these line of business systems are bespoke and unique to a particular authority, it is not practical for the Keeper’s assessment team to familiarise themselves with the information management specification of each.

However, the Keeper requires a statement from each authority to the effect that they are confident in the records management provision their line of business systems offer. An authority should consider the relevant elements in their RMP (such as information security), and satisfy themselves that any line of business system offers a similar standard to that reported on for the main records management provision. They should then state this clearly to the Keeper.

Evidence

The Keeper does not require authorities to provide him with evidence down to file level, or containing all the details of an information asset register. He/she does, however, expect an authority to be able to classify its functions, the activities that deliver these functions, and an indication of the classes of records being created (or held) while pursuing these activities. The Keeper expects an authority to explain the format of these records and where they are being managed.

Sample business classification documents:

N.B. Business Classification Schemes, Information Asset Registers and Retention Schedules are all 'living documents' – they are, quite properly, subject to regular review and alteration. The examples given below are to demonstrate potential layouts and the types of information that might be included. None are supplied as evidence of the current schemes in operation in the authority.

PDF 04/01 A sample Business Classification Scheme and Retention Schedule as a combined document (Falkirk Council)

Link: *https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/04-01-falkirk-council-example-business-classification-scheme-and-retention-schedule.pdf*

PDF 04/02 A sample extract showing the information that could be included in an Information Asset Register (North Lanarkshire Council)

Link: *https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/04-02-north-lanarkshire-council-example-information-asset-register-extract.pdf*

PDF 04/03 It is not necessary for a small authority to develop a scheme of the complexity shown in the examples above. Here is an alternative simple style that is perfectly acceptable (Scottish Criminal Cases Review Commission)

Link: *https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/04-03-scottish-criminal-cases-review-commission-business-classification-scheme.pdf*

PDFs 04/04-10 A business classification is a living document liable to change to reflect alterations in the business procedures of an authority. Below are examples of documents from a business classification review framework (NHS National Services Scotland)

Link (04/04): *https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/04-04-national-services-scotland-review-of-business-classification-scheme.pdf*

Link (04/05): *https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/04-05-national-services-scotland-business-classification-scheme-framework.pdf*

Link (04/06): *https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/04-06-national-services-scotland-business-classification-scheme-communication-and-training-toolkit-guidance.pdf*

Link (04/07): *https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/04-07-national-services-scotland-business-classification-scheme-business-as-usual-model.pdf*

Link (04/08): *https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/04-08-national-services-scotland-business-classification-scheme-progress-report-template.pdf*

Link (04/09): *https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/04-09-national-services-scotland-business-classification-scheme-screenshots.pdf*

Link (04/10): *https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/04-10-national-services-scotland-business-classification-scheme-user-guidance-redacted.pdf*

PDFs 04/11-13 Three further examples of how a business classification scheme might be presented:

The Office of the Scottish Charity Regulator

Link (04/11): *https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/04-11-office-of-the-scottish-charity-regulator-business-classification-scheme.pdf*

The Scottish Funding Council

Link (04/12): *https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/04-12-scottish-funding-council-file-plan.pdf*

The Scottish Information Commissioner

Link (04/13): *https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/04-13-scottish-information-commisioner-file-plan-and-retention-schedule.pdf*

Guidance to Element 5

Retention schedule

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

In line with the Keeper of the Records of Scotland's (The Keeper's) obligations under the Public Records (Scotland) Act 2011 (the Act), the following guidance is issued regarding an authority's retention or disposal schedule.

It is required by the Act that an authority's records management plan (RMP) submitted for agreement with the Keeper, confirms that the authority has developed, or is in the process of developing, records retention and disposal schedules.

Current best practice guidance, such as that contained in the Section 61 Code of Practice on Records Management, issued by Scottish Ministers under the Freedom of Information (Scotland) Act 2002, advises that:

> *Authorities should define how long they need to keep particular records, should dispose of them when they are no longer needed and should be able to explain why records are no longer held. For the purpose of this Code, disposal means the decision as to whether the record should be destroyed or transferred to an archives service for permanent preservation, and the putting into effect of that decision.*[1]

A retention or disposal schedule is for the operational level of business records (as opposed to the policy at a strategic level), and is essential for the smooth running of an efficient records management system. It governs the retention and disposal of all records generated during the course of the activities of the organisation, ensures continuity, protects the organisation's legal rights, and preserves information for the archives.

Evidence

[1]Code of Practice on Records Management: http://www.gov.scot/About/Information/FOI/18022/13383

The Keeper will expect to see that a retention decision (even if that decision is 'review') has been applied to all the authority's public records in whatever format and management system that record is kept (see Element 4).

The authority should provide the Keeper with a retention schedule showing that it understands how long certain types of records should be kept. This schedule may appear in the form of a single document that applies to the entire operation, or as several documents, perhaps divided by the different functions and activities the authority undertakes. If the authority is submitting a comprehensive business classification scheme or information asset register, as described under Element 4, this may include retention instructions for each record series. In such a case there would be no need for the authority to submit a separate retention schedule.

The Keeper understands that for some authorities providing a comprehensive retention schedule may present a challenge in the short term. However, the Keeper would require indication that the authority is working towards completing such a schedule for all corporate records held throughout its entire operation. Evidence of an authority's improvement project for retention scheduling might be an explanatory statement, or an action plan, approved by the senior accountable officer.

Sample Retention Documentation:

N.B. Business Classification Schemes, Information Asset Registers and Retention Schedules are all 'living documents'. They are, quite properly, subject to regular review and alteration. The examples given below are to demonstrate potential layouts and the types of information that might be included. None are supplied as evidence of the current schedules in operation in the authority.

PDF 05/01 A sample Retention Schedule (Shetland Council)

Link: *https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/05-01-shetland-islands-council-retention-schedule.pdf*

PDF 05/02 A combined Business Classification Scheme/Retention schedule from a small authority (Dunbartonshire and Argyll and Bute Valuation Joint Board)

Link: *https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/05-02-dunbartonshire-valuation-joint-board-business-classification-and-retention-schedule.pdf*

PDF 05/03-04 Disposition (normally destruction) naturally follows retention and here we have two examples of combined retention/destruction policy (David MacBrayne Limited and Skills Development Scotland)

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/05-03-david-macbrayne-records-retention-and-disposal-policy.pdf

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/05-04-skills-development-scotland-retention-and-disposal-policy.pdf

PDF 05/05-06 It is, obviously, important that staff understand the purpose of a retention schedule and what actions they are expected to pursue in order that it is imposed effectively. Here is an example of a retention schedule with accompanying staff guidance (Board of Trustees for the National Galleries of Scotland)

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/05-05-national-galleries-of-scotland-records-retention-schedule.pdf

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/05-06-national-galleries-of-scotland-retention-schedule-guide.pdf

PDF 05/07 Guidance on retention (Scottish Further and Higher Education Funding Council)

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/05-07-scottish-funding-council-how-long-should-we-keep-records.pdf

Guidance to Element 6

Destruction arrangements

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

In line with the Keeper of the Records of Scotland's (The Keeper's) obligations under the Public Records (Scotland) Act 2011 (the Act), the following guidance is issued regarding an authority's destruction arrangements:

It is vital that an authority's records management plan (RMP), submitted for agreement with the Keeper, confirms that the authority has developed, or is in the process of developing, proper destruction arrangements. Public records should be destroyed as part of a controlled, secure and irretrievable process.

