Records Management Plan

Integration Joint Board

Version.	Records Management Plan Version 1.3.
Owner.	Chief Officer.
Date Approved.	
Date for Review.	April 2028.

Version.	**Date.**	**Status.**	**Prepared By.**	**Reason for Amendment.**
1.1.	22.03.22.	Approved.	Gavin Mitchell, IJB Standards Officer.	Address typographical errors, reflect changes in personnel and job titles, and confirm place of publication of Records Management Policy.
1.2.	29.01.24.	Approved.	Shaun Hourston-Wells, Acting Strategic Planning Lead.	Biennial review.
1.3.	17.03.26.	Draft.	Shaun Hourston-Wells, Policy and Performance Manager.	Biennial review.

Contents

Introduction

The Public Records (Scotland) Act 2011 (hereafter referred to as "the Act"), came fully into force in January 2013. The Act obliges the Board and other public authorities to prepare and implement a records management plan (RMP). The RMP sets out proper arrangements for the management of records. The plan is agreed with the Keeper of the Records of Scotland (the Keeper) and reviewed by the Board on a biennial basis.

The Board's Records Management Plan is based on the Keeper's published Model Records Plan. The plan has 15 Elements:

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.
15. Public records created or held by third parties.

The Board has provided the Keeper with evidence of policies, procedures, guidance, and operational activity on all elements of the Plan.

The Plan was agreed with the Keeper on 5 February 2021 and was reviewed by the IJB on 22 March 2022, 21 February 2024 and, again, on 22 April 2026.

The Board's RMP relates to records throughout their lifecycle, from creation and acquisition, to archive and destruction.

For more information about the Public Records (Scotland) Act 2011, visit the website of the National Records of Scotland.

A copy of the Act can be viewed online via The National Archives website.

About Integration Joint Boards

The integration of health and social care is part of the Scottish Government's programme of reform to improve care and support for those who use health and social care services. It is one of the Scottish Government's top priorities.

The Public Bodies (Joint Working) (Scotland) Act 2014 provides the legislative framework for the integration of health and social care services in Scotland.

It has put in place:

- Nationally agreed outcomes, which apply across health and social care, in service planning by Integration Joint Boards and service delivery by NHS Boards and Local Authorities.
- A requirement on NHS Boards and Local Authorities to integrate health and social care budgets.
- A requirement on Partnerships to strengthen the role of clinicians and care professionals, along with the third and independent sectors, in the planning and delivery of services.

Records Management in the Board

The records of the Board constitute an auditable account of the authority's activities, which provides evidence of the business, actions, decisions and resulting policies formed by the Board.

Records represent a vital asset, which support the functions of the Board. Effective record keeping supports efficiency, consistency, and continuity of work. It ensures that the correct information is captured, stored, maintained, retrieved, and destroyed or preserved in accordance with business need, statutory and legislative requirements.

Records management is an essential part of enabling the Board to achieve priority outcomes that reflect what is most important to the people and communities of Orkney, as set out in the Board's Strategic Plan available on the Board's website. The Board maintains a Records Management Policy and procedures and practices across all its service areas. These are based upon the requirements of the Public Records (Scotland) Act 2011, records management best practice and the principles detailed below.

Records Management Principles

The following principles drive activities relating to records management:

- Records are a valuable resource and must be managed as such.
- Records are maintained in accordance with legislation.
- Records are stored within record keeping systems, rather than in personal filing.
- Records are shared and not duplicated.
- Records are stored in a consistent manner that reflects the Board's functions.
- Records are appropriately secured.
- Records are easily accessible for as long as they are required.
- Records that are identified as vital are protected.
- Records that are identified as of historical significance are preserved.

- Records are disposed of in accordance with approved Records Retention Schedules.
- Records management procedures are understood by all staff and staff are appropriately trained.
- Records management is a responsibility of all staff.
- Records management practices adhere to the Board's policy, procedures, and standards.
- Records keeping systems are compliant with the requirements to manage records throughout their lifecycle.
- Records management practices will support the Board's values.

Records Covered by this Plan

In line with the Act, all records created in the carrying out of the Board's functions (whether directly or by third parties) are public records. Part 1, section 3.1 of the Act states that:

"... "public records", in relation to an authority means –

(a). Records created by or on behalf of the authority in carrying out its functions.

(b). Records created by or on behalf of a contractor in carrying out the authority's functions.

(c). Records created by any other person that have come into the possession of the authority or a contractor in carrying out the authority's functions."

Records Management Systems and the Board

The Board uses four main types of records management systems:

- Manual filing systems.
- IT applications and databases (that process records for specific functions e.g. HR, Purchasing, Housing Management etc.).
- Corporate Electronic Documents and Records Management System (EDRMs).
- Electronic documents stored on a shared drive using Windows Folders.

