NHS Tayside

Records Management Plan

Version 1.0

Version:	1.0
Document Type:	Action Plan
Owner/Author:	Lynda Petrie obo Corporate Records Compliance Group
Review Date:	April 2018

DOCUMENT CONTROL SHEET:

Key Information:

Title:	NHS Tayside Records Management Plan
Date Published/Issued:	April 2016
Date Effective From:	5 May 2016
Version/Issue Number:	1.0
Document Type:	Action Plan
Document Status:	Approved
Author:	Lynda Petrie, obo Corporate Records Compliance Group

Revision History:

Version:	Date:	Summary of Changes:	Name:
0.1	December 2015	Establish RMP	L Petrie
0.2	March 2016	Update evidence documents and statements	L Petrie
1.0	April 2016	Finalise evidence documents and statement for submission to Keeper of the Records of Scotland	L Petrie

Review:

This plan will be reviewed every two years (or sooner if new legislation, codes of practice or national standards are to be introduced).

Introduction

Records management is the systematic control of an organisation's records, throughout their life cycle, in order to meet operational business needs, statutory and fiscal requirements, and community expectations. Effective management of information allows fast, accurate and reliable access to records, ensuring the timely destruction of redundant information and the identification and protection of vital and historically important records.

Effective records management involves efficient and systematic control of the creation, storage, retrieval, maintenance, use and disposal of records, including processes for capturing and maintaining evidence.

Systematic management of records allows organisations to:

- know what records they have, and locate them easily
- increase efficiency and effectiveness
- make savings in administration costs, both in staff time and storage
- support decision making
- be accountable
- achieve business objectives and targets
- provide continuity in the event of a disaster
- meet legislative and regulatory requirements
- protect the interests of employees, clients and stakeholders

The guiding principle of records management is to ensure that information is available when and where it is needed, in an organised and efficient manner, and in a well maintained environment.

The importance of good records management has been brought into sharp focus by the 2007 Historical Abuse Systemic Review of Residential Schools and Children's Homes in Scotland by Tom Shaw ('the Shaw Report'). The recommendations of the Shaw Report and the subsequent 2009 review by the Keeper of the Records of Scotland led to the Public Records (Scotland) Act 2011 ('PRSA') in March 2011.

The Act makes provision about the management of public records by named public authorities. Provisions include the preparation of a Records Management Plan ('RMP') setting out and evidencing proper arrangements for the management of the authority's public records, and its submission for agreement by the Keeper. Each Board's Health Records and Corporate Records Management Policies should provide further detail concerning standards for the management of records.

The PRSA defines a record as "Anything in which information is recorded in any form." A record can be recorded in computerised or manual form or in a mixture of both. Data can be held on a range of media, including text, sound, image, and/or paper. Increasingly records are being kept on electronic and document management systems. Records may include such things as hand-written notes; emails and correspondence; radiographs and other imaging records; printouts from monitoring equipment; photographs; videos; and tape-recordings of telephone conversations.

Public Records (Scotland) Act 2011 – Records Management Plan

Under the Public Records (Scotland) Act 2011 Scottish public authorities must produce and submit a records management plan setting out proper arrangements for the management of the organisations records to the Keeper of the Records of Scotland for his agreement under Section 1 of the Public Records (Scotland) Act 2011.

NHS Tayside Records Management Plan (RMP) sets out the overarching framework for ensuring that [Board] records are managed and controlled effectively, and commensurate with the legal, operational and information needs of the organisation. The RMP considers all 14 elements as advised in the Keeper's Model RMP and supporting guidance material. The 14 elements are:

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

The RMP defines NHS Tayside's Action Plan for improving the quality, availability and effective use of records in NHS Tayside and provides a strategic framework for all records management activities.

NHS Tayside's Records Management Plan is effective from 5 May 2016. This plan is to be continuously reviewed and updated. Reports will be submitted to the Corporate Records Compliance Group quarterly and annually to the Information Governance Committee.

Summary of Evidence

1.1 Health Records Strategy and Management Policy
1.2 Records Management Policy
1.3 Information Governance Policy
1.4 Policy Development, Review and Control Policy
1.5 NHS Tayside Code of Corporate Governance
1.6 Letter from CE supporting and endorsing RMP
2.1 Head of Health Records Job Description
2.2 Corporate Records and Web Manager Job Description
3.1 Records Creation and Registration Policy
3.2 Records Retention Schedules Policy
3.3 Health Records Committee Terms of Reference
3.4 Corporate Records Compliance Group Terms of Reference
3.5 Internal Audit Report T35/12 - Records Management
3.6 Health Records Operational Guidance and Service Operating Procedures
3.7 Screenshot of electronic policy tracker
3.8 Vital Signs 593 - Policy Tracker
4.1 NHS Tayside Departmental RMP Template
4.2 Acute Medical Unit Record Management Plan
4.3 Corporate Services Record Management Plan
4.4 Electronic document store metadata matrix
4.5 Records Management Responsibilities Presentation
6.1 Waste Management Policy
6.2 Equipment Disposal Report October 2013
6.3 Copy certificate of destruction of health records
6.4 Copy certificate of destruction of confidential waste from Stracathro
6.5 Copy of Mitie Confidential Waste Skips Feb 16 (Ninewells and Claverhouse)
6.6 Statement from IT regarding back ups and destruction of electronic records
6.7 IT Equipment Disposal process
6.8 Maryfield destruction arrangements
7.1 Weblink to list of records held by University of Dundee Archive
7.2 Original agreement with University of Dundee Archivist
8.1 System Access Policy
8.2 Use of Email and Network Services Policy
8.3 Portable Computing and Removable Media Policy
8.4 using e-mail in NHST good practice guide
8.6 System Security Policy and Secure Operating Procedure Template
8.7 Information Risk Assessment Template
8.8 sample system security policy - Mobile Health Application
8.9 sample system security policy - Wardview
8.10 Screenshot of LDAP application form
8.11 Screenshot of system access management staffnet page
8.12 DL(2015)17 Director Letter Information Governance
8.13 SBAR CEO DL2015(17) Information Governance and Security Improvement Measures