Please note that the Keeper does not require authorities to provide a list of the records destroyed. However, the RMP should explain the destruction process in place, including all formats, and evidence that this process is properly carried out. The destruction process is likely to vary depending on the format in which the record is held.

For digital records, the Keeper will want to see evidence that appropriate processes are in place to delete records at the end of their retention period (see Element 5). With some systems this happens automatically; in other cases the information asset owner will be prompted to do this 'manually'. The Keeper will want to see that adequate guidance is provided to asset owners, and others with this responsibility, to ensure that destruction is carried out correctly.

Using a commercial disposal firm for the disposal of hard-copy records is recommended because their practices will be controlled, audited, and fully compliant with current environmental regulations (their business can only exist if they are). They may be able to issue a certificate of destruction, which should be maintained with the disposal schedule as proof that the record has been destroyed. In the context of both Data Protection and Freedom of Information legislation, these sorts of procedures are the clear proof of controlled destruction of information. This is what the Information Commissioner would be looking for in any disputed request that the authority was unable to answer.

As well as digital and hard-copy records, the Keeper will also need to be reassured that the authority understands the destruction of records held in back-up systems. Most authorities, quite correctly, keep back-ups of their records for business continuity purposes

(see Element 10). The Keeper will ask how long after deletion could a record be restored using back-up processes. There is not necessarily a right or wrong answer to this, but the Keeper must be satisfied that the authority understands their situation.

Finally, the Keeper requires an authority to explain the processes for the secure destruction of records that are held on IT hardware once that hardware is deemed to be redundant. For example, if an authority recycles its laptops, what processes are in place to ensure all records are thoroughly purged from the hard drive? If hardware is destroyed by a third-party technical provider (as is often the case), what stipulations appear in the service agreement relating to the deletion of information? Have these clauses been approved by the authority's information security team or SIRO?

It is considered important that a list of records that have been destroyed is retained, probably permanently, to show the types of record an authority has previously created, and to confidently respond to requests to access information that has been properly destroyed or deleted.

It is also important that when a record is destroyed, it cannot easily be recovered. The United Nations Archives and Records Management Section advises as follows:

Destruction of records should be irreversible. This means that there is no reasonable risk of the information being recovered again. Failure to ensure the total destruction of records may lead to the unauthorised release of sensitive information.[2]

Evidence

Potential evidence of compliance would include a copy of the contract with a record destruction contractor (redacted for commercial-in-confidence purposes if necessary), or the authority's formal destruction policy approved by the senior accountable officer. A retention schedule alone would not be considered evidence that record destruction is actually taking place in an authority.

[2] https://archives.un.org/

As well as destruction certificates and contracts demonstrating that an external service provider is in place, the Keeper would expect to see staff guidance on the authority's destruction procedure. This might include instructions on how to delete records from an electronic records management system or network drive at the end of its retention period.

The Keeper can accept a statement from an authority regarding the availability of back-up copies. In the case that a continuity back-up service is provided by a third party, the Keeper would expect to see details around record recovery periods as part of a service agreement or similar.

Sample Documents Showing Destruction Arrangements:

The following sample destruction documentation might give you an idea what information such documents might include, and how they might be styled. Any samples provided should not be taken to represent the current procedures operational in the authority that provided the sample; they are for 'inspiration' only.

PDF 06/01-02 Sample instructions for staff, used to ensure that disposal procedures are correctly implemented (East Ayrshire Council and the National Library of Scotland)

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/06-01-east-ayrshire-council-records-disposal-policy.pdf

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/06-02-nls-disposal-guidance.pdf

PDF 06/03 The Keeper will be intertest to see that authorities properly consider the destruction of public records created on ancillary systems, such as e-mail

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/06-03-scottish-government-e-mail.pdf

PDF 06/04 The Keeper will be intertest to see that authorities properly consider the eventual destruction of public records held in back-up systems for business continuity purposes

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/06-04-scottish-government-back-up.pdf

PDF 06/05 The Keeper will be intertest to see that authorities properly consider the secure destruction of public records that are held on IT hardware once that hardware is deemed to be redundant.

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/06-05-audit-scotland-it-disposal.pdf

PDF 06/06-07 Finally examples of staff guidance around specific destructions issues where records may be destroyed outwith the authority's retention schedule

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/06-06-scottish-funding-council-deleting-records-before-retention-deadline.pdf

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/06-07-scottish-funding-council-what-records-can-we-routinely-destroy.pdf

Guidance to 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'.

In line with the Keeper of the Records of Scotland's (The Keeper) obligations under the Public Records (Scotland) Act 2011 (the Act), the following guidance is issued regarding an authority's archiving policy and transfer arrangements.

N.B. Under the Act, the term 'archive' refers to the permanent preservation of public records in a suitable repository. This is normally undertaken with future research purposes in mind, potentially long after the original record-creating authority has ceased to exist. In this context, 'archive' does not refer to the long-term storage of records for business purposes, whether in-house or with a commercial storage contractor.

A small proportion of records created by a public authority will be earmarked for permanent retention. These records will normally be removed from operational systems and transferred to an archive. This applies to records in all formats although the procedure for transfer will vary (for example, digital records allow for records to remain 'live' until the successful transfer of the archive copy has been confirmed).

It is a fundamental part of a Records Management Plan (RMP) that procedures for facilitating such transfers are in place and are followed.

The Keeper will expect to see evidence that a formal arrangement is in place between a public authority and a suitable repository. S/he will also expect the transfer process to be made clear. Evidence might include a memorandum of understanding between an authority and an archive repository, an internal schedule of preservation, or an explanation of how automated systems archive electronic records and details of how metadata transfers with those archival records.

The Keeper does not wish to dictate what records an authority chooses to preserve, but it is a requirement of a robust RMP that a formal process for transferring records for permanent preservation exists. The nature and content of the records being selected for permanent preservation within the system is a matter for the authority and archive repository to consider.

Many of the public records of an authority will now be ‘born-digital’. In the future, a small selection of these will require transfer to an archive for permanent preservation. It is therefore important that the Keeper can be confident that an authority has properly considered this when making its archive arrangements under the Act. S/he will expect, at the very least, that the archive repository, identified by a Scottish public authority as suitable for the permanent preservation of digital records, is taking steps to allow controlled transfer in a manner which secures the relevant metadata that supports the authenticity of the document.

Under Element 7 of the authority’s Records Management Plan, the Keeper will expect statements, and evidence if possible, confirming that this is being pursued by the identified repository.

The Keeper’s digital archiving team have published Guidance online at
Electronic Records Management | National Records of Scotland (nrscotland.gov.uk).

