Information Security

Policy

Date Approved: 31/10/2025
Approved by: SIRO
Version: 6.0

Next Review Date: 31/10/2026
Owner: Data Protection and Information Governance Officer

Document Version Control

Version Number	Change/Update	Author/Owner	Date
V1.0	N/A	Information Governance Lead	15/05/2013
V1.1	Addition of policies and procedures at section 4; amendment of the Government Classification Policy information at 6.1; amendment of 7.3.	Information Governance Lead	10/12/2013
V1.2	Addition of policies and procedures at section 4; amendment of review frequency at 2.2; addition of legislation at 3.2; rewording at 5.4, 6.3 and 7.1; addition of doc and status control tables.	Information Governance Lead	20/02/2014
V1.3	Review period extended from 6 months to 2 years.	Information Governance Lead	03/06/2014
V1.4	Amendment of responsibilities at 5.3 and policies at section 4.	Information Governance Lead	29/07/2014
V1.5	Reviewed by Audit and Risk Management Committee (ARMC) – additional sections at 1.3 and 1.4. Clarification of roles and responsibilities at section 5.	Information Governance Lead	19/08/2014
V2.0	Final policy approved by the CHS Board.	Information Governance Lead	26/08/2014
V2.1	Minor amendments to reflect changes in job titles and additions to the legislative framework.	Information Governance Lead	25/03/2015
V3.0	Final policy approved by SLT.	Information Governance Lead	31/03/2015
V3.1	Minor amendments made to terminology with a comprehensive review to take place prior to implementation of GDPR in May 2018.	Information Governance Lead	
V3.2	Review to be compliant with GDPR.	Information Governance Lead	
V4.0	Final policy approved by SIRO.	Information Governance Lead	30/03/2018
V4.1	Updates to GDPR/DPA-related policy, clarification of roles, amendments to Standards references, updates to reflect online & computer-based storage, updates to legislation and to related policies, procedures & guidance.	Information Governance & DPO	18/02/2022
V5.0	Final policy approved by SIRO.	Information Governance & DPO	28/02/2022
V5.1	Amended to updated policy template. Minor amendments, such as job titles.	Information Governance Officer	29/10/2025

V5.2	Updates to align with ISO 27001 ISMS requirements such as objectives, updates to legislation, and addition of definitions.	Information Governance & DPO	30/10/2025
V6.0	Final policy approved by SIRO	Information Governance & DPO	31/10/2025

Information Security Policy

Contents

1. Definitions

1.1 The definitions below are to help with the understanding of this policy and other similar documents.

Information Asset	Definable pieces of information, stored in any manner which is recognised as valuable to the organisation.
Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person (Article 4(1) of the GDPR).
Data Protection legislation	This includes the UK General Data Protection Regulation (GDPR), Data Protection Act 2018, Data (Use and Access) Act 2025, the Privacy and Electronic Communications Regulations, and any future laws concerning data protection and privacy.
Publication Scheme	The purpose of the Publication Scheme is to allow the public to see what information is available (and what is not available) to access in relation to each class, state what charges may be applied, explain how to find the information easily, provide contact details for enquiries and to get help with accessing the information, and explain how to request information we hold that has not been published.

2. Overview/Introduction

2.1 Information is one of Children's Hearings Scotland's (CHS) most valuable assets and must be adequately protected against loss or compromise. We will consider all processes involved that require us to collect, store, use and dispose of personal data. We will consider how valuable, sensitive, or confidential the information is and what damage or distress could be caused to individuals if there was a security breach.

2.2 CHS will take steps to ensure that information is safeguarded from unauthorised use, modification, disclosure, or destruction, whether accidental or intentional. CHS will also ensure that information is made available to those authorised to access it and that we meet our regulatory and legislative requirements. To meet the minimum mandatory measures to minimise information risk CHS will appoint an Accountable Officer (AO), Senior Information Risk Owner (SIRO), Information Asset Owner (IAO), and a Data Protection Officer (DPO). The requirement to keep information secure will be balanced with the need for CHS staff, volunteers, Clerks, and the Children's Panel to operate effectively. CHS will ensure data is accurate, up to date and not kept for longer than is necessary or useful.

2.3 CHS are committed to openness, transparency, and accountability within the framework of the data protection legislation, the Freedom of Information (Scotland) Act 2002 (FOISA), the Environmental Information (Scotland) Regulations 2004 (EIRs) and the Public Records (Scotland) Act 2011 (PRSA).