2015-2017

8.14 IGC February 2016 Item 4a IG and IS Improvement Plan December 2015
8.15 SBAR Info Gov Committee about DL(2015)17
8.16 Report to Info Gov Committee about Information Security Framework May 2015
9.1 NHS Tayside Data Protection Register details
9.2 Data Protection Policy
9.3 Caldicott Approval Procedure
9.4 Caldicott Data Processing Specification
9.5 Caldicott Approval Form
9.6 InfoAware User Guide
9.7 InfoAware Course Details
9.8 InfoAware Information Governance Update Report January 2015
9.9 Information Governance Committee - FairWarning Report
9.10 LearnPro Information Governance Training Record September 2014
9.11 FairWarning Alerts Manager's Guidance
9.12 Link to data protection webpages
10.1 Business Continuity Plan Template
10.2 Corporate Business Continuity Plan
10.3 NHS Tayside Major Incident Plan
10.4 eHealth ICT Detailed Recovery Plan
10.5 Internal Audit Report T26-13 Resilience Planning
10.6 Internal Audit Report T44-13 Data Management, Security and Business Continuity
10.7 IT Business Continuity Factors Summary
10.8 Managed Hosting Services Definition V1.0
10.9 Business Continuity ICE Service Provision Review
10.10 PROTECT NHS Scotland - Health Board IT Resilience Review
10.11 PROTECT ICT Resilience Review Terms of Reference
10.12 Quarterly BC Update 7th Edition
10.13 Quarterly BC Update 14th Edition
10.14 Letter to Keeper of the Records covering Element 10
10.15 Health Records Business Continuity Plan
11.1 Version Control Guidance
11.2 Screenshot of version control in document store
11.3 Screenshots from learnpro module describing various drives
11.4 Screenshot of health records case record tracking
11.5 TrakCare Project Governance Documents
12.1 Health Records Management LearnPro module
12.2 Health Records Manager record of training
12.3 InfoAware Training records to end September 2014
12.4 Vital Signs - IG Information handling in Practice (September 2013)
12.5 Vital Signs - Safe Information handling (May 2013)
12.6 Vital Signs - Looking After Information (June 2014)
12.7 Database - medical records staff qualifications
12.8 Corporate Records and Web Manager record of training
12.9 Records management workshops poster 2013
12.10 Records Management Presentation to department RM leads April 2014

12.11 Vital Signs – Information Governance Update (April 2016)
13.1 Report to Directors Meeting December 2015
13.2 Agenda of Directors Meeting December 2015
13.3 Extract from Action Note of Directors Meeting December 2015
13.4 Report to Information Governance Committee February 2016
13.5 Agenda of Information Governance Committee February 2016
13.6 Minute from Information Governance Committee February 2016
13.7 Report to Corporate Records Compliance Group December 2015
13.8 Corporate Records Compliance Group Agenda December 2015
13.9 Corporate Records Compliance Group Action Note December 2015
14.1 Sharing Information with the Police Policy
14.2 Information Sharing Protocol Scottish Prison Service
14.3 Information Access Protocol
14.4 Scottish Accord on the Sharing of Personal Information (SASPI)
14.5 Email Information Transfer Protocol
14.6 Guidance for completing the Email Information Transfer Protocol
14.7 Draft Health and Social Care Integration Infrastructure and Data Sharing Joint Issues
14.8 Tayside Health and Social Care Integration Joint Issues Minute March 2014
14.9 Tayside Data Sharing and Improvement Board Minute April 2014
14.10 NHS Tayside Integration Scheme Framework May 2014
14.11 Tayside Data Sharing and Improvement Board Workshop Report April 2014

Element 1: Senior Management Responsibility (Guidance)			
Element Requirement:	**NHS Tayside Statement:**	**Corporate Evidence:**	**Actions:**
Identify an individual at senior level who has overall strategic accountability for records management.	**The senior individual** *(Board level)* who has overall strategic responsibility for records management is Ms Lesley McLay, Chief Executive.	• 1.1 Health Records Strategy & Records Management Policy, section 2.6 – Roles & Responsibilities. • 1.2 Records Management Policy, section 5 – Responsibilities. • 1.3 Information Governance Policy – Section 5 - Organisation arrangements. • 1.4 Policy Development, Review and Control Policy –All NHS Tayside policies are in line with the 'Policy Development, Review & Control Policy' which requires that all polices state the Policy Manager and Policy Review group. • 1.5 NHS Tayside Code of Corporate Governance – Section 2.2.6 outlines the Chief Executive has overall strategic accountability for records management.	No further action required.

		• 1.6 Letter from CE of NHS Tayside supporting and endorsing RMP.	