Evidence

Archiving arrangements are specifically mentioned in the Act (1(2)(b)(iii)). The inclusion of evidence that appropriate processes are in place must be submitted to the Keeper.

The Keeper has published guidance as to what constitutes suitable archival arrangements. The Keeper’s Supplementary Guidance on Proper Arrangements for Archiving Public Records is available at Supplementary Guidance on Proper Arrangements for Archiving Public Records (nrscotland.gov.uk).

The Keeper will expect a public authority to ensure that the archive identified for the permanent preservation of their public records can meet the standard explained in this guidance. Evidence in support of this may include a link to their public website or a statement from the archivist. It may also be useful if the authority can provide a selection of the archive’s policies (such as their collection policy) and procedures.

Potential evidence of a suitable agreement between an authority and an archive might include a formal policy approved by the senior accountable officer, a memorandum of understanding or deposit agreement with an archive repository, or receipts from such a repository as evidence of records deposited over time and by agreement.

Guidance to Element 8

Information security

Records are held in accordance with information security compliance requirements.

In line with the Keeper of the Records of Scotland's (The Keeper) obligations under the Public Records (Scotland) Act 2011 (the Act), the following guidance is issued regarding an authority's information security processes:

In the course of their business it is likely that public authorities will create records containing sensitive information about people or details of business transactions that the authority may wish to protect from general consultation. Similarly, it may create records that hold information which should not be amended or deleted without appropriate authority. In both these cases information security policies and procedures should be implemented by staff at the time of document creation.

As well as the security of the information contained in a document, an authority must consider the physical safety of records (in all formats). This would include attending to the proper storage of hard-copy records and the protection of servers used to store digital material. The Keeper would expect an authority to have policies in place to assure that records cannot be lost due to poor storage.

If your organisation is vacating premises you must take particular care of the security of records. You might consider having a formal policy on this matter.

As part of a full Records Management Plan (RMP), the Keeper would expect to see that such policies and procedures exist and are available to staff involved in the creation of records. S/he will also require confirmation that an authority has relevant staff-monitoring in place to ensure the security of its information assets. As evidence S/he will expect to be provided with copies of all relevant documentation.

The Keeper understands that in some rare cases the authority may be unwilling to share full security documents with him/her. For example, sharing a document that details out-of-hours access to building, or where records are stored, might be considered to compromise the general security of the authority's estate if it is shared beyond officers of that authority. If you have any concerns regarding this, please submit redacted samples accompanied by a short explanation of why you have taken this decision.

British Standard ISO 15489-1: 2001 states:

> *The regulatory environment, in which the organisation operates, establishes broad principles on access rights, conditions or restrictions that should be incorporated into the operation of records systems. There may be specific legislation covering areas such as privacy, security, freedom of information and archives. Records may contain personal, commercial or operationally sensitive information. In some cases, access to the records, or information about them, should not be permitted.*[3]

Evidence

Potential evidence that an authority is properly considering information security might include a formal information security policy, approved by the senior accountable officer; details of the password protection and encryption systems in operation; information regarding access restrictions to record storage areas; description of electronic record back-ups held on separate servers; staff information security manuals, regulations and/or circulars; and routine information security reports or updates to senior management.

Sample Security Documents:

The following samples suggest some of the documents that make up an information security framework and how these might be structured. Many authorities have chosen to provide the Keeper with a suite of security documents under this Element.

Any samples should not be taken to represent the current procedures operational in the authority that provided the sample; they are for 'inspiration' only.

[3] BS ISO 15489-1:2001 Information and documentation – Records management Part 1: General section 9.7.

PDF 08/01-08/03 Most authorities have a stand-alone Information Security Policy, although some choose to embed it in a larger Information Governance Strategy document. Here are three examples of how a separate Information Security Policy might be presented.

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/08-01-angus-council-information-security-policy.pdf

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/08-02-audit-scotland-information-security-management-policy.pdf

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/08-03-aberdeenshire-council-information-security-policy.pdf

PDF 08/04 The Information Security Policy may be supported by a framework of other related policy and guidance documents

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/08-04-aberdeenshire-council-acceptable-use-policy.pdf

PDF 08/05 For some authorities it makes sense to combine information security and data protection instructions for staff. See also element 9 below.

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/08-05-ayrshire-valuation-board-data-protection-and-information-security-guidelines.pdf

Guidance to Element 9

Data protection

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

In line with the Keeper of the Records of Scotland's (The Keeper) obligations under the Public Records (Scotland) Act 2011 (the Act), the following guidance is issued regarding an authority's responsibilities under data protection legislation:

The Data Protection Act is UK-wide legislation that was first introduced in 1998 and then reintroduced in a new DP Act in 2018 to take account of the General Data Protection Regulation (GDPR) developed in the EU and adopted by the UK Government. The Data Protection Act relates to the security of information and the rights of the individual to access information held about them, and as such has major implications for public authority records management. Many authorities have formally published data protection statements. Some examples are provided below.

The Keeper expects a public authority's Records Management Plan (RMP) to include a data protection or privacy statement.

If an authority is registered as a data controller with the Information Commissioner, the Keeper would also expect them to provide him with

1. Their registration number
Each data controller should have been provided with a registration certificate and this will show the registration number. A copy of the current certificate would be good evidence.

2. Data Protection Officer
Each data controller must identify a Data Protection Officer. The Keeper will also need them to be identified in the authority's Records Management Plan. Often, but not always, this is the authority's SIRO.

3. Data Protection Policy
A data controller should develop a formal data protection policy or statement. Often this is supported by staff guidance. Both should be provided to the Keeper.

4. Online instructions for Subject Access Requests
If an authority processes (and this includes simply holding) personal information about members of the public, the authority should provide them with instructions on how to exercise their rights under data protection legislation. This should be published on an authority's website. The Keeper will need the URL in evidence.

However, it is worth noting that the Keeper does not expect a detailed list of all the record types produced by an authority that might be affected by data protection legislation. Furthermore, as the Public Records (Scotland) Act 2011 does not change existing data protection requirements, there should be no need to create a new document unless one does not already exist. If a public authority does not have a formal data protection (or privacy) statement this would be the ideal opportunity to consider creating one.

In the case that a public authority does not process personal information about members of the public, the Keeper accepts that they may have adequate processes in place to fulfil the requirements of the Data Protection Act without publishing a formal public statement. If this is the case, evidence supporting these processes should be submitted to the Keeper as part of the authority's proposed Records Management Plan.

The Information Commissioner has produced specific guidance for organisations which is available at https://ico.org.uk/for-organisations/.

Provision 57 of the Data protection Act 2018:
Data protection by design and default
(1)Each controller must implement appropriate technical and organisational measures which are designed—
(a)to implement the data protection principles in an effective manner, and
(b)to integrate into the processing itself the safeguards necessary for that purpose.[4]

Evidence

Potential evidence that data protection legislation is being properly considered by an authority might include a copy of an authority's privacy notice or data protection statement issued to all service users, or a guide to submitting subject access requests appearing

[4] Data Protection Act 2018 (legislation.gov.uk)

on an authority's website and proof of registration with the Information Commissioner's Office as required under the Data Protection Act 2018.

