children's hearings scotland

February 2024

Version 2.0

Records Management Plan

The National Convenor and Children's Hearings Scotland

Contents

Document Control

Title	Records Management Plan
Author	Sophie-Elise Anker & Danielle Metcalfe
Approved by	Senior Information Risk Owner (SIRO)
Date of approval	22/02/2024
Version number	2.0
Review frequency	1 year after implementation, then every two years
Next review date	February 2025

Version	Date	Owner	Summary of Changes
v1.0	24/03/2015	Information Governance Officer	Final Records Management Plan approved by the Board
v1.1	20/11/2023	Information Governance & Data Protection Officer	Revised Records Management Plan drafted in line with current processes
v1.2	21/11/2023		Evidence list added and minor edits to the draft Plan
v1.3	11/12/2023		Draft RMP sent to NRS for feedback prior to formal submission
v1.4	05/01/2024		Minor edits following NRS feedback
v2.0	22/02/2024		Final Records Management Plan approved by SIRO

Approvals	SIRO 02/2024

Introduction

The 2011 Public Records (Scotland) Act requires all named authorities in Scotland to produce a Records Management Plan which details the arrangements in place for managing records.

This is the Records Management Plan of the National Convener and Children's Hearings Scotland (CHS). This covers all records created and processed by the National Convener, CHS National Team, Board, Clerks, and volunteer community, including Area Support Teams and Tribunal Members.

Since the implementation of the 2011 Children's Hearings (Scotland) Act in June 2013, the National Convener and CHS have undertaken the recruitment, training, monitoring and support of volunteer Tribunal Members, who make legal decisions with and for children and young people in children's hearings. As a non-departmental public body, CHS has introduced and developed an organic and bespoke records management framework. This flexible approach has allowed for continuity in records management as the organisation has changed and grown, including a programme of organisational transformation across 2023.

This Records Management Plan, which has been significantly updated since its last submission in 2015, is structured to follow the Keeper's Model Records Management Plan. Key evidence has been appendiced or linked, and key roles and responsibilities identified and named, for the 15 Elements, as required under the Public Records (Scotland) Act.

Element 1: Senior management responsibility

Introduction

An individual at senior level is identified who has overall strategic responsibility for records management on behalf of the National Convenor of CHS.

Statement of Compliance

The senior manager with responsibility for records management on behalf of the National Convenor of CHS is the Director of Business & Finance, Jessica MacDonald. CHS has undergone an organisational change programme in 2023, during which the National Convenor & Chief Executive, Elliot Jackson, has temporarily taken on Senior Information Risk Owner (SIRO) responsibilities, but this responsibility will be transferred to the Director of Business & Finance during 2024.

The Director of Business & Finance oversees Information Governance strategic planning and infrastructure development, and acts as an advocate for Information Governance in their SIRO role as part of the Audit & Risk Management Committee.

Evidence of Compliance

Primary evidence:

- Records Management Competency Framework
- Covering letter/ Supporting Statement

Supporting evidence:

- SLT minutes approval for temporary SIRO position

Future Developments

Once the Director of Business & Finance has fully taken on the SIRO role, no further developments are planned.

Assessment and Review

The Records Management Competency Framework is reviewed every two years. Additional assessment and review of roles is managed through the Audit & Risk Committee.

Responsible Officer

National Convenor & Chief Executive Officer of CHS.

Element 2: Records manager responsibility

Introduction

A CHS staff member holds operational responsibility for records management within the organisation. They are answerable to senior management, and are provided with access to resources and skills.

Statement of Compliance

The officer with operational responsibility for records management at CHS is the Information Governance & Data Protection Officer. The Information Governance & Data Protection Officer is the initial point of contact for the National Records of Scotland (NRS) on records management issues, and is responsible for day-to-day implementation of the National Convenor and CHS's records management plan. The knowledge, skills and experiences required by individuals who take on this role are detailed in the relevant job description and the Records Management Competency Framework.

The Information Governance & Data Protection Officer role requires a Masters degree in Information Management or equivalent experience, and continuing personal development is maintained through access to training in line with the implementation of an agreed annual Personal Development Plan.