Element 2: Records Manager Responsibility (Guidance)			
Element Requirement:	**NHS Tayside Statement:**	**Corporate Evidence:**	**Actions:**
Identify individual within the authority, answerable to senior management, to have day-to-day operational responsibility for records management within the organisation.	The records manager who has responsibility for development and operation of Corporate Records Management is Mrs Lynda Petrie, Corporate Records and Web Manager. The records manager who has responsibility for development and operation of Health Records Management is Mrs Ruth Anderson.	• 2.1 Head of Health Records Manager job description. • 2.2 Corporate Records and Web Manager job description. • 1.6 Letter from CE of NHS Tayside supporting RMP and outlining responsibilities.	No further action required.

Element 3: Records Management Policy Statement (Guidance)

Element Requirement:	NHS Tayside Statement:	Corporate Evidence:	Actions:
A records management policy statement that describes how the authority creates and manages authentic, reliable and usable records, capable of supporting business functions and activities for as long as they are required.	NHS Tayside is committed to a systematic and planned approach to the management of records within the organisation, from their creation to their ultimate disposal. This will ensure that NHS Tayside can: ▪ control the quality, quantity and security of the information that it generates; ▪ maintain that information in an effective manner whilst ensuring compliance with the recommendations of the appropriate authorities. NHS Tayside has an approved and current Records Management Policy. NHS Tayside has a policy development, review and control policy. This policy details how policies should be communicated throughout the organisation and outlines the duties of managers in respect of this.	• 1.1 Health Records Strategy & Records Management Policy. • 3.1 Records Creation & Registration Policy. • 1.2 Records Management Policy. • 3.2 Records Retention Schedule. • 3.3 Health Records Committee Terms of Reference. • 3.4 Corporate Records Compliance Group Terms of Reference. • 3.5 Internal Audit Report T35/12 – Records Management. • 3.6 Health Records Operational Guidance. • 1.4 Policy Development, Review and Control Policy.	No further action required.

		• 3.7 Screenshot of electronic policy tracker. • 3.8 Vital Signs 593 – Policy Tracker.	

Element 4: Business Classification (Guidance)

Element Requirement:	NHS Tayside Statement:	Corporate Evidence:	Actions:
A business classification scheme that reflects the functions of the authority. Demonstrating at a given point in time, the information assets the business creates and maintains, and in which function or service they are held.	NHS Tayside recognises that a robust Business Classification Scheme (BCS) is the keystone of the records management function within NHS Tayside. There is currently a BCS for records managed within the Electronic Document Store. All users must adhere to this and it is outlined in each departmental RMP which must be completed before a user is provided with access to the use the EDS to manage records. A department RMP template is provided to department as a basis. NHS Tayside has initiated work to develop a Business Classification Scheme for all records in future, with plans to build on current department RMPs. The organisational BCS will aim to provide a framework for managing NHS Tayside records and information, and will be developed in partnership with each business unit and function, to ensure that it meets specific operational requirements.	• 3.1 Records Creation & Registration Policy. • 4.1 NHS Tayside Department Records Management Plan Template. Sample Departmental RMPs: • 4.2 Acute Medical Unit Record Management Plan. • 4.3 Corporate Services Record Management Plan. • 4.4 Electronic Document Store Metadata Matrix. • 4.5 Records Management Responsibilities Presentation. • 4.6 Information Asset Owners and Administrators Handbook.	The Corporate Records Compliance Group will oversee the development of the BCS for NHS Tayside. An implementation plan for roll out of the Business Classification Scheme and Information Asset Register is to be developed. This will be added to the published RMP when ready. It is expected this roll-out across the board area will take around three to five years.

	The Information Governance team are developing an Information Asset Register and working with departments to facilitate them taking ownership of their identified Information Assets.		

Element 5: Retention Schedules (Guidance)			
Element Requirement:	**NHS Tayside Statement:**	**Corporate Evidence:**	**Actions:**
A retention schedule that detail the procedures that the authority follows to ensure records are routinely assigned to disposal dates and that they are subsequently destroyed at the appropriate time, or preserved permanently by transfer to an approved repository or digital preservation programme.	The Board maintains corporate records retention schedules and a health records strategy and management policy, both of which are approved by NHS Tayside's Information Governance Committee. These are produced in line with the current NHS Records Management Code of Practice and other relevant guidance and standards. These are subject to review every two years or earlier in the case of significant regulatory change. These schedules are available electronically on NHS Tayside's intranet, Staffnet and are communicated to staff through the process outlined in the policy development review and control policy and the electronic policy tracker.	• 3.2 Records Retention Schedule • 1.1 Health Records Strategy & Management Policy • 1.4 Policy Development, Review and Control Policy • 3.6 Health Records Operational Guidance • 1.4 Policy Development, Review and Control Policy • 3.7 Screenshot of electronic policy tracker • 3.8 Vital Signs 593 – Policy Tracker.	No further action required.