Sample Data Protection Documentation:

The following sample data protection schedules might give you an idea what such a document should include and how it might be styled.

Any samples should not be taken to represent the current procedures operational in the authority that provided the sample; they are for 'inspiration' only.

PDF 09/01 Most authorities have a Data Protection Policy although, as noted under element 8 above, this may be combined with an Information Security Policy or even included as part of a larger Information Governance Strategy document. Unlike the Information Security Policy is it usual for an authority to publish its Data Protection Policy or an extract from it for the benefit of service users. Therefore will be many examples online (sometimes termed 'Privacy Policy'). However, here is an examples of what should be contained in a Data protection Policy and how such a policy might be laid out.

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/09-01-nrs-data-protection-policy.pdf

PDF 09/02 It is important that members of the public (and staff) are able to exercise their subject access rights and therefore it is expected that instructions on how to pursue these rights are made available by the data controller (the public authority). Again there should be plenty of examples online, but here is a sample

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/09-02-argyll-and-bute-subject-access-request-form.pdf

PDF 09/03 The Keeper will expect evidence that staff in a public authority understand their responsibilities in regard to data protection legislation. Staff guidance is less likely to be published online.

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/09-03-scottish-funding-council-data-protection-guidance-for-staff.pdf

Guidance to Element 10

Business continuity and vital records

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

In line with the Keeper of the Records of Scotland's (The Keeper) obligations under the Public Records (Scotland) Act 2011 (the Act), the following guidance is issued to support authorities with regard to business continuity and vital records.

It is recommended that public authorities have a business continuity plan that includes access to records during an unexpected event, and that they can identify key records that facilitate the operation of the authority.

This applies whether the records kept are paper-based, digital, or both.

It is important to note that the Keeper will not want to see any information, policy documents or other material that might compromise the security of a public authority. If you have any concerns regarding this, please submit redacted samples accompanied by a short explanation of why you have taken this decision.

Evidence

The authority should provide evidence that, in the case of an emergency, recovery of records is appropriately considered.

The Keeper would expect to see evidence of this in the form of a business continuity plan or similar (featuring system/record recovery). Some authorities have an overarching business continuity policy and multiple local plans supporting the objectives of that policy. The Keeper would need to see the policy and a sample of one of the local plans.

Other potential evidence for this Element might include a 'disaster plan' or similar, or a policy approved by the senior accountable officer, identifying records that are vital to the operation of the authority, and explaining how they should be protected.

It is possible that vital records will be identified in a comprehensive information asset register (Element 4) or under the authority's retention scheduling procedures (Element 5). If this is the case, an authority would not be required to submit a separate vital records policy. However, even in such a case, reference should still be made to the recovery of vital records in the authority's RMP.

The identification of vital records and robust plans to recover them is particularly important when the authority cannot rely on the return of all records from a full immediate digital back-up.

For example, how are those vital records that are held in hard-copy format protected against loss in an emergency situation? This might mean that an authority needs a separate disaster recovery plan for its paper records.

The Keeper will expect to see evidence that staff have access to the appropriate business continuity arrangements and that these are tested routinely.

Business continuity plans may contain information that the authority considers as sensitive (a call out plan with home phone numbers for example). The Keeper has agreed that evidential documents can be heavily redacted if necessary. In lieu of evidence, s/he can also accept a guarantee from the individual identified at Element 1 (or above) confirming that business continuity arrangements are in place and are properly reviewed/tested. This Chief Executive confirmation is not normally accepted under any other Element.

Finally, it is commendable if any business continuity plan itself is listed under 'vital records'. It may be the first thing you need to access in an emergency.

Sample Business Continuity Documentation:

Guidance to Element 11

Audit trail

The location of records is known and changes recorded.

In line with the Keeper of the Records of Scotland's (The Keeper) obligations under the Public Records (Scotland) Act 2011 (the Act), the following guidance is issued regarding audit trails:

It is considered good practice that the whereabouts of records should be known at all times, and that movement of files around an electronic system or between physical storage areas should be logged.

This Element is principally concerned with an authority's ability to locate the record they are looking for. This means being able to discover a record and to be confident in identifying the correct version. This Element may also include evidence of the ability to track changes to a record, although this may be considerably harder to do in some systems (such as Network Drives) than in others.

This Element is NOT about 'auditing' records management processes; these should be covered under Element 13.

The Keeper would expect each record-keeping system described in Element 4 to be considered under this Element. For example, the processes in place to track a hard-copy file would be different from tracking something held digitally. Similarly, the procedures around locating a hard-copy file held internally will differ from those in place for recalling files from a third-party record store.

Digital records should be subject to an audit trail mechanism that registers the movement of records within an authority's record-keeping system. Electronic Document and Records Management Systems (EDRMS) and cloud platforms (such as M365) usually offer this functionality, as well as allow for the creation of audit reports and other tracking functionality.

In most cases the efficient operation of a digital document-tracking system depends on a record being searched by name. Digital record-keeping systems can be expected to search through the whole system to locate a record including, in some cases, where records can be saved in different file formats. For example, the M365 e-discovery tool can locate a record by name whether it is saved in SharePoint or in Exchange (e-mail). This makes the correct naming of records very important as the emphasis in these systems is on tracking a record by title rather than browsing through a particular container, as might have been done in a more traditional network file structure. Despite this improved tracking functionality, it is still best practice that records should be subject to

an authority-wide policy that promotes efficient management of records through a logically organised and structured hierarchical filing system, and through using appropriately named folders.

Records held on physical media, such as paper or microform, should be subject to an authority's registry system recording the movement of records around the organisation. Evidence of this might be a description of a 'paper trail' from retrieval request to return of a document to store. Such a system should ensure that the whereabouts of a particular record are known at all times.

For all records, in whatever format, a mechanism that monitors their movement and any changes to their content helps authorities ensure the records' authenticity and legal admissibility. The Keeper therefore wishes to see reference under public authority Records Management Plan (RMP) to any audit provisions, either in place or being developed, to manage record movement and version control. In many systems, version control is applied automatically, but the authority should be clear about how this automated system operates in order to remain compliant with this Element.

Some systems routinely offer functionality that allows all access to records to be logged. Where this access does not result in editing, deletion or movement of records, the Keeper will not require evidence of such access. Under the Keeper's Model Plan, Element 11 is concerned with the best practice need for authorities to know where their records are at any given time and to be aware of the need for robust version control. It is not concerned with routine business access to records that ***does not*** lead to changes or movement of records.

For certain record classes, such as adoption records, access restrictions may, however, be of primary importance. This sort of access control is properly part of Element 8 (Information Security).