Evidence of Compliance

Primary evidence:

- Information Governance & Data Protection Officer Job Description
- Records Management Competency Framework
- Template Personal Development Plan & Objectives
- Covering letter/ Supporting Statement
- CEO Response to Invitation

Supporting evidence:

- CHS Records Management Policy

Future Developments

The Information Governance & Data Protection Officer role is currently vacant, and a recruitment campaign is underway to appoint to this role.

Assessment and Review

The Records Management Competency Framework and Records Management Policy are reviewed every two years. Personal Development Plans and objectives are put in place following annual performance reviews.

Responsible Officer

Director of Business & Finance

Element 3: Records management policy statement

Introduction

The National Convenor and CHS have an appropriate policy statement on records management that provides for the effective management of records at CHS.

Statement of Compliance

The National Convenor and CHS have a Records Management Policy statement, which was last approved in February 2022. The Policy demonstrates the organisation's commitment to best practice in the management of its records by implementing the records management plan. It also outlines CHS's commitment to maintaining authentic, reliable and useable records that are capable of supporting the organisation's functions and activities. The Policy includes provision for the management of records that include personal data in accordance with Data Protection law. It also addresses the roles and responsibilities of the individuals named in Elements 1 and 2, as well as the responsibilities of all staff in relation to records management. The Policy is available for access on the CHS website.

Evidence of Compliance

Primary evidence:

- CHS Records Management Policy

Supporting evidence:

- SIRO approval of policies (includes CHS Records Management Policy)

Future Developments

There are no future developments planned at the current time.

Assessment and Review

The National Convenor and CHS's Records Management Policy is reviewed every 2 years and approved by the SIRO, who is part of the Senior Leadership Team.

Responsible Officer

Information Governance & Data Protection Officer

Element 4: Business classification

Introduction

The National Convenor and CHS's records are fully known and information assets are identified within a classification structure.

Statement of Compliance

The National Convenor and CHS have implemented an Information Asset Register (IAR) recording business classification. It is structured according to directorate and then by function. This was completed with Information Asset Owners (IAOs), ensuring it is a comprehensive and accurate record of all CHS's information assets and risks at the time of completion.

The IAR includes all records and information produced and managed by CHS and for which CHS is data controller, including functions contracted to third parties. It covers all record systems used by CHS as an organisation holding only born-digital records, and covers information assets created and managed centrally as well as locally within Area Support Teams. The National Convenor and CHS's business records are held primarily in shared drives, in the Scottish Government system, and CHS's digital system, CSAS. Any records held in additional line of business systems are covered in the IAR and assessed for information security risks.

The IAR also identifies information assets that contain personal data and special category data and records the General Data Protection Regulation (GDPR) Article 6 legal basis for processing in each case. It also records the GDPR Article 9 and Data Protection Act 2018 Schedule 1 conditions for processing special category data, where such data is processed.

Value and sensitivity ratings have been applied to each information asset, and any risks and current security measures identified. Appropriate risk mitigations and actions are also identified in the IAR, with deadlines assigned according to risk level and business need. Risk mitigation actions are identified and followed up on as part of bi-annual IAR updates. The SIRO is periodically informed of key risks and actions taken to mitigate them.

The most recent version of the IAR was approved by the Senior Leadership Team in April 2023, and brought to the Audit and Risk Management Committee in May 2023. The IAR provides key details of all CHS's information assets in one document, structured according to Directorate, and then function.

Evidence of Compliance

Primary evidence:

- CHS Information Asset Register template

Supporting evidence:

- Minutes from SLT approving the IAR

- Minutes from ARMC noting the IAR
- Information Asset Register Guidance
- Information Asset Register How-To session presentation
- Email to SIRO outlining risks to information assets
- Example email to IAOs outlining controls to be implemented

Future Developments

Due to the present ongoing organisational changes at CHS, there are plans in place for the IAR to undergo a full review by June 2024 to align with the new organisational structure.

Assessment and Review

The National Convenor and CHS conduct a full review of the IAR every 12 months, and conduct a partial review where key updates are added 6 months after the full review has taken place. The initial IAR was approved by the Senior Leadership Team and brought to the Audit and Risk Management Committee. Subsequent reviews will be approved by the SIRO, with any major changes to process approved by the Senior Leadership Team.