Element 6: Destruction Arrangements (Guidance)			
Element Requirement:	**NHS Tayside Statement:**	**Corporate Evidence:**	**Actions:**
Demonstrate that proper destruction arrangements are in place. Disposal arrangements must also ensure that all copies of a record – wherever stored – are identified and destroyed.	The Board has procedures for managing the confidential destruction of expired records in all formats, in a way that is auditable and irreversible. NHS Tayside has a variety of contractors who dispose of confidential paper records. Evidence supplied shows a copy of certificates from the various contractors who provide this service. Records are destroyed in accordance with CAREB NP 803.11 (non clinical waste) a document which is owned by National Procurement and NSS. (Commercial in confidence document) Staff log a call with the Service Desk when they want any IT **equipment** disposed of and Endpoint Services arrange to collect it and dispose of it via the process outlined in evidence 6.7. When a record is deleted from a shared drives, it is permanently removed after 8 weeks when the backup is overwritten (6.6) For records in the electronic document	• 3.2 Records Retention Schedules. • 3.6 Health Records Operational Guidance. • 6.1 Waste Management Policy. • 6.2 Equipment Disposal Report – October 2013 (includes destruction certificates). • 6.3 Copy certificate of destruction of health records. • 6.4 Copy certificate of destruction of confidential waste from Stracathro • 6.5 Copy of Mitie Confidential Waste Skips Feb 16 (Ninewells and Claverhouse). • 6.6 Statement from IT regarding backups and destruction of electronic	No further action required

	store, when a document reaches its Expiry Date it is no longer available for access within the Electronic Document Store. However, the file is still available on our 'Network Attached Storage' which is part of the Oracle UCM environment that stores the system's document files with related metadata. On a monthly basis we delete the expired content using the Oracle UCM Archiver facility which then deletes the files/metadata permanently.	records. • 6.7 IT Equipment Disposal process. • 6.8 Maryfield destruction arrangements.	

Element 7: Archiving and Transfer Arrangements (Guidance)			
Element Requirement:	**NHS Tayside Statement:**	**Corporate Evidence:**	**Actions:**
Detail the authority's archiving and transfer arrangements, ensuring that records of enduring value are deposited in an appropriate archive repository.	Records identified as having enduring value or are of historic interest are transferred to the Archivist at Dundee University. There is an arrangement dated back to 1987, however NHS tayside is keen to improve links between itself and the Dundee University Archive. Health records are not routinely archived permanently as health records are destroyed in line with NHS Tayside's Health Records Policy, with the exception of a small sample that are sent to the Dundee University Archive for enduring interest value. Corporate records for permanent or long term retention are stored in NHS Tayside's Electronic Document Store.	• 7.1 Weblink to List of Records held by University of Dundee Archivist. • 7.2 Original agreement with University of Dundee Archivist. • 1.1 Health Records Strategy & Records Management Policy.	NHS Tayside should formalise the arrangements with the University of Dundee for archiving records. It is expected this to be achieved within two years and the RMP will be updated when this has been achieved.

Element 8: Information Security (Guidance)

Element Requirement:	NHS Tayside Statement:	Corporate Evidence:	Actions:
Ensure provision for the proper level of security for its public records. The security procedures must put in place adequate controls to prevent unauthorised access, destruction, alteration or removal of records.	NHS Tayside provides systems which maintain appropriate confidentiality security and integrity for all data including storage and use in line with the NHSS Information Security Policy Framework 2015. NHS Tayside is responsible for ensuring that adequate physical controls are put in place to ensure the security and confidentiality of all health and business sensitive data, whether held manually or electronically. The NHSS Information Security Policy Framework commenced in 2015 and has replaced both the NHSS Information Security Policy (2006) and the NHSS Information Assurance Strategy (2011-2015). The new framework, which is aligned to ISO27001, sets out a number of improvement measures. These improvement measures form the basis of a revised NHS Tayside Information Governance and Security Improvement Plan 2015-2017	• 8.1 System Access Policy. • 1.3 Information Governance Policy. • 8.2 Use of e-mail and Network Services Policy. • 8.3 Use of Portable Computing and Removable Media. • 8.4 Using e-mail in NHST Good Practice Guide. • 8.6 System Security Policy & Secure Operating Procedure Template. • 8.7 System risk assessment form. Sample System Security Policies: • 8.8 Mobile Health Application. • 8.9 Wardview.	No further action required.

		• 8.10 Screenshot of LDAP Application Form. • 8.11 Screenshot of System Access Management page. • 8.12 DL(2015)17 Director Letter Information Governance. • 8.13 SBAR CEO DL2015(17) Information Governance and Security Improvement Measures 2015-2017. • 8.14 IGC February 2016 Item 4a IG and IS Improvement Plan December 2015. • 8.15 SBAR Info Gov Committee about DL(2015)17. • 8.16 Report to Info Gov Committee about Information Security Framework May 2015. • 12.11 Vital Signs – Information Governance Update (April 2016).	

Element 9: Data Protection (Guidance)			
Element Requirement:	**NHS Tayside Statement:**	**Corporate Evidence:**	**Actions:**
Demonstrate compliance with the authority's data protection obligations.	NHS Tayside is responsible for large volumes of personal and sensitive personal data subject to the Data Protection Act 1998 and, in the case of patient data, the Caldicott Principles. All NHS Scotland staff are bound by the NHS Code of Confidentiality. Fairwarning software is deployed within NHS Tayside and detects unauthorised or inappropriate access to our information systems. NHS Tayside is registered with the ICO and our registration number is Z8537226. NHS Tayside publishes on their website details about data protection and how to make subject access requests.	• 9.1 NHS Tayside Data Protection Register details. • 9.2 Data Protection Policy. • 9.3 Caldicott Approval Process guidance. • 9.4 Caldicott data processing specification. • 9.5 Caldicott approval form. • 9.6 InfoAware User guide. • 9.7 InfoAware course details. • 9.8 InfoAware uptake report January 2015. • 9.9 Information Governance Committee – September 2013. Fairwarning progress report. • 9.10 LearnPro uptake report – 30 September	No further action required.

		2014. • 9.11 Fairwarning Alerts Managers guidance. • 9.12 Link to data protection pages on website.	