British Standard 10008 states:

> *This audit trail information is needed to enable the working of the system to be demonstrated, as well as the progress of information through the system, from receipt to final deletion. Audit trails need to be comprehensive and properly looked after, as without them the integrity and authenticity, and thus the evidential weight, of the information stored in the system could be called into question.*[5]

[5] BS 10008 Evidential Weight and Legal Admissibility of Information Stored Electronically 2.15 page 79.

Evidence

The Keeper requires evidence that an authority can locate its records and that it can confidently declare these records to be true and authentic. S/he should also be confident that an authority can follow a public record through its lifecycle with all changes, movements and final disposition tracked.

The degree of audit trails required will vary according to the legislative and regulatory framework in which an authority operates.

Depending on the situation in a particular authority, potential evidence might include some of the following: a description of the search system used to locate electronic records or the paper records location system; sample ‘paper’ document movement logs version controls followed; or details of audit trails included in an EDRMS or a cloud-based system.

The Keeper understands that for some authorities a comprehensive audit trail system may not be fully functional for all of the systems explained in Element 4. However, the Keeper would require to know that authorities are working towards implementing appropriate tracking system for all records held throughout its entire operation. Evidence of any improvement project should be approved by the senior accountable officer.

For digital records held on an EDRM, cloud platform or similar, the Keeper would need confirmation that there is a ‘search’ function, and that staff have instructions how to name records in such a way that the search can be used. This is liable to require the authority to provide a naming convention document.

For digital records held on Network Drives or similar, the Keeper would need both a naming convention and a version control document (or a single document that has both). Network Drives do not automatically register a new version when a document is updated.

For hard-copy records held internally, the Keeper would be looking for evidence of some type of file registry, and an explanation of how files are appropriately annotated when they are updated (for example, a cover sheet).

For hard-copy records held externally, the Keeper would need to see evidence of tracking/retransmission arrangements. This may be a clause in the original contract.

For ‘line-of-business’ systems (see guidance to Element 4 for more on line of business), the Keeper would expect a statement to the effect that the authority is confident that the functionality of these systems allows the appropriate tracking of the records created/held.

Sample Tracking Documents:

The following sample retention schedules might give you an idea what such a document should include and how it might be styled.

Any samples should not be taken to represent the current procedures operational in the authority that provided the sample; they are for ‘inspiration’ only.

PDF 11/01-11/04 It is of fundamental importance in any records management system that records, once created, can be retrieved in an efficient manner, including the ability to determine the correct version of a document that may have been edited. To ensure this can be done the Keeper would expect a public authority to provide staff with instructions in how to save records consistently and to apply version control where this is not done automatically. Below are some examples from a public authority:

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/11-01-scottish-funding-council-creating-a-file.pdf

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/11-02-scottish-funding-council-naming-records.pdf

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/11-03-scottish-funding-council-managing-emails.pdf

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/11-04-scottish-funding-council-paper-records-storage.pdf

PDF 11/05-11/07 And similar from a local authority

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/11-05-east-renfrewshire-council-using-the-records-store.pdf

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/11-06-east-renfrewshire-council-taking-control-of-our-digital-records.pdf

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/11-07-east-renfrewshire-council-version-control.pdf

Guidance to Element 12

Competency framework for records management staff

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

In line with the Keeper of the Records of Scotland's (The Keeper) obligations under the Public Records (Scotland) Act 2011 (the Act), the following guidance is issued regarding the skills required by an authority's records manager and the training offered to all staff creating or otherwise managing records.

As part of a robust plan, the Keeper would expect to see that the individual responsible for the day-to-day implementation and operation of the RMP has the relevant skills and training to carry out the task to a reasonable standard. The Keeper will welcome proof that a public authority recognises that records management is a separate function from general office duties and will require specific resources applied in the form of training. S/he or she will also expect that the individual or individuals named in Element 2 (Responsibility – Records Manager) have access to the latest thinking in the field.

The Keeper would expect to be assured that a continuing personal development programme is available to the records manager, and be provided with evidence that a records management 'learning stream' is offered to relevant staff members.

The Keeper would expect that individuals carrying out records management in a public authority should have this task as a specific formal 'objective'.

That said, it is understood that it will not always be practical for a public authority to appoint a qualified records manager to carry out this function, and also that it may be necessary for the individual to carry out a records management function alongside other duties.

The Keeper will also expect an authority to explain what records management training has been made available to other staff in the organisation. This might be in the form of access to relevant training modules. The authority might also require a level of competence to be proved before access to certain record-keeping systems is permitted. In many cases, authorities might require staff to undergo mandatory training, perhaps renewed annually, in key areas such as information security.

Evidence

Potential evidence that an authority considers records management as a specific business activity requiring specific skills might include a copy of the records manager's annual objectives, a job vacancy description, or a statement, perhaps included as part of the records management policy (Element 3), that senior officers in the authority appreciate the specific skills required to operate an efficient records management system. This should be accompanied by an agreement that resources will be allocated to maintaining an appropriate level of competence for the records manager

It is likely that all staff will receive training on information security and data protection. This should be reported, and broad details of any training modules that can be shared with the Keeper provided.

This Element is also where an authority can explain how their records management procedures are advertised to staff. Suitable evidence might include, for example, e-mails, newsletters, or presentations.

Other suitable evidence under this Element might be an overview of a training programme, an attendance log, or a screen-shot of an e-learning portal showing information governance topics. The Keeper would particularly commend a records management component of the corporate induction syllabus.

The Keeper would also expect a general 'training' statement in the Records Management Policy (Element 3).

Sample documents showing evidence of records management training in an authority:

Any samples provided should not be taken to represent the current procedures operational in the authority that provided the sample and are for 'inspiration' only.

Guidance to Element 13

Review and assessment

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

In line with the Keeper of the Records of Scotland's (The Keeper) obligations under the Public Records (Scotland) Act 2011 (the Act) the following guidance is issued regarding self-assessment and review:

Section 1(5)(i)(a) of the Act says that an authority must keep its Records Management Plan (RMP) under review.

With this requirement in mind, the Keeper considers that it is a fundamental part of an RMP that it is reviewed

1. shortly after implementation to determine whether it is operating as expected; and
2. on a regular basis thereafter (to check that it still appropriate to the business needs of the organisation and has properly responded to the changes in circumstance that occur over time).

It is important to schedule these reviews from the outset. The Keeper expects to see provision for review in an authority's RMP.

As it is important that an authority's records management provision is properly assessed before and after the implementation of a plan, the Keeper would suggest that public authorities consider implementing a self-assessment survey of their level of records management development in advance of updating and submitting an RMP for submission. It is worth noting that the creation of this sort of 'baseline', while good practice, is not a requirement of the Act.

Under the provisions of the Act (section 5.2), the Keeper has the authority to ask a scheduled public authority to review their records management plan and submit this for (re)assessment after five years have passed since the previous review. However, it is hoped that this review will be done more frequently by the authority itself as part of a regular scheduled review.

The Keeper should be notified of any changes made to an authority's RMP, including those made as the result of a scheduled review. Internal assessment of an RMP might be facilitated by a user evaluation exercise. Larger organisations might consider the establishment of a review group.