Responsible Officer

Information Governance & Data Protection Officer

Element 5: Retention schedules

Introduction

The National Convenor and CHS have a full Retention and Disposal Schedule in place that assigns retention policies and disposal procedures to all business records.

Statement of Compliance

A Retention and Disposal Schedule covering all of the National Convenor and CHS's business records is well established within the organisation, and was last reviewed and approved in August 2023. The Schedule is arranged according to function, activity, and transaction, from which each of CHS's record types have been identified.

Business areas that have seen key changes since the last review are consulted on Retention Schedule entries for their areas during reviews of the Schedule. Sector best practice is also considered from the Scottish Council on Archives. Required changes to the Schedule are also identified during Data Protection Impact Assessments (DPIAs) to ensure compliance with the storage limitation principle.

Appropriate retention policies have been assigned to each record type, accounting for any legislative requirements, best practice, business need and historical value, ensuring records are retained as long as is necessary. The Schedule also identifies a disposal procedure for each record type to ensure records are disposed of appropriately at the end of the retention period.

The Schedule distinguishes records holding vital status for business continuity purposes. IAOs are listed next to each record type, ensuring that Owners are aware of their responsibilities regarding retention and disposal of CHS's records. Scottish Government security classifications have been applied to each record type and listed next to each Schedule entry to align with CHS's Security Classifications Policy.

CHS has sought advice from the NRS on any records identified to be retained permanently for historical value following appraisal, as to which records the NRS would select for archival transfer.

Evidence of Compliance

Primary evidence:

- CHS Retention and Disposal Schedule
- CHS Security Classification Policy

Supporting evidence:

- Retention Schedule approval

- NRS email confirmation of types of records for transfer
- Example DPIA recommending retention policies

Future Developments

The National Convenor and CHS have a comprehensive Retention and Disposal Schedule in place. An updated extract containing relevant Schedule entries is planned to be rolled out to local authority Clerks in early 2024.

Assessment and Review

The National Convenor and CHS's Retention and Disposal Schedule is reviewed in full every two years, with individual retention policies updated as and when required. The Schedule is approved by the Information Governance & Data Protection Officer and the Senior Leadership Team are made aware of any reviews of the Schedule.

Responsible Officer

Information Governance & Data Protection Officer

Element 6: Destruction arrangements

Introduction

The National Convenor and CHS's records are securely destroyed according to the Retention & Disposal Schedule and a log is maintained of their destruction.

Statement of Compliance

Disposal procedures are identified for each of the National Convenor and CHS's record types in the Retention and Disposal Schedule. Secure destruction of records stored on shared drives is completed manually, in line with the retention schedule. A Disposals Log was rolled out to IAOs in September 2023, in which the justification for records disposal, including details of the applicable retention policy, is recorded along with the date of disposal.

In CHS's digital system, CSAS, destruction is systematic, except in the contact database where data is manually deleted in line with retention policies. Retention policies are applied in accordance with CHS's Retention and Disposal Schedule. In the case of erasure requests submitted under Data Protection law, personal data can be securely and fully erased within statutory deadlines.

The National Convenor and CHS's business records are held digitally, however staff may print a small amount of paper records for short-term and specific purposes. These papers are destroyed at CHS's office, Thistle House, once no longer required, using confidential waste bins and ISO accredited supplier contracted through the Scottish Legal Aid Board, from whom CHS rents the office. Disposal guidance is available to staff and updated in line with system changes.

CHS maintains an Asset Tracker of hardware, which records the lifecycle of all assets, including disposal. Disposal of SCOTS equipment is managed in line with the iTECS Terms of Supply.

Evidence of Compliance

Primary evidence:

- Disposals Log template
- CHS Retention & Disposal Schedule
- Keeping Information Safe Guidance pack
- Memorandum of Understanding between CHS and SLAB
- iTECS Terms of Supply
- Asset Tracker template

Supporting evidence:

- Example erasure request completion

Future Developments

The National Convenor and CHS plan to create and implement a formal procedure for the disposal of hardware. CHS has plans to work jointly with the Scottish Children's Reporter Administration (SCRA) to determine architectural changes within CSAS contact database to embed automated retention.