Element 10: Business Continuity and Vital Records (Guidance)			
Element Requirement:	**NHS Tayside Statement:**	**Corporate Evidence:**	**Actions:**
Detail arrangements in support of records vital to business continuity.	NHS Tayside has corporate, departmental and service Business Recovery/Continuity Plans. These plans provide information for the applications used and their manual workarounds. Business Continuity Plan owners have been issued with information relating to the 15 critical agreed services supported by IT and this information will also form part of the new template. In the event of fire, flood or any other circumstance where paper case records would be unavailable the Health Records Department would invoke the Health Records Business Continuity Plan. If paper case records were destroyed by fire/flood NHS Tayside would then rely on patient information captured on electronic systems, including Patient Administration System, Clinical Portal and individual clinical systems. NHS Tayside backs up information from its shared drives and electronic document stores to disk arrays hosted at two independent sites. After the	• 10.1 Business Continuity Plan template. • 10.2 Corporate Business Continuity Plan – overarching business continuity plan. • 10.3 NHS Tayside Major Incident Plan. • 10.4 eHealth ICT Detailed Recovery Plan. • 10.5 Internal Audit report T26/13 – NHS Resilience. • 10.6 Internal Audit report T44/13 – Data Management, Security & Business Continuity (Continuity of eHealth services) . • 10.7 Advice to BCP owners - T Business Continuity factors summary. • 10.8 Managed Hosting	NHS Tayside recognises that should an incident occur all its vital records are sufficiently protected and backed up. However, should there be significant hardware failure there may be a time delay in accessing vital records. We propose to address this gap in provision and identify potential solutions to ensure time sensitive vital electronic records will always be available.

	backup is complete, each copies itself to the other one, meaning backup copies reside at alternate sites in case of site loss. Backup is carried out daily and kept for 8 weeks. After 8 weeks the disk is overwritten by the 9th week's backup. These disks do not require to be disposed of. .	Services Definition – May 2014 – To be redacted for website. • 10.9 Example - ICE Service Provision Review. • 10.10 PROTECT Health Board IT Resilience Review report. • 10.11 PROTECT Terms of Reference. • 10.12 Quarterly BC Update 7th Edition. • 10.13 Quarterly BC Update 14th Edition. • 10.14 Letter to the Keeper regarding BC from the Board Secretary. • 10.15 Health Records Business Continuity Plan.	

Element 11: Audit Trail (Guidance)

Element Requirement:	NHS Tayside Statement:	Corporate Evidence:	Actions:
Provide evidence that the authority maintains a complete and accurate representation of all changes that occur in relation to a particular record. An audit trail is a sequence of steps documenting the movement and/or editing of a record resulting from activities by individuals, systems or other entities.	NHS Tayside has adopted naming conventions and version control. This guidance is part of the NHS Tayside Records Management Policy. Training on this will be included with the roll out of the Business Classification Scheme descried in element 4. NHS Tayside has an Electronic Document Store to electronically store vital corporate records. The document store creates and records version control every time a new version of a record is checked in/out. NHS Tayside recognises there are challenges around managing records on department shared drives. To start addressing this a LearnPro module 'IT Security and Good Practice' has been created with a section titled: file management. This module has been mandated as compulsory and will be included as part of the corporate induction for all new starts in the organisation. The module is in testing phase at the moment and is planned to go live in Summer 2016. An improvement plan will then follow to address longer term management and usage of shared drives.	• 11.1 Version Control Guidance. • 11.2 Screenshot of version control in document store. • 11.3 Screenshot from learnpro module describing the shared drives. • 11.4 Screenshot of health records tracking module. • 11.5 TrakCare Project Governance Documents. • 3.1 Records Creation & Registration Policy. • 1.3 Information Governance Policy.	An Improvement plan will be developed to address long term management of organisational shared drives.

	Health records are currently tracked electronically within NHS Tayside's Patient Administration System (TOPAS). NHS Tayside will be moving to tracking case records via iFIT (TrakCare) which is an advanced tracking system. The tracking of movement and changes to records is undertaken by all staff involved in the handling of patient case records. The TrakCare programme will deliver a replacement to TOPAS. The planned programme of work will see the replacement system being available during the early part of 2017. A formal project governance structure has been formed. The programme of work will deliver suitable Disaster Recover and Business Continuity Plans for NHS Tayside.		

Element 12: Competency Framework for Records Management Staff (Guidance)			
Element Requirement:	**NHS Tayside Statement:**	**Corporate Evidence:**	**Actions:**
Detail a competency framework for person(s) designated as responsible for the day-to-day operation of activities described in the elements in the authority's RMP.	NHS Tayside will provide appropriate training and development support to ensure all staff are aware of their records management responsibilities. This has taken the form of drop in workshops and presentations to department RM leads. Vital Signs have also been issued to all staff on Information Governance issues. NHS Tayside has produced a Learnpro module about managing Health Records. The Head of Health Records and 8 other staff within Medical Records are fully qualified members of IHRIM. The Corporate Records and Web Manager is educated to university degree level in core business subjects. She participates in and attends conferences, webinars and training events around records management where resource allows. This, along with on the job	• 4.5 Records Management Responsibilities Presentation. • 12.1 Health Records LearnPro module. • 12.2 Health Records Manager record of training. • 12.3 InfoAware Training records to end September 2014. • 12.4 Vital Signs – IG Information handling in Practice (September 2013). • 12.5 Vital Signs – Safe Information Handling Training (May 2013). • 12.6 Vital Signs – Looking After Information (June 2014). • 12.7 Database - Medical Records staff completion	No further action required

	learning and over 10 years NHS experience has helped to provide the Corporate Records and Web Manager with a good grounding in the key concepts of records management and how to implement these. This will ensure that the post-holder will be sufficiently able to ensure NHS Tayside complies with the requirements of the Act.	of Certificate of Technical competency (delivered by the Institute of Health Records & Information Management (IHRIM). • 12.8 Corporate Records and Web manager record of training. • 12.9 Records management workshops poster 2013. • 12.10 Records Management Presentation to department RM leads April 2014. • 12.11 Vital Signs – Information Governance Update (April 2016).	