Evidence

Evidence that an authority appreciates the importance of periodic review of its records management procedures may be detailed under the formal records management policy (Element 3).

Alternatively, evidence that this element is being properly considered may be submitted separately. This can be in the form of details of the self-assessment mechanism used with reports from assessments undertaken or underway.

An authority will be expected to explain four components of the review process in its RMP:

1. When will the RMP be reviewed?
2. Who is responsible for the review?
3. How will the results of the review be reported up to senior management for action?
4. What form will this review take? What is the methodology?

The final component might cause authorities the most difficulty when first submitting an RMP. If the authority identifies that they must select a review methodology, but have not done so at time of submission (where review may be more than a year away), the Keeper will agree this element as an Amber 'improvement plan' if. The Keeper will insist that the other components (such as responsibility for review) are in place at the outset.

Evidencing the methodology component may be also be problematic as, by definition, a review will not have taken place at the time of a first submission.

Some authorities have overcome this difficulty by providing samples of other, similar reviews that have taken place (for example many authorities created reviews for management of their GDPR preparedness in 2017/18). A statement accompanying a first submission explaining that the authority will conduct their review in a similar style to an earlier review, supported by evidence of that review, might be strong enough for the Keeper's agreement.

For subsequent submissions the Keeper should expect to see evidence of reviews taking place in the years since original agreement.

Evidence of review might include a template staff survey regarding records management operations in their local business area;
reports to management;
objectives in the responsible officer's work plan to carry out a review; or
an internal audit action plan.

Finally, you should note that while the Keeper's Progress Update Review (PUR) process is clear evidence that an authority understands the need to keep its RMP under review, it is not in itself a formal review process. PUR is a reporting mechanism; it does not suggest how an authority should carry out a review (self-assessment module, staff survey, internal audit etc.).

PDF 13/01-13/02 It is likely that a formal Records Management Plan review process will map the established review procedures in the authority. However, here are two examples of a records management self-assessment 'dashboard' used by Scottish public authorities. If not restricted to already existing systems, you could consider setting up something similar to record the review of your RMP.

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/13-01-care-inspectorate-maturity-model-screen-shot.pdf

Link: https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/13-02-nhs-forth-valley-maturity-model.pdf

Guidance to Element 14

Shared information

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

The Keeper of the Records of Scotland (The Keeper) has issued the following statement about information sharing in line with obligations under the Public Records (Scotland) Act 2011 (the Act):

Information has been shared between separate public authorities for a number of years for the benefit of clients and stakeholders, but also in the interests of efficient public services. Sharing relevant information leads to benefits for service users in the form of improved and more joined-up services. The Scottish Government positively encourages information sharing across the public sector when this benefits society in general, but particularly when it is necessary to protect vulnerable adults or children. If your authority is not currently sharing information, then it is very likely that you will be doing so in the future. An authority's Records Management Plan (RMP) must indicate what safeguards are in place to ensure that information will be shared lawfully and securely. It might, for example, include reference to information sharing protocols (ISPs), policy documents, or data sharing agreements. Samples of these, and other information sharing documentation, should be submitted as evidence that this aspect of records management is being handled appropriately.

Formal data sharing agreements, such as ISPs, are recognised by the Information Commissioner as important in helping organisations share personal information lawfully and securely. In this regard, data sharing agreements must impose practice that complies with the Data Protection Act 2018, and have regard to the Data Sharing 'Code of Practice' issued by the Information Commissioner. However, similar formal agreements should also be used for routine sharing of non-personal records (such as financial or statistical information). For both personal and non-personal information, the Keeper will expect to see an agreement around what can be shared, with whom, and when. These agreements also need to provide clauses that help practitioners make informed decisions.

Although they primarily set out the principles and general procedures for appropriately sharing information, formal data sharing agreements should also address storage and archive provision. This is particularly important for information that is of enduring value and may need to be disposed of to a place of permanent deposit. This applies whether this information is shared or jointly created.

Data sharing agreements may be an integral part of an authority's overall information governance framework which might include the following:

• An **Information Sharing Code of Practice,** outlining the organisation's intentions and commitment to information sharing and promoting good practice when sharing personal information.

• **Information Sharing Procedures**, describing the chronological steps and considerations required after a decision to share information has been made, for example, the steps to be taken to ensure that information is shared securely. Information sharing procedures set out, in detail, good practice in sharing information.

• **Privacy, confidentiality, consent (service users)**. The organisation should have in place processes and documentation for service users, such as 'Privacy/Confidentiality Statement', 'Fair Processing Notice', 'Consent', and 'Subject Access'. Relevant staff within the organisation must understand these processes and be able to access documentation when required.

Although not an exhaustive list, the following are the most obvious issues that an information sharing protocol might cover:

- Needs-based sharing: a statement on why it is necessary to share information with specific partner organisations, describing the framework which will allow this to happen.
- Fairness and Transparency: a statement on how the authority will advertise and make known their intention to share information.
- Information Standards: a statement on the authority's commitment to maintain accurate and up-to-date information.
- Retention of Shared Information: a statement on the retention schedule governing the information being shared.
- Security of Shared Information: a statement on the mechanisms in place to ensure the security and safety of the information being shared.
- Access to Personal Information: a statement on how Subject Access Requests (SARs) will be dealt with.

- Freedom of Information: a statement on how the authority will deal with requests legislation about their information sharing practices and policies under FOISA.

- Review: a statement on how the authority intends to keep its protocol under review to ensure it continues to protect the rights of individuals, and remains fit for purpose.

  Public authorities should consider whether to publish their data sharing practice documentation.

  Audit Scotland have provided a sample 'Code of Data Matching Practice'. This code deals specifically with the sharing of personal information for the purposes of fraud detection. However, the general principles around which the code has been based have been approved by the UK Information Commissioner and may be considered to have general application when developing procedures that allow data sharing for other purposes. Appendix 2 of this code gives examples of text that might be used to alert the public to the potential sharing of their personal data:
  Link: http://www.audit-scotland.gov.uk/docs/central/2010/nr_101112_nfi_data_matching_practice.pdf

  It is important to recognise that this Element does not refer to one-off events, such as an authority responding to an FOI enquiry. Rather, it covers routine information sharing, for example one public authority providing monthly updates to another to allow them both to pursue their functions. However, Element 14 does cover the management of records created in shared projects. For example, when two or more public authorities combine for a specific limited purpose, there should be processes put in place to manage any records created during that activity – especially after the project ends.

  To give a hypothetical example:

  a) If a social work department of a council sends information about a child to Police Scotland, they should do so under the terms of an Information Sharing Protocol. The Keeper would need to see a sample of such a protocol, and be satisfied that it is clear whose record it is, and what will happen to the Police copy of the record.

  b) If there is then a multidisciplinary group put in place around the child with a meeting between the police, the council and the local health board, one of the earliest decisions that must be made is what happens to the record of their deliberations. Which of the partners will be responsible for managing the records of the group? This is liable to be stated in a standard protocol if these sorts of meetings regularly occur. The Keeper would need to see a sample of such a protocol.

c) Finally, if it is then determined that a new general procedure needs to be developed and representatives of council, police and health board are sequestered from their normal jobs to work together for six months to create a new policy, it should be decided at the outset who will take the records management role. In this case, because this is new situation, a ‘terms of reference’ style document may be drawn up. The Keeper would need to see this and to check that the management of the records created the new group have been properly considered.