Assessment and Review

The Retention & Disposal Schedule and Keeping Information Safe Guidance are reviewed every two years.

Responsible Officer

Information Governance & Data Protection Officer
Digital Strategy & Delivery Manager

Element 7: Archiving and transfer arrangements

Introduction

The National Convenor and CHS employ mechanisms of retention management and transfer to ensure that records that have enduring value are permanently retained and made accessible.

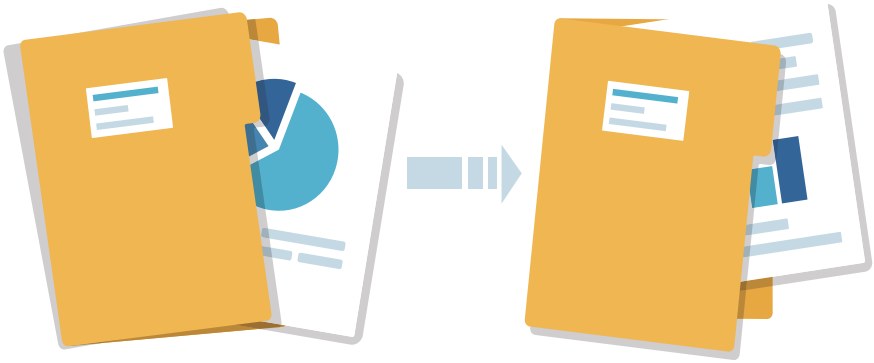
Statement of Compliance

The National Convenor and CHS first established a Memorandum of Understanding with NRS in 2015, to govern the transfer of records of historical significance for permanent preservation and access. A Deposit Agreement was further signed with NRS on 31st August 2023, to facilitate record transfers, and record types which would be considered for transfer have been agreed. Internal assessment of records with significant historical value is carried out in line with the CHS Retention and Disposal Schedule.

Evidence of Compliance

Primary evidence:

- CHS & NRS Memorandum of Understanding
- CHS & NRS Deposit Agreement
- CHS Retention & Disposal Schedule



Supporting evidence:

- Approval of CHS Retention & Disposal Schedule
- Communication with NRS regarding types of records for transfer

Future Developments

As a young organisation, CHS records have only recently begun to trigger an assessment for long term preservation and storage. CHS is progressing transfer arrangements with NRS and will continue to assess future needs.

Assessment and Review

The CHS Retention & Disposal Schedule will next be reviewed and updated in 2025. SIRO will be updated on transfer arrangements as required.

Responsible Officer

Information Governance & Data Protection Officer

Element 8: Information security

Introduction

Measures are in place to protect the National Convenor's and CHS's information and records. Information is safeguarded by policy and security mechanisms from unauthorised use, modification, disclosure or destruction. Records are held in accordance with information security compliance requirements.

Statement of Compliance

The National Convenor and CHS utilise a comprehensive Information Security Incident management structure to ensure any incidents are mitigated, risks and vulnerabilities can be identified, and emerging issues can be prevented. This is managed through the CHS Information Security policy, the Acceptable Use policy, the Information Security Incident Matrix, and the Managing Information Security Incidents procedure.

All incidents are logged in the Information Security Incidents Log, and reported quarterly to senior leadership and the Audit & Risk Management Committee. Any trends identified are also reported on, and an end of business year summary of incidents and trends, including any reports to the Information Commissioner's Office (ICO), is provided.

All business records are securely stored either on the SCOTS network, with security provided through the Scottish Government, or through CHS's digital system CSAS, which is securely hosted by CHS's sister organisation SCRA. IAOs are responsible for ensuring relevant security measures are in place for identified information assets, including folder permissions and password protection. All controls are recorded on the Information Asset Register. All employees undertake mandatory training which covers information security.

Evidence of Compliance

Primary evidence:

- Information Asset Register (redacted)
- Information Security policy
- Acceptable Use policy
- CHS Managing Information Security Incidents procedure

Supporting evidence:

- SLT minutes- IG report approval
- ARMC minutes- IG report approval
- SIRO approval of policies (includes Information Security Policy)

Future Developments

There are no future developments planned at the current time.