Element 13: Assessment and Review (Guidance)			
Element Requirement:	**NHS Tayside Statement:**	**Corporate Evidence:**	**Actions:**
Detail the procedures in place to ensure regular self-assessment and review of records management systems in place within the authority.	The Corporate Records and Web Manager will regularly review NHS Tayside's Records Management Plan and report to the Corporate Records Compliance Group (CRCG). A corporate records improvement plan will be developed to project manage all the work required to fulfil the commitments made within this plan. The Public Records (Scotland) Act is a standing item on the NHS Tayside CRCG agenda, which meets quarterly. Progress reports are submitted for each meeting. This group reports to the Information Governance Committee which in turn reports to the Finance Resources Committee, a standing committee of Tayside NHS Board. The progress of the Records Management Plan will also be reviewed by NHS Tayside Internal Audit Service.	• 3.4 Corporate Records Compliance Group Terms of Reference. • 13.1 Report to Directors Meeting December 2015. • 13.2 Agenda of Directors Meeting December 2015. • 13.3 Extract of action note of discussion at Directors Meeting December 2015. • 13.4 Report to Information Governance Committee – February 2016. • 13.5 Agenda of Information Governance Committee February 2016. • 13.6 Minute of IG Committee February 2016. • 13.7 Report to Corporate Records Compliance Group – December 2015. • 13.8 Corporate Records	No further action required.

		Compliance Group Agenda December 2015. • 13.9 Corporate Records Compliance Group Action Note December 2015. • 3.5 Internal audit report T35/12.	

Element 14: Shared Information (Guidance)			
Element Requirement:	**NHS Tayside Statement:**	**Corporate Evidence:**	**Actions:**
Provide evidence that the authority has considered the implications of information sharing of good records management. Include reference to information sharing protocols that govern how the authority will exchange information with others and make provision for appropriate governance procedures.	Sharing of information is a core NHS Scotland activity and takes place in line with the Data Protection Act 1998 and other relevant privacy regulation. All sharing of information is subject to the appropriate level of risk assessment. NHS Tayside has relevant sharing agreements in place with partner organisations.	• 14.1 Sharing Information with the Police Policy. • 14.2 Information Sharing Protocol - Prison service. • 8.4 NHST Email Usage Policy. • 9.3 NHST Caldicott Approval Procedure. • 14.3 Information Access Protocol. • 14.4 SASPI (NHS Tayside & Local Authorities). • 14.5 E-mail Information Transfer Protocol template. • 14.6 Guidance on completing the E-mail Information Transfer Protocol. • 14.7 Health and Social Care Integration Partnership Working	NHS Tayside should undertake a gap analysis of existing Sharing Protocols and put in place a work plan to address identified gaps.

		Across Agencies: Infrastructure and Data Sharing Joint Issues report. • 14.8 Tayside Health and Social Care Integration Joint Issues minute 19 March 2014 • 14.9 Tayside Data Sharing & Improvement Board minute 28 April 2014. • 14.10 NHS Tayside Integration Scheme Framework May 2014. • 14.11 Tayside Data Sharing & Improvement Board workshop report April 2014.	

Guidance to Element 1: Senior Management Responsibility

Identify person at senior level who has overall strategic responsibility for records management. This is a compulsory element under the terms of the Public Records (Scotland) Act: Section 1(2)(a)(i).

In line with the Keeper of the Records of Scotland's obligations (the Keeper) under the Public Records (Scotland) Act 2011 (the Act) the following guidance is issued regarding the identification of senior person to have overall strategic responsibility within the organisation.

It is required by the Act that an authority's records management plan (RMP), submitted for agreement with the Keeper, has the support of that authority's senior management team. 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 Keeper in agreeing an authority's RMP will need to be assured that the overall strategic responsibility for records management is held at a senior level and that, if all information functions are not part of the same command, there are close working relationships between them. The Keeper will therefore require evidence to be submitted confirming the name, the job title of the senior responsible officer with overall responsibility for the RMP that has been submitted for agreement.

Evidence:

Evidence of compliance could take the form of a covering letter or, perhaps more properly, the signature of the senior accountable officer on the records management policy (Element 3). The identification of an individual is specifically mentioned in the Act 1(2)(a)(i) and a name must be supplier. Neither a job title (i.e. 'CEO') nor a collective body (i.e. 'XXX' City Council') is acceptable under the terms of the Act.

Guidance to Element 2: Records Manager Responsibility

Identify individual within the organisation, answerable to senior management, to have operational responsibility for records management within the organisation. This is a compulsory element under the terms of the Act.

The Keeper in agreeing an authority's RMP will wish to be assured that proper provision has been established for the day-to-day management of the authority's records. The Keeper will therefore require evidence to be submitted confirming the name and job title of the person or persons responsible for the day-to-day operation of the activities described in the authority's RMP. The Keeper will expect an authority to name an individual rather than simply a job title.