All records management systems are subject to records management policy, procedures, guidelines, and elements of this Plan.

The 15 Elements of the Board's Records Management Plan

1: Senior Management Responsibility

Senior Management responsibility for the Records Management Plan lies with the Chief Officer for the Board.

Responsibility for providing advice on data protection and advising on and monitoring compliance with data protection laws, lies with the Board's Data Protection Officer, namely the Head of Corporate Governance for Orkney Islands Council.

For enquiries relating to the Records Management Plan, please contact:

Chief Officer, Orkney Health and Care, School Place, Kirkwall, Orkney, KW15 1NY.Telephone: 01856873535, email: ohacfeedback@orkney.gov.uk.

2: Operational Records Management Responsibility

The point of contact for the operation of records management within the Board is the Council's Information Governance Officer.

For enquiries relating to Records Management, please contact:

Information Governance Officer, Orkney Islands Council, School Place, Kirkwall, Orkney, KW15 1NY. Telephone: 01856873535, email: OHACfeedback@orkney.gov.uk.

3: Records Management Policy Statement

The Board's commitment to effective records management is set out in its Records Management Policy published on the website of Orkney Islands Council and is subject to ongoing monitoring and annual review.

Online guidelines and procedures are available to staff. This is supported by online training and ready access to the Information Governance Officer for advice.

The Board uses a series of different systems that manage documents and records, such as folders on SharePoint, within the Council, and these systems will be reviewed and, where necessary, plans put in place to ensure that the systems apply the Board's Records Management policies.

4: Business Classification

The Board uses the Scottish Council on Archives Records Retention Schedule (SCARRS) as the basis of its Business Classification Scheme.

The Board recognises the importance and benefits of organising its information in such a way that facilitates business efficiency and information management and has developed a business classification scheme covering all functions of the Board:

- Governance documents.
- Equalities.
- Human resources.
- Appointment of members of the Board.
- Finance.
- Management and Administration.
- Policies and Procedures.
- Strategic Planning.
- Oversight of Services.

The Business Classification Scheme is developed in a structure that supports the business activities of the Board. The Board is structured in three tiers:

- Level 1: functions.
- Level 2: activities.
- Level 3: transactions.

The Board has combined its Business Classification Scheme and Records Retention and Disposal Schedule.

Some records and documents are held in personal drives and personal email accounts which makes them effectively inaccessible to other officers and means that they are not effectively managed by the Board. To help manage the amount of information held in shared drives and email accounts, the Council's EDRMS Project is continuing with the process of making SharePoint available as a repository for records and introduce new procedures, including the automatic deletion of emails for most accounts after a period.

The deployment of EDRMS in the Council requires file plans to be developed, to accommodate strict security models, whilst facilitating information sharing, and the application of retention scheduling. Whilst this process is largely complete, it is still in the process of being made available across all Services.

5: Retention Schedules

The Board has developed a Retention and Disposal Schedule with records organised according to the Business Classification Scheme (element 04). The Schedule also lists those Vital Records that would be required for ensuring that the Board can implement its Business Continuity Plans.

The Retention and Disposal Schedule covers all the Board's records and draws together into a single reference document all existing statutory, regulatory, and best practice retention and disposal arrangements. The Board has adopted the Scottish Council for Archives records retention schedule model (SCARRS) as the basis for its Retention and Disposal Schedule and has mapped its schedule to its Business Classification Scheme. The Retention and Disposal Schedule applies to both electronic records and paper records.

Requests for changes to the Schedule should be made to the Information Governance Officer, who maintains the Schedule: Information Governance Officer, Orkney Islands Council, School Place, Kirkwall, Orkney, KW15 1NY. Telephone: 01856873535, email: OHACfeedback@orkney.gov.uk.

The Schedule is located on the IJB Governance page of the Board's website here.

Non-current operational records are stored in the main offices of the Board, and there will be no requirement to find alternative long-term storage within the five-year lifetime of this Records Management Plan and well into the lifetime of any subsequent Plan. The Orkney Library and Archive service provides a service for the preservation of historical records. This resource manages the retention and disposal

of these records and works with the Board to identify records for archival, preservation or destruction.

Standards for records retention are built into any contracts and agreements with third parties who share or process information on the Board's behalf.

6: Destruction Arrangements

The Board recognises that a disposal policy secures the position of the Board and helps every member of staff in their day-to-day work.

The Board has procedures for the disposal of records. The procedures require disposals to be:

- Authorised.
- Appropriate.
- Secure and confidential.
- Timely.
- Documented.

Destruction of highly sensitive hard-copy records will be supervised by an appropriate officer.