Evidence

Potential evidence that an authority undertakes information sharing in a controlled and suitable manner might include formal policy documents such as protocols or codes of practice; a copy of a data sharing agreement or ISP (redacted if necessary); public statements about the handling of personal information; or a project governance document detailing responsibilities for records created during and beyond the life of the project.

It is likely that a public authority may have more than one separate data sharing arrangement to consider. If this is the case, the Keeper simply requires a sample in evidence; s/he does not need to view every data sharing agreement pursued by an authority.

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.

In line with the Keeper of the Records of Scotland's (The Keeper's) obligations under the Public Records (Scotland) Act 2011 (the Act), the following guidance is issued regarding an authority's obligations to public records being created by third party organisations, when delivering a public function under contract to a public authority scheduled under the Act.

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 a function of the public authority, are not public records under the Act.

It is important to make clear that the Act applies only to named authorities. The Keeper's authority as regulator of the Act does not extend to private, commercial, charitable or public bodies not named under the Schedule to the Act even if they are delivering the functions of named public authorities. The obligation to ensure that public records being created or held as described above lies entirely with the named authority.

This guidance is therefore designed to help named authorities meet their obligations to those public records being created and held on their behalf, by third parties contracted to supply one or more of their public functions.

It is a fundamental requirement of a records management plan that it can satisfy the Keeper that public records being created or held by third party organisations are being properly managed, in line with the public authority's records management plan. This will be best achieved by the named authority providing the Keeper with evidence of how it satisfies itself that the third party can meet this requirement.

Evidence

The Keeper will expect to see evidence under an authority's records management plan of the processes it follows in order to provide it with the necessary assurances that third party organisations, when contracted to deliver a public function on its behalf, can robustly manage the public records it will create and hold as a consequence.

Such evidence would include the contractual paperwork that provides for the arrangement. It could also include policies and procedures created and followed by the authority in the process of running a reliable, transparent and credible procurement procedure.

Procurement guidance for authorities and contractors

This guidance, '*Records Management Clauses for Contractors'* and the "*Guidelines for Contractors'*, sets out general good records management practice that all named authorities and third party contractors should consider, before embarking on a procurement exercise. **https://www.scottisharchives.org.uk/resources/arms/**

Contractual arrangements

Sample documents, regarding contractual arrangements which safeguard public records created and/or held by a third party, might give you an idea of what such a document should include and how it might be styled. Examples of contractual arrangements between a public authority and third party contractor:

PDF 01. The Service Level Agreement template of the commissioning authority, NHS Ayrshire and Arran, provides an example of a clause which sets out the expectations of the commissioning authority on its third party, in relation to fulfilment of PRSA obligations - http://www.nrscotland.gov.uk/files/record-keeping/public-records-act/element-15-nhs-ayrshire-and-arran.pdf

PDF 02. Food Standards Scotland have adopted standard Scottish Government terms and conditions for all contracts. The template contracts used for whichever function is being contracted, whether for goods or services, clearly set out the arrangements for information and records governance which ensure compliance with the authority's Records Management Plan - http://www.nrscotland.gov.uk/files/record-keeping/public-records-act/element-15-food-standards-scotland.pdf

PDF 03. The Scottish Prison Service have developed minutes of agreement with third party contractors, which set out requirements for compliance with all SPS records management policies and procedures - http://www.nrscotland.gov.uk/files/record-keeping/public-records-act/element-15-scottish-prison-service.pdf

Policy commitment

The inclusion of third party records in the named authority's own records management policy would indicate a strategic commitment by the authority to ensure robust records management is extended to third party contractors.

PDF 04. Dumfries and Galloway Council's Records Management Policy includes a statement establishing the scope and purpose of the policy, which includes specific reference to third parties who create, capture or maintain records relating to council functions - http://www.nrscotland.gov.uk/files/record-keeping/public-records-act/element-15-dumfries-and-galloway-council.pdf

Appendix 1

Glossary of terms used in this document

Administrative Records - Records relating to those general tasks or activities performed within an organisation that are common to all businesses or organisations, such as maintenance of resources, care of the physical plant or other routine office matters. Also known as housekeeping records.

Audit Trail – The mechanism by which an organisation monitors use of a record. This could include recording when it is consulted, edited or disposed of.

Authority/Public Authority – For the purpose of the Public Records (Scotland) Act 2011, a body that appears in the schedule to the Act: http://www.legislation.gov.uk/asp/2011/12/schedule/enacted
This schedule can be amended under the terms of section 2.2 of the Act.

Business Activity – An umbrella term covering all the functions, processes, activities and transactions of an authority, and its employees. This includes public administration as well as commercial business.

Business Classification Scheme -
An intellectual structure that categorises business functions/activities or subjects to preserve the context of records relative to others. It is useful for aiding activities such as retrieval, storage and disposal scheduling of records.

Business Continuity – A system in place that ensures that the activities of an organisation can carry on in the event of major disruption.

Competency Framework – Formal document showing the skills required for a post, in this case posts relating to records management. Often this will be divided into ‘essential’ and ‘desirable’ skills. A competency framework may or may not include required formal qualifications.

Content (of a plan) – The various parts of a records management plan that, combined, make up a complete plan that might be agreeable to the Keeper. The Keeper's Model Plan calls these parts 'elements'.

Data Protection – Issues around the Data Protection Act 2018, the main purpose of which is the protection of private information about living people and to confirm that an individual has the right to know what information is held about them. N.B. The Data Protection Act does not give members of the public the right to access the actual records held by a public authority.

Destruction – The system of disposal of records by permanently destroying them and the recording that such action has been taken.

Disposal – The decision as to whether the record should be destroyed, transferred to an archive service for permanent preservation, or presented and the putting into effect of that decision.

Disposal Schedules – Schedules that identify types of records and specify how long they will be kept before they are destroyed, designated for permanent preservation or subject to further review.

Document – Information or data fixed in some medium, which may or may not be considered in whole or in part an official record.

Electronic Document and Records Management System (EDRMS) – An electronic system or process – managed with the aid of computers and software – implemented in order to manage both electronic documents and electronic records within an organisation. Electronic document and records management systems combine the functions of document and records management.

Element – In this document, the term used to signify a component part of a record management plan. There are 14 elements in the Keeper's Model Plan and s/he would expect them all to be considered by an authority before submitting their Records Management Plan (RMP).

File Plan – Scheme showing the records created by an organisation. In larger public authorities each department is likely to have its own file plan. For the purposes of the Act the Keeper will not expect to see file plans submitted by authorities in support of their RMP.