Assessment and Review

Guidance and policies are regularly reviewed, with trends and risks escalated to appropriate levels, including Audit & Risk Management Committee. The National Convenor and CHS will continue to manage and monitor information risks and incidents.

Responsible Officer

Information Governance & Data Protection Officer
Senior Information Risk Owner

Element 9: Data protection

Introduction

Records involving personal data are managed in compliance with data protection law, with procedures in place to manage and protect the personal information held by the National Convenor and CHS.

Statement of Compliance

CHS demonstrates and monitors compliance with Data Protection legislation (including the UK GDPR and the Data Protection Act 2018) through key Information Governance policies and procedures.

CHS is a registered Data Controller with the ICO, and has a designated Data Protection Officer who is able to advise leadership on data protection matters.

The principles of data protection are considered and complied with throughout all processing activities, and privacy statements relating to the groups of data subjects for whom CHS processes their personal information are available on the CHS website. These are reviewed and updated in line with process changes, and demonstrate compliance with the data protection principle of lawfulness, fairness, and transparency. A statement outlining the data protection rights of individuals is linked to and displayed alongside all privacy statements.

All key policies which are central to demonstration of compliance with data protection legislation are managed under the Information Governance Policy framework. These include the Data Protection Policy, the Information Security Policy, the Acceptable Use Policy, and the Records Management Policy. These policies each regulate an area of compliance which is in line with the data protection principles.

All breaches of data protection legislation are handled under the Managing Information Security Incidents procedure, in addition to the Information Security Policy. This procedure offers practical steps to the prevention and mitigation of information security incidents and data breaches. All breaches and near misses are recorded as part

of this procedure in the Information Security Incidents Log.

DPIAs are utilised across CHS to ensure data protection by design and default. They consist of a screening form, and a full DPIA. Consideration of the need for a DPIA is embedded into submission of papers and projects to senior leadership, through an Impact Assessment Form 1.

Compliance with the principles of data minimisation and storage limitation are demonstrated through the application of the CHS Retention and Disposal Schedule.

Evidence of Compliance

Primary evidence:

- Privacy Statements webpage
- Data Protection Policy
- Information Security Policy
- Acceptable Use Policy
- Records Management Policy
- Information Governance Policy Framework
- Managing Information Security Incidents Procedure
- Information Security Incidents Log template
- Impact Assessment Form 1 template
- Template full DPIA
- DPIA Guidance
- CHS Retention & Disposal Schedule

Supporting evidence:

- DPO registration with ICO

Future Developments

There are no future developments planned at the current time.

Assessment and Review

All policies are regularly reviewed and updated. Privacy statements are updated when there are changes to processing activities, and are often required for DPIA completion and sign off. The Information Security Incidents log is reviewed quarterly.

Responsible Officer

Information Governance & Data Protection Officer

Element 10: Business continuity and vital records

Introduction

The National Convenor and CHS have arrangements in place to prepare for, respond to and recover records, in particular vital records, in the event of a Business Continuity incident.

Statement of Compliance

Arrangements for the restoration of systems and records is of high priority in CHS's Business Continuity planning, as is detailed in the Business Impact Analysis. iTECS have business continuity arrangements in place for the SCOTS system, on which CHS's shared drives and most business records are located. iTECS performs daily incremental back-ups, and full back-ups of the system at the weekend. Regular back-ups of the data and duplicate back-ups are retained at two separate Data Centres. The back-ups are retained for four weeks, at which point they are destroyed and the information then becomes irretrievable.

Vital records are identified in CHS's Retention & Disposal Schedule and the IAR. CHS's IAR identifies vital records requiring back-ups to be retained. The Register also identifies records containing personal data, and arrangements have been put in place to protect such records, as has been addressed in Elements 4 and 9.

Evidence of Compliance

Primary evidence:

- Vital Records Strategy
- CHS Retention & Disposal Schedule
- Business Continuity Plan extract
- Business Continuity plan policy
- CHS Information Asset Register
- iTECS Terms of Supply

Supporting evidence:

- Approval of Vital Records Strategy
- ARMC minutes- Business Continuity Plan

Future Developments

The criteria for identifying vital records is planned to be reviewed, to be defined in line with the Business Continuity Plan, and the vital records are planned to be reviewed to align with the Business Impact Analysis. CHS also plans to ensure vital records have back-ups retained in a separate location to the original record.