Disposals of hard drives will be disposed of securely by the Orkney Islands Council IT Service in accordance with the Council's Information Security Policy.

Data in other electronic business systems will be deleted in such a way that prevents reconstruction.

7: Archiving and Transfer Arrangements

Orkney Library and Archive provide facilities for the preservation of historical records.

The official records of the Board will form a part of Orkney Library and Archive. Archiving and transfer arrangements are detailed within the County's Archive "Procedure for Appraising which Records should be Transferred to the Archive Service" and within the IJB's approved records retention schedules.

The archivist is responsible for deciding which records are to be kept permanently after liaising with the appropriate service areas. The Orkney Archive Service has adopted clear principles approved to help ensure that records which document the principal actions of the Board and its officials, the rights of the islanders and the community experience are identified and preserved.

Records identified in the Retention and Disposal Schedule as being suitable for permanent preservation will be transferred from the Board's Records Store to Orkney Library and Archive. Transfer is undertaken using Council employees directed by the Board, using Council vehicles.

Records received in Orkney Library and Archive are documented on an Accession Receipt Form prior to entry in the Archive catalogue.

8: Information Security

Board records are held on IT systems provided by Orkney Islands Council or, in the case of paper records, stored on Council premises. Most staff who manage and have access to Board records are employees of the Council. The Joint Clinical and Care Governance Committee records are held on NHS systems. However, these records are subject to the appropriate NHS Orkney Policy and Procedures. The Board has, therefore, decided that it is appropriate to adopt and follow the Council's Policy and Procedures. The Board's staff, the Chief Officer, employed by NHS Orkney, and the Chief Finance Officer, employed by Orkney Islands Council, are already required by their employment contracts to comply with their respective employer's Information Security Policy, guidance, and procedures.

Orkney Islands Council's Information Security Policy is a high-level document which sets out the Council's strategic direction regarding information security.

The Policy is based on the seven principles of information security listed below:

1. Data Protection – Ensuring data is protected.
2. Relevance and Consistency – Ensuring the controls in place to ensure information security are relevant to the risk, proportionate and applied consistently across the organisation.
3. Security is an Enabler – Viewing information security as a means of assisting rather than hindering the business strategy.
4. The Right Access – Employees require the right access to effectively do their job coupled with the principle of least privilege, but how can we share information securely to improve efficiencies and effectiveness.
5. Plan for the Unexpected – Regardless of vigilance vulnerabilities will emerge as new attacks occur, and malware mutate. Orkney Islands Council must anticipate this and be prepared.
6. Security for the Whole Lifecycle – Security should be considered from the start of a project and not bolted on later.
7. Accountability – It must be possible to hold authorised users of information accountable for their actions.

To ensure effective implementation in practice, this policy is underpinned by guidelines. The Corporate Information Security Staff Guidance booklet, published by Orkney Islands Council, gives advice on information security, use of the internet at work, email, and mobile devices. It also provides guidance on taking information out of the workplace, using IT equipment at home and what to do if something goes wrong. It also explains how ICT facilities may be used and the conditions in place relating to individual use. This booklet is provided to all staff who manage or have access to Board records and staff are instructed to follow this guidance.

All staff who manage or have access to Board records are required to complete an online Information Security course.

Governance

The Council's Head of Property and Asset Management champions information security and provides strategic leadership and reports to the Council's Corporate Leadership Team (CLT). The Board's Chief Officer is a member of this CLT. Professional advice and guidance are provided by the Council's Information Security Officer.

The Council's Corporate Leadership Team sets the strategic direction in relation to information security and ensures resources for implementation. The fact that Information Security is represented at board level demonstrates its level of importance to Orkney Islands Council.

Orkney Islands Council has engaged the services of a CLAS consultant to advise on matters of infrastructure and operational security. A CESG CHECK compliant organisation is used to provide independent IT Health Checks to ensure that systems are compliant.

CESG is the Communications Electronic Security Group.

CLAS is the CESG Listed Advisor Scheme.

CHECK is an assurance scheme for security testers managed by the CESG.

9: Data Protection

Data Protection legislation is enforced and promoted by the Information Commissioner, who provides guidance and advice on complying with the terms of Data Protection legislation and investigates complaints regarding possible breaches of the obligations contained within this legislation.

The Information Commissioner maintains a register of Notifications listing all Data Controllers in the UK. Data Controllers are required to register the types of personal data processed by them, the purposes of that processing and the third parties with whom the personal data may be shared. The Board is registered with the Information Commissioner's Office as a data controller and its registration number is ZA207653.

The Board has appointed the Council's Head of Corporate Governance as its Data Protection Officer.