It is vital that an authority's records management plan (RMP) submitted for agreement with the Keeper confirms that an individual has been appointed to have overall day-to-day responsibility for the implementation for the authority's RMP.

All staff members who create records should be made aware of the organisations 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 records manager of equivalent. The Keeper's Model Plan says 'This person should be the National Records of Scotland's initial point of contact for records management issues' and this may be the easiest way for an authority to identify the correct person to list in this element.

Evidence:

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. This person would be the Keeper's first point of contact for day-to-day records management issues. The identification of an individual is specifically mentioned in the Act 1(2)(a)(ii) and a name must be supplied. Neither a job title (i.e. 'Records Manager') nor a collective body (i.e. 'Finance Department') is acceptable under the terms of the Act.

Guidance to Element 3: Records Management Policy Statement

A records management policy statement underpins effective management of an authority's records and information. It demonstrates to employees and stakeholders that managing records is important to the authority and serves as a mandate for the activities of the records manager. This is a compulsory element under the terms of the Public Records (Scotland) Act 2011: Section 1(2)(b)(i).

It is important that an authority's records management plan (RMP), submitted for agreement with the Keeper, confirms that the authority has developed a records management policy governing 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 statement 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.

The records management policy document should 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.

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

Evidence:

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.

Guidance to Element 4: Business Classification

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

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.

The purpose of this element is to demonstrate that the records management plan takes account of the complete organisation and all its various business functions. This process will assist an authority in making good retention or disposal decisions under each of these business functions. To properly fulfil this element, an authority will need to demonstrate that its business classification scheme can be applied to the record management systems which it operates.

Evidence:

As evidence of a business classification the Keeper would expect to see a hierarchical representation of the functions of an authority and a clear indication of the business areas responsible for delivering these functions to the public.

The Keeper does not initially require authorities to provide him with evidence down to file plan or information asset register level for each business area. He does, however, expect an authority to be able to classify its functions, the areas of the authority delivering these to the public and an indication of the classes for records being created or held by each business area.

Clearly, if an authority has a detailed and mature business classification scheme that provides a functional or organisational overview of all the authority's information assets the Keeper would be happy to receive it. However, at this early stage of implementation a clear indication that an authority understands where its record creating are and the types of record they create of hold will suffice. Any improvement plan, supported by senior accountable officer sign-off, and committing the authority to the development of a robust business classification scheme in the future, will attract the agreement of the Keeper.

Guidance to Element 5: Retention Schedule

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

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, record 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 record 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 archive service for permanent preservation, and the putting into effect of that decision.

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 records generated during the course of the daily business of the organisation and ensures continuity, protects the organisation's legal rights and preserves information for the archives.

Evidence:

An authority should provide the Keeper with a retention schedule showing that it understands how long certain types of record 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.

Guidance to Element 6: Destruction Arrangements

It is not always cost-effective or practical for an authority to securely destroy records in-house. Many authorities engage a contractor to destroy records and ensure the process is supervised and documented. This is a compulsory element under the terms of the Public Records (Scotland) Act 2011 Section 1 (2)(b)(iii).

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.

Using a commercial disposal firm for the disposal of records other than electronic 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 must be able to issue a certificate of destruction that 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 clear proof of controlled destruction of information that the Information Commissioner would be looking for in any disputed request which the institution was unable to answer.

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 (all formats) and evidence that this process is properly carried out.

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 would not be considered evidence that record destruction is actually taking place in an authority.

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

Guidance to Element 7: Archiving and Transfer Arrangements

This is the mechanism by which an authority transfers records of enduring value to an appropriate archive repository, specifying the timing of transfers and other terms and conditions. This is a compulsory element under the terms of Public Records (Scotland) Act 2011 Section 1 (2)(b)(iii).

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 electronic 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 that procedures for facilitating such transfers are in place and are followed.

The Keeper will expect to see evidence of the processes in place as part of an authority's RMP. Such evidence might include memoranda of understanding between an authority and an archive repository, an internal schedule of preservation of an explanation of how automated systems archive electronic records and details of how metadata transfers with those records.

The Keeper does not wish to dictate what records an authority chooses to preserve, but it is a requirement for a robust RMP that a formal **process** for transferring records for permanent preservation exits. 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.

Evidence:

Potential evidence of compliance would include a formal policy, approved by the senior accountable officer; a memorandum of understanding or deposit agreement with an archive repository or receipts form such a repository as evidence of records deposited over time and by agreement.

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

Guidance to Element 8: Information Security

Information security is the process by which an authority protects its records and ensures they remain available. It also maintains privacy where appropriate

and provides for the integrity of the records. This is a compulsory element under the terms of the Public Records (Scotland) Act 2011 Section 1 (2)(b)(ii).

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 an information security code should advise staff. As part of the full RMP the Keeper would expect to see that such a code exists and is generally available to staff involved in the creation of records. As evidence he will also want to view the authority's code.

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 only, perhaps accompanied by a short explanation of why you have taken this decision.

As well as the security of the information contained in a record, an authority must consider the physical safety of documents (in whatever format). This would include attending to the proper storage of paper records and the protection of servers if they are used to sore electronic 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.

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 and staff information security manuals, regulations and/or circulars and routine information security reports or updates to senior management.

Guidance to Element 9: Data Protection

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

The Data Protection Act is UK-wide legislation and was introduced in 1998. It relates to the security of information and the rights of the individual to access information held about them. Therefore, it has major implications for public authority records management. Many authorities have formally published data protection statements.