Assessment and Review

The Vital Records Strategy is reviewed annually and approved by the Senior Leadership Team. The Business Continuity Plan is subject to quarterly review and is submitted every 2 years, with the Business Continuity Policy, to the Audit and Risk Management Committee, for consideration, assurance, and approval of any substantial changes in approach.

Responsible Officer

Information Governance & Data Protection Officer
Business Operations & Governance Manager

Element 11: Audit trail

Introduction

The National Convenor and CHS know the location of their records, and track, within the capabilities of current systems, any changes made.

Statement of Compliance

The National Convenor and CHS hold their business records digitally, and records can be located via folder structures and search functions. On shared drives, records are structured, organised and named in line with the approach outlined in the Shared Drives Guidance which is provided to all staff and includes naming conventions. Information Governance Officers oversee the implementation of folder structures and naming conventions. CHS's digital system, CSAS, consists of databases containing data for different services. Each database has filter and sorting options that enables the database to be easily searched and records located.

Version control and document control is in place for CHS business records that are subject to regular reviews or updates. Version control is applied to business records stored on the shared drives by stating the version in the file title and adding version control within the document, following the guidelines set out in the Shared Drives Guidance. Document control is applied to policy documents and outlines changes made to the record during each update.

On shared drives, previous versions of documents can be located and the date and time the document was last modified can be seen, as well as the user who last saved the document, the author's username, and the date the content was created. Audit logs are maintained of each CSAS database, accessible through Power BI. The logs track changes such as when a record is edited, what action was taken, when the change was made, what record it concerns, and why. The specifics of these logs are tailored to the requirements of each database.

Evidence of Compliance

Primary evidence:

- Shared Drives Guidance
- Keeping Information Safe Guidance pack
- CHS Retention & Disposal Schedule

- CSAS Audit Log extract
- Information Governance induction

Supporting evidence:

- Screenshot of example of shared drive file Properties

Future Developments

There are regular improvements to CSAS on an ongoing basis.

Assessment and Review

Policies and guidance are regularly reviewed.

Responsible Officer

Information Governance & Data Protection Officer
Digital Strategy & Delivery Manager

Element 12: Records management training for staff

Introduction

Staff creating, or otherwise processing records, are appropriately trained and supported. Staff with responsibility or oversight of elements of records management can evidence additional training and support. Training is regularly refreshed and monitored.

Statement of Compliance

The core competencies and key knowledge for all roles with records management responsibilities are set out in the CHS Records Management Competency Framework. This framework indicates the relevant expectations for each role, including staff with IAO responsibility, staff who are designated records officers, and the Data Protection Officer and SIRO. All staff receive an Information Governance Induction which includes information on the Records Lifecycle, guidance on storage, and directions on where to seek advice. They are also directed to guidance on utilising the CHS Retention & Disposal Schedule. Supplementary guidance on managing information is available from the Keeping Information Safe guidance pack.

Staff members with IAO responsibilities have received in-depth training on the application of this responsibility, and also receive one to one support and guidance from a designated records officer. They are able to function as localised decision makers, with the support of the Information Governance team.

The Information Governance team provide support and deliver training on all aspects of records management. All roles within the Information Governance team require a master's degree in information management, or relevant experience to an equal degree, and opportunities for continuing professional development, such as supplementary training courses, are regularly offered.

All staff complete online training once every two years. This training is designed by the Information Governance team and includes a policy refresh as well as an assessed module. Completion records are maintained and updated in line with the launch and closure of each cohort.

Evidence of Compliance

Primary evidence:

- CHS Records Management Competency Framework
- CHS Keeping Information Safe Module
- CHS Keeping Information Safe Guidance Pack
- CHS Managing Retention Needs
- Information Asset Register 'How To' Training
- Information Governance Induction
- IG training completion records (staff)
- Shared Drives guidance

Supporting evidence:

- Approval of CHS Records Management Competency Framework

Future Developments

Module development and completion will continue to be managed under a model of continuous improvement.