The Board does not handle any personal information relating to service users or patients that has not already been pseudonymised or anonymised. The only personal data handled by the Board relates to its two members of staff, the Chief Officer, and the Chief Finance Officer, who are employees of NHS Orkney and Orkney Islands Council respectively, and members of the Board. The Board has decided to adopt and follow the Council's Data Protection Policy and Data Protection Procedure. As employees of the Council or NHS Orkney, the Board's staff are required by their employment contracts to comply with the Council or NHS Orkney Data Protection Policy and Procedure, as appropriate.

The Data Protection legislation regulates the processing of personal data by the Board. The General Data Protection Regulation (the 'Regulation') and the Data Protection Act 2018 give individuals rights which are:

- The right to be informed about how their information will be used.
- The right of access to their personal information.
- The right to rectification, which is the right to require the Board to correct any inaccuracies.
- The right to request the erasure of any personal information held by the Board where the Board no longer has a basis to hold the information.
- The right to request that the processing of their information is restricted.
- The right to data portability.
- The right to object to the Board processing their personal information.
- Rights in relation to automated decision making and profiling.

The General Data Protection Regulation sets out six data protection principles which must be complied with when the Council is processing personal data. The six principles require that personal data is:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and, where necessary, kept up to date.
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

The Council's Data Protection Policy and Data Protection Procedures set out the responsibilities of members of staff.

Both the Council and NHS Orkney have a Data Protection Policy to ensure compliance with the requirements of the Data Protection legislation. The Policies will be regularly reviewed. In addition, the Council has developed Data Protection Procedures and Guidance for officers to ensure compliance with the responsibilities of the Council when processing personal data. This includes policies and procedures for the use of mobile electronic devices, the use of Council email and internet systems, the application of passwords to electronic information, the disposal of IT hardware and a general records management policy.

All staff employed within the Orkney Health and Social Care Partnership, who manage or have access to Board records, are required to undertake data protection training to ensure that personal data is processed in accordance with the data protection principles. This training will be refreshed annually and is reinforced

through the year with ongoing guidance provided by the Council and Health Board to staff employed within the Orkney Health and Social Care Partnership.

10: Business Continuity and Vital Records

The Vital Records are those records which the IJB and services will need to implement their Business Continuity Plans. The IJB's vital records are set out in the IJB's Retention and Disposal Schedule.

The Business Continuity 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.

The IJB's records are managed by the Council and are subject to the policies and procedures of the partner body in relation to business continuity. Business Continuity Plans for the Council services responsible for the IJB's records, are in place.

All services will continue to be provided or commissioned directly by NHS Orkney or Orkney Islands Council. As such there is no direct current requirement for the IJB to have its own arrangements for business continuity of vital records held by these services. Both NHS Orkney and Orkney Islands Council have adequate business continuity arrangements to ensure the sustainability of health and social care services for which the IJB has overall responsibility.

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.

Control sheets are attached to IJB policies and procedures so it is possible to identify which is the current version, what changes may have been made to the policies and procedures and when.

The IJB's records are created by Orkney Islands Council, often with data supplied by the Council or Health Board and are managed via Orkney Islands Council's IT system. The records are held in folders on the secure SharePoint system, within the Council. This works well for the relatively small number of records that the IJB has created.

12: Competency Framework for Records Management Staff

The staff responsible for managing IJB records, the Chief Officer, the Chief Finance Officer and the Council's Service Manager (Governance), have all completed the appropriate training for Records Management, Data Protection and Information Security.

The IJB is supported by the Information Governance Officer who is fully trained on Records Management and Information Governance.

13: Assessment and Review

The IJB relies on the partner authority to ensure that the systems, policies, and procedures that govern its records are being regularly assessed.

This RMP will be reviewed and updated through the Orkney Health and Social Care Partnership's Senior Management Team.

14: Shared Information

Under certain conditions, information given in confidence may be shared. Most commonly this relates to information which is not confidential and any personal information will have been anonymised or pseudonymised. However, confidential corporate records may be shared with the Council, Health Board, the Scottish Government, and others where there are legal requirements to do so.

No personal data or confidential data is routinely shared by the IJB. The only information that the IJB routinely shares is information that it publishes and is available to the public.

Where personal data is shared on a regular basis by the bodies contracted by the IJB to provide services, the Council, and the Health Board, with the IJB, a Data Processing Agreement will be put in place.

The IJB will not share personal information, other than that relating to the staff employed to support the IJB, the Chief Officer and the Chief Finance Officer. This information will be managed according to the Council and NHS Orkney Data Protection and Information Security policies.

The Publication Scheme identifies information which is available under the Freedom of Information (Scotland) Act 2002 (FOISA).

15: Public Records Created or Held by Third Parties

No third party carries out an IJB function on its behalf.