The Keeper might expect a public authority's records management plan to include a data protection or privacy statement. This would normally be a document explaining how an authority treats personal information and how a member of the public can determine what information that authority holds about them. Therefore, the Keeper would welcome a high-level, public facing statement (known as a 'privacy statement'

in some organisations). However, the Keeper would not expect a detailed list of records that might be affected by data protection legislation.

If an authority already has a published data protection policy, this should be submitted. 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.

A public authority may have adequate processes in place to fulfil the requirements of the Data Protection Act without publishing a formal 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.

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; a guide to submitting subject access requests appearing on an authority's website or proof of registration with the Information Commissioner's Office as required under the Data Protection Act 1998.

Guidance to Element 10: Business Continuity and Vital Records

A business continuity and vital records plan serves as the main resource for the preparation for, response to, and recovery from, an emergency that might affect any number of crucial functions in an authority.

It is recommended that public authorities have a business continuity plan and that they can identify key records that facilitate the operation of the authority.

This applies whether the records kept are paper based, electronic or, most likely, a hybrid of the two.

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 only, perhaps accompanied by a short explanation of why you have taken this decision.

Evidence:

Potential evidence for this element might include a 'disaster plan' or similar, and 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 retained.

It is possible that vital records will be identified in a comprehensive business classification scheme (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 policy. However, even in such a case, reference should still be made to business continuity in the authority's RMP.

If an authority is genuinely unable to provide evidence of their business continuity/disaster plan or vital records policy because to do so would, for example, compromise the authority's security, a statement from the senior accountable officer

explaining that this is the case would be perfectly acceptable to the Keeper under the spirit of the Act.

Guidance to Element 11: Audit Trail

An audit trail is a sequence of steps documenting the movement and/or editing of a record resulting from activities by individuals, systems or other entities.

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

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 is known at all times.

Electronic records should be subject to an audit trail mechanism that records the movement of records within the IT infrastructure or out of the IT infrastructure. Electronic Document and Records Management Systems (EDRMS) usually offer this functionality and allow for the creation of audit reports, but a great deal of electronic records created by public authorities remain unstructured and are not subject to content management systems. Electronic records that are therefore held on network drives for which there is no in-built audit trail functionality, should be subject to an authority wide policy that promotes efficient management of records, through a logically organised and structured hierarchical filing system, using appropriately named electronic folders.

For all records, in whatever format, a mechanism that monitors their movement and changes to content helps authorities to ensure their authenticity and supports legal admissibility. The Keeper therefore wishes to see reference under public authority RMPs to audit provisions in place or being developed to manage record movement and version control.

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.

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 formal policy, approved by the senior accountable officer, governing access permissions; 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.

The Keeper understands that for some authorities a comprehensive audit trail system may still be some way off. However, the Keeper would require to know that authorities are working towards implementing an appropriate system(s) for all records

held throughout its entire operation. Evidence of an improvement project should be approved by the senior accountable officer.

Guidance to Element 12: Competency Framework for Records Management Staff

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

As part of a robust plan, the Keeper would expect to see that the individual(s) responsible for the implementation and operation of the overall RMP has the relevant skills and training to carry out the task to a reasonable standard. He 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. He will also expect that the individual or individuals named in (Element 2) 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 individuals who are carrying out records management in a public authority should have this as a specific formal 'objective'.

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 would be accompanied by an agreement that resources will be allocated to maintaining an appropriate level of competence in this business activity.

Guidance to Element 13: Review and Assessment

Regular assessment and review of records management systems will give an authority a clear statement of the extent that its records management practices conform to the Records Management Plan as submitted and agreed by the Keeper.

The Keeper considers that it is fundamental part of a records management plan (RMP) that it is reviewed:

- Shortly after implementation to determine whether it is operating as expected.
- On a regular basis thereafter to check that it sill appropriate to the business needs of the organisation and has properly responded to the changes in circumstances that occur over time.

With this in mind it is important to schedule these review from the outset. The Keeper would expect to see some provision for review in an authority's RMP.

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 should consider implementing a self assessment survey of their level of records management development, before creating a RMP for submission. This 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 after five years. It is hoped that this review will be done more frequently by the authority itself.

The Keeper should be notified of any changes made to an authority's RMP including those made as the result of a scheduled review.

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 already undertaken, **or** that are underway.

Guidance to Element 14: Shared Information

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

Information has been shared between 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 improved and more joined-up services. Scottish Government positively encourages information sharing across the public sector when it 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 likely that you will be doing this in the future. An authority's RMP must indicate what safeguards are in place to ensure that information will be shared lawfully and securely. It will for example include reference to Information Sharing Protocols (ISPs). Policy documents, protocols, agreements and other information sharing documentation should be submitted as evidence that this aspect of records management is being handled appropriately.

ISPs are not a legal requirement under the terms of the Data Protection Act 1998, but they are recognised by the Information Commissioner as important in helping organisations share information lawfully and securely. ISPs create a routine around

what can be shared, with whom and when and help practitioners make informed decisions. In this regard ISP's must propose practice that complies with the Data Protection Act 1998 and have regard to the Data Sharing Framework issued by the Information Commissioner.

ISPs primarily set out the principles and general procedures for appropriately sharing information, but they should also address storage and archive provision. This is particularly important for information stored or jointly created that is of enduring value and may need to be disposed of to a place of permanent deposit. ISPs under these circumstances will need to consider storage and archive arrangements.

Evidence:

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