Assessment and Review

Completion of mandatory training is monitored and audited for all roles, with induction training completed through the HR onboarding programme. The CHS Records Management Competency Framework is regularly reviewed and updated.

Responsible Officer

Information Governance & Data Protection Officer

Element 13: Assessment and review

Introduction

The National Convenor and CHS's records management arrangements are systematically and regularly reviewed and assessed for future developments.

Statement of Compliance

Regular review of the organisation's Information Governance policies, procedures and guidance is in place and upcoming reviews and completions are tracked in CHS's policy tracker. Relevant policies, procedures and guidance have been appropriately assigned to regular review of either every 12 months or every 2 years. CHS's policies and procedures were reviewed in advance of GDPR implementation to ensure compliance.

The Information Governance & Data Protection Officer is responsible for instigating reviews. Policies and procedures updated and reviewed in line with the review schedule are submitted as appropriate to the Senior Leadership Team and/or Audit & Risk Management Committee. Guidance is submitted for approval offline to SIRO or the Information Governance & Data Protection Officer as appropriate.

Any identified records management related risks are added to the Operational Risk Register, along with mitigations, for monitoring, and are reviewed every month.

CHS conducts a continual programme of internal audit in which information governance functions are assessed. Audit actions are monitored and implemented within an agreed timeframe. A data protection audit and a Freedom of Information (FOI) audit were conducted in 2022.

Evidence of Compliance

Primary evidence:

- Risk register template
- Policy tracker extract
- GDPR preparations for implementation
- Data Protection Audit Report
- FOI Audit Report

Supporting evidence:

- ARMC minutes of Data Protection audit approval
- FOI audit approval
- SIRO approval of Policies

Future Developments

Following the Keeper's assessment of the National Convenor

and CHS's Records Management Plan, future developments and any issues identified will be incorporated into the Information Governance work plan for 2024/25.

The National Convenor and CHS will review their Records Management Plan one year after implementation, and then every two years in response to the National Records of Scotland's invitation to conduct a Progress Update Review. Reviews will be instigated by the Information Governance & Data Protection Officer, and will ensure the Plan remains fit for purpose.

Assessment and Review

All policies and procedures are subject to ongoing monitoring and regular review.

Responsible Officer

Information Governance & Data Protection Officer

Element 14: Shared information

Introduction

Safeguards are in place to ensure information is shared lawfully, when necessary, and through a controlled approach.

Statement of Compliance

The National Convenor and CHS have ongoing needs that require the sharing of information with key partners. These partners include the Scottish Children's Reporter Administration, local authorities, and the Scottish Government, amongst others. Information shared is governed by a Data Processing Contract or Information Sharing Protocol, as appropriate. Data Processing Contracts outline the information being shared, and are tailored to the purpose of each sharing relationship. They also record the specific data being shared, and the policies under which the information will be managed.

Information sharing needs are identified and assessed through the DPIA process. This gives an opportunity to mitigate any emerging risks and ensure information is shared in line with data protection principles.

Evidence of Compliance

Primary evidence:

- Data Processing contract template
- Example Information Sharing Protocol

Future Developments

Additional ways of reporting on and monitoring sharing agreements are being explored.

Assessment and Review

The National Convenor or SIRO reviews and signs off any Information Sharing Protocols and other significant sharing agreements.

Responsible Officer

Information Governance & Data Protection Officer

Element 15: Public records created by third parties

Introduction

Arrangements are in place to safeguard the management of records created and held by third parties who carry out any functions of the National Convenor & CHS.

Statement of Compliance

All records created and held by third parties in order to carry out functions of CHS are governed by a signed Data Processing Contract (DPC). The DPC provided by CHS includes clauses on retention and disposal, termination of contract, data controller and processor rights and obligations, and any bespoke clauses necessary to the functions being carried out. Types of data, data subject groups, and purpose of sharing are also agreed within the Schedules of the DPC.

CHS works with local authorities who employ Clerks to create, maintain, store, and manage local CHS records. Each local authority which employs a Clerk does so under a DPC. Clerks who hold records management responsibilities in local areas, execute this function in line with DPC requirements.

CHS regularly contracts other third parties to carry out short term functions, and the records management safeguards for each relationship are managed through the Data Processing Contract log.