2.4 Our Publication Scheme identifies the classes of information we routinely make available through our website. We are committed to regularly reviewing the Scheme to identify additional classes of data that can be published to build greater public trust in the way we operate whilst at the same time safeguarding personal data from misuse and protecting individuals' rights to privacy.

2.5 We will adopt a risk-based approach to withholding data. Our objective is to strike the right balance in achieving transparency and maintaining confidentiality whether the privacy of individuals or commercial interests, or where protection is in the public interest. Where necessary we will protect the privacy of individuals by anonymising data.

2.6 The implementation of this policy is important to maintain and demonstrate CHS's integrity in our dealings with all our stakeholders.

3. Purpose

3.1 The purpose of this policy is to set out CHS's approach to protecting our corporate information from information security threats, whether internal or external, deliberate, or accidental.

3.2 The aim is to ensure that information is adequately protected against loss or compromise.

4. Scope

4.1 This policy applies to all CHS staff and Board Members, volunteers, Clerks (including their teams), Experts by Experience, and third-party suppliers/contractors with access to CHS information and/or systems.

4.2 The scope of this policy includes all information owned by or entrusted to CHS to support processes in relation to the operation of the national Children's Panel. This is inclusive of, but not limited to:

- information that is the intellectual property of CHS,
- personal information relating to employees of and volunteers of CHS and other personal information held by CHS as set out in our Privacy Statements, and
- information relating to IT systems, manual systems, utilities, and data used in the functioning of the organisation.

5. Legislative Framework

5.1 CHS must operate within a legal framework in terms of how it collects, holds, uses, shares and destroys information.

5.2 The following legislation provides a framework in which CHS will operate:

- Age of Criminal Responsibility (Scotland) Act 2019
- Children's Hearings (Scotland) Act 2011
- The Children's Hearings (Scotland) Act 2011 (Rules of Procedure in Children's Hearings) Rules 2013
- Children and Young People (Scotland) Act 2014
- Children (Scotland) Act 2020
- Communications Act 2003
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988

- Disclosure (Scotland) Act 2019
- Employment Rights Act 1996
- Environmental Information (Scotland) Regulation 2004
- Equality Act 2010
- Freedom of Information (Scotland) Act 2002
- General Data Protection Regulation 2018 & Data Protection Act 2018
- Human Rights Act 1998
- Local Government Scotland Act 1994
- Prescription and Limitation Acts 1973 and 1984
- Privacy and Electronic Communications Regulation 2003
- Public Records (Scotland) Act 2011
- Regulation of Investigatory Powers Act 2000
- Data (Use and Access) Act 2025
- Children (Care and Justice) (Scotland) Act 2024
- UNCRC (Incorporation) (Scotland) Act 2024

5.3 CHS also aims to operate in accordance with the following best practice standards:

- BS ISO 15489: 2016 - Information and Documentation – Records Management
- BS ISO 27001: 2022 - Information Security Management System
- Government Security Classifications Policy

6. **Relationship to other CHS policies, procedures, and guidance**

This policy is supported by the following CHS policies, procedures, and guidance:

- Information Security Management System (ISMS) Policies
- Security Classifications Policy and Classifying sensitive documents and emails – summary guidance.
- Acceptable Use Policy
- Business Continuity Plan and Vital Records Strategy
- Data Protection Policy
- Handling Information Requests – summary guidance
- Information Governance Policy Framework
- Keeping Information Safe Guidance Pack
- Managing Information Security Incidents Procedure and Reporting Information Security Incidents– summary guidance
- Records Management Policy
- Retention and Disposal Schedule and Retention and Disposal – Guidance for Clerks

7. Roles and responsibilities

7.1 Chief Executive and SIRO

The Chief Executive (CEO) of CHS, as Accountable Officer, has overall responsibility for information security. The CEO is responsible for ensuring that all individuals within the scope of this policy receive the appropriate level of training, supervision and direction to support the implementation of this policy.

7.2 The Director of Business and Finance is designated as the SIRO for CHS and is the senior member of staff responsible for information risk in the organisation. The SIRO is responsible for ensuring compliance with this policy and for assigning Information Asset Owners (IAOs) to information assets held by CHS. Details of these IAOs can be found in CHS's Retention and Disposal Schedule.