Folder - A type of aggregation or container within a file system used to store records (and other folders). In an electronic environment, an assembly of one or more documents grouped together because they relate to the same subject, activity or transaction. The folder is the principal building block of a file plan.

Form (of a plan) – For the purposes of the Public Records (Scotland) Act 2011 the term 'form' refers to the physical media in which an authority's records management plan is submitted. It does not refer to textual content or to the internal structure of such a plan.

Freedom of Information – Issues around the Freedom of Information (Scotland) Act 2002 – known as FOI(S)A – this Act introduced a statutory right of access to all types of recorded information of any age held by Scottish public authorities, subject to certain conditions and exemptions. The Act is promoted and enforced by a fully independent Scottish Information Commissioner.

Guidance Document – This document. It is designed to assist public authorities who are in the process of creating a records management plan that will be robust enough to gain agreement of the Keeper. The Guidance Document points to many other pieces of guidance and to sample documents.

Information Security – The process by which information is protected from unauthorised use (including amendment and disposal). This includes issues regarding intellectual and physical access and the appropriateness of document storage.

Keeper of the Records of Scotland - The NRS is headed by the Keeper of the Records of Scotland, who is responsible to the Scottish Ministers for the management of the NRS and to the Lord President of the Court of Session for the efficient management of the court and other legal records in Scotland. The office of Keeper of the Records of Scotland was created in 1949, although its antecedents date back to the 13th century.

Metadata – Information about the context within which records were created, their structure and how they have been managed over time. Metadata can refer to records within digital systems, for example event log data. It can also refer to systems such as paper files that are controlled either from a digital system or by a register or card index, for example the title and location. In a robust records management system, metadata should 'travel' with the record to ensure provenance is retained.

Model Records Management Plan – Document produced by the Keeper of the Records of Scotland that shows the elements s/he considers should be addressed in the records management plans of all public authorities.

National Records of Scotland - From 1 April 2011, the General Register Office for Scotland merged with the National Archives of Scotland to become the National Records of Scotland (NRS): http://www.nrscotland.gov.uk/

Permanent Preservation – The principle that some material created by an authority will be of enduring value and will be preserved beyond its business use.

Public Authority - For the purpose of the Public Records (Scotland) Act 2011, an organisation that appears in the schedule to the Act: http://www.legislation.gov.uk/asp/2011/12/schedule/enacted
This schedule can be amended under section 2.2 of the Act.

Public Records – For the purpose of this document, this refers only to records that are subject to the Public Records (Scotland) Act 2011.

Public Records (Scotland) Act 2011 - http://www.legislation.gov.uk/asp/2011/12/contents/enacted

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

Records Management - The practice of formally managing records within a system (electronic and/or paper) including classifying, capturing, storing and disposal.

Records Management Plan – A formal statement by which an organisation explains the procedures it has in place to ensure the proper management of its records. A public authority, if it appears in the schedule to the Public Records (Scotland) Act 2011, will be required to have its records management plan agreed by the Keeper of the Records of Scotland.

Records Manager – The individual (or occasionally individuals) with responsibility for prosecuting an organisation's records management plan. The person who other staff look to for records management advice and, in a public authority, the first point of contact for the National Records of Scotland regarding records management issues.

Retention Schedule – Document showing how the records of an organisation will be treated over time. For example how long after creation they should be destroyed.

Retrieval/Tracking – The mechanism by which an organisation notes record movement.

Self-Assessment – Review of systems carried out internally by an organisation for its own internal benefit. The Guidance Document points to published record management self-assessment tools that can be used for this purpose.

Senior Manager – For the purpose of the Act, the officer in an organisation who gives approval to its records management plan and by doing so sanctions its use throughout the relevant business areas. For many public authorities this may well be the Chief Executive.

Shared Information – A record created by an organisation and then passed to another for agreement, amendment or use OR a record created by two or more organisations jointly using a shared platform.

Vital Records – The fundamental records of an organisation required for it to operate. An appreciation of which these records are is considered a major part of business continuity.

Appendix 2

Formal Records Management Standards

The following standards can be purchased from: http://shop.bsigroup.com/

ISO 15489-1:2001
Records Management: Part 1: General

ISO 15489-2:2001
Records Management Part 2: Guidelines

ISO 30300:2011
Management systems for records - Fundamentals and vocabulary

ISO 30301:2011
Management systems for records - Requirements

ISO 23081-1:2006
Records management processes - Metadata for records - Part 1: Principles

ISO 23081-2:2009
Managing metadata for records - Part 2: Conceptual and implementation issues

ISO 23081-3:2011
Managing metadata for records - Part 3: Self-assessment method

ISO 2700:2005
Information technology, security techniques, information security management systems - Requirements
ISO 16175-1:2010
Principles and functional requirements for records in electronic office environments - Part 1: Overview and statement of principles

ISO 16175-2:2011
Principles and functional requirements for records in electronic office environments - Part 2: Guidelines and functional requirements for digital records management systems

ISO 16175-3:2010
Principles and functional requirements for records in electronic office environments - Part 3: Guidelines and functional requirements for records in business systems

BS 10008:2008
Evidential weight & legal admissibility of electronic information. Specification.

BIP 0008-1:2008
Evidential weight & legal admissibility of information stored electronically – Code of practice for the implementation of BS 10008

BIP 0008-2:2008
Evidential weight & legal admissibility of information transferred electronically – Code of practice for the implementation of BS 10008

BIP 0008-3:2008
Evidential weight & legal admissibility of linking electronic identity to documents – Code of practice for the implementation of BS 10008

Electronic records management
MoReq2
MoReq2 is short for “Model Requirements for the Management of Electronic Records”, second version. It consists of a formal requirements specification for a generic electronic records management system, accompanied by testing documentation and related information. These might be used as a framework to guide development of new electronic records management systems:

https://irms.org.uk/page/moreq2

Appendix 3

Published Records Management Plans

Aberdeenshire Council and Licensing Board

Angus Council and Licensing Board

City of Edinburgh Council and Licensing Board

Ethical Standards for public life in Scotland

Crown Estate Scotland

Dumfries and Galloway Council

Dunbartonshire and Argyll and Bute Valuation Joint Board

Glasgow City Council

Highland and Western Isles Valuation Joint Board

Historic Environment Scotland

Integration Joint Board-Midlothian

Inverclyde Council and Inverclyde Licensing Board

Judicial Appointments Board for Scotland

NHS Forth Valley Records

NHS Greater Glasgow & Clyde

NHS Lanarkshire

NHS Lothian

NHS National Waiting Times Centre Board aka NHS Golden Jubilee National Hospital

NHS Orkney

NHS Tayside

Scottish Borders Council and Licensing Board

Scottish Courts and Tribunals Service

Scottish Parliament, Corporate Body and Scottish Commissioner for Public Audit

Scottish Sports Council (SportScotland)

South East of Scotland Transport Partnership

South Lanarkshire Council and Licensing Board

South West of Scotland Transport Partnership

West Lothian Council