Evidence of Compliance

Primary evidence:

- Example Data Processing Contract
- Data Processing Contract log

Future Developments

No future developments are currently planned.

Assessment and Review

The Data Processing Contract log covers all active contracts, and is regularly reviewed.

Responsible Officer

Information Governance & Data Protection Officer

Evidence List

Item no.	Document Name	In support of Element(s)
001	Records Management Competency Framework (PE)	1, 2, 12
002	SLT minutes- approval for temporary SIRO position (SE)	1
003	IG&DPO Job Description (PE)	2
004	Template Personal Development Plan & Objectives (PE)	2
005	Covering letter/Supporting Statement (PE)	2, 1
006	CEO Response to Invitation (PE)	2
007	CHS Records Management Policy (PE/SE)	2, 3, 9
008	SIRO approval of Policies: Records Management, Data Protection, Information Security, and IG Policy Framework (SE)	3, 8, 13
009	CHS Information Asset Register template (PE)	4, 8, 10
010	SLT minutes- approving IAR (SE)	4
011	ARMC minutes- noting IAR (SE)	4
012	Information Asset Register Guidance (SE)	4
013	Information Asset Register How-To session presentation (SE)	4, 12
014	Example email to SIRO outlining risks to information assets (SE)	4
015	Example email to IAOs outlining controls to be implemented (SE)	4
016	CHS Retention & Disposal Schedule (PE)	5, 6, 7, 9, 10, 11
017	CHS Security Classifications Policy (PE)	5
018	Retention schedule approval (SE)	5, 7
019	NRS email confirmation of types of records for transfer (SE)	5, 7
020	Example DPIA recommending retention policies (SE)	5

021	Disposals Log template (PE)	6
022	CHS Keeping Information Safe Guidance Pack (PE)	6, 11, 12
023	Memorandum of Understanding between CHS and SLAB (PE)	6
024	iTECS Terms of Supply (PE)	6
025	Asset Tracker template (PE)	6
026	Example erasure request completion (SE)	6
027	Memorandum of Understanding between CHS & NRS (PE)	7
028	CHS & NRS Deposit Agreement (PE)	7
029	CHS Information Security Policy (PE)	8, 9
030	CHS Acceptable Use Policy (PE)	8, 9
031	CHS Managing Information Security Incidents procedure (PE)	8, 9
032	SLT minutes- IG report approval (SE)	8
033	ARMC minutes- IG report approval (SE)	8
034	Privacy Statements (PE)	9
035	CHS Data Protection Policy (PE)	9
036	CHS Information Governance Policy Framework (PE)	9
037	Information Security Incidents Log template (PE)	9
038	Full DPIA templates (PE)	9
039	Impact Assessment Form 1 (PE)	9
040	DPIA Guidance (PE)	9
041	DPO registration with ICO (SE)	9
042	CHS Vital Records Strategy (PE)	10
043	CHS Business Continuity Plan extract (PE)	10
044	Business Continuity plan policy (PE)	10

045	Approval- Vital Records Strategy (SE)	10
046	ARMC minutes- Business Continuity Plan (SE)	10
047	Shared Drives Guidance (PE)	11, 12
048	CSAS Audit Log extract (PE)	11
049	Shared drive folder Properties screenshot (SE)	11
050	CHS Keeping Information Safe Module (PE)	12
051	CHS Managing Retention Needs (PE)	12
052	Information Governance Induction (PE)	11, 12
053	IG training completion records for staff (PE)	12
054	Approval- CHS Records Management Competency Framework (SE)	12
055	Risk register template (PE)	13
056	Policy Tracker extract (PE)	13
057	ARMC minutes- Data Protection audit approval (SE)	13
058	GDPR preparations for implementation (PE)	13
059	Freedom of Information Audit report (PE)	13
060	Data Protection Audit report (PE)	13
061	FOI audit approval (SE)	13
062	Data Processing Contract template (PE)	14
063	Example Information Sharing Protocol (PE)	14
064	Example Data Processing Contract (PE)	15
065	Data Processing Contract log (PE)	15

3rd Floor Thistle House | 91 Haymarket Terrace | Edinburgh | EH12 5HE t: 0131 460 9569 | www.chscotland.gov.uk