7.3 Information Governance and Data Protection Officer

The implementation of, and compliance with, this policy is delegated to the Information Governance and Data Protection Officer (IG&DPO). They will be supported by the Information Governance Team and Digital Team.

The IG&DPO will be responsible for the following:

- Supporting all roles within the scope of this policy to comply with their obligations under this policy by issuing guidance and training.
- Monitoring and reporting compliance with this policy and information security incidents.

7.4 All roles within the scope of this policy

All roles within the scope of this policy as set out in section 4 are responsible for the following:

- That they have read, understood, and comply with this policy and all related policies, procedures, guidance and processes[1].
- They are expected to take all reasonable steps to protect CHS information from unauthorised use, modification, disclosure, or destruction.

[1] For details of which policies, procedures, and guidance, CHS consider to be essential reading for your role, please refer to the *Information Governance Policy Framework.*

8. Policy statement

8.1 CHS has identified information security objectives, which are set out in the ISMS Strategic Control Objectives document (under Measures/Metrics section). Objectives are allocated to relevant business owners to consider resource and support. The Information Security Forum is responsible for overall delivery of the Organisation's objectives, and this is monitored on a continual basis. Specific objectives are managed by individuals responsible for the completion of objectives.

8.2 All information owned by, or entrusted to, the organisation will be protected in a manner that is consistent with the value attributed to it, the risk we are willing to accept and the cost we are willing to pay.

8.3 This policy applies to (but is not limited to) information stored in the following formats:

- computers and networks
- magnetic or optical storage media (e.g. hard drive, tape, CD, USB)
- in physical storage environments (e.g. offices, filing cabinets, drawers)
- CCTV or other video format
- online (e.g. Microsoft Teams, SharePoint)
- audio recordings
- printed media (e.g. forms, reports, documents, records, books)

9. Managing our information assets

9.1 CHS takes a risk-based approach when assessing and understanding the risks posed to information and we will use physical, personnel, technical and procedural means to achieve appropriate security measures ensuring processes are regularly audited.

9.2 Confidentiality and security rules continue to apply to all business conducted on behalf of CHS when an individual within the scope of this policy is working at home. Official information must not be disclosed to those unauthorised to receive it, this includes information recorded in any format e.g. physical documents and information stored on IT and online systems. Individuals within the scope of this policy are responsible for ensuring the security of the papers, equipment, and digital information, and that basic levels of security are in place, such as locked windows and doors, and screen lock etc.. Particular care must be taken when confidential papers are being transported to and from home.

9.3 CHS has identified its information assets and the owners of these assets. This information is contained in the Information Asset Register. From identification of the assets, we ascertain any risks to those assets, the potential impact of these risks and mitigating controls to safeguard the information.

9.4 Please refer to the Information Asset Register for more information about how CHS will assess the risks associated with these assets and circulate to staff to ensure they are aware of the risks and the controls in place to limit exposure to risk.

10. Implementation, Communication and Compliance

10.1 To implement this policy, CHS will ensure that all roles within the scope of this policy are aware, and that the most up-to-date version is available and accessible.

10.2 All staff, Board members, Experts by Experience and volunteers, must complete Information Governance training as part of their mandatory induction training and refresher training. The information security policy forms part of this training.

10.3 In the event of a serious information security incident or breach of this policy by a member of staff, which has the potential to cause damage or distress to individuals, CHS or the Children's Hearings System, may find it necessary to suspend the staff member from their duties whilst an investigation is carried out. Depending upon the outcome of the investigation, it may lead to disciplinary action and/or dismissal, in accordance with the Staff Code of Conduct.

10.4 In the event of a serious information security incident or breach of this policy by a member of the CHS Board, which has the potential to cause damage or distress to individuals, CHS or the Children's Hearings System, may find it necessary to liaise with Scottish Government for them to take action whilst an investigation is carried out by The Standards Commission for Scotland in line with the Board member's Code of Conduct.

10.5 In the event of a serious information security incident or breach of this policy by a panel member, PPA, or Expert by Experience, which has the potential to cause damage or distress to individuals, CHS or the Children's Hearings System, may find it necessary to suspend the panel member or PPA from their duties, or require the Expert by Experience to step back from their activities whilst an investigation is carried out. Depending upon the outcome of the investigation, it may lead to removal from their role at CHS.

10.6 In the event of a serious information security incident or breach of this policy by a Clerk or their team member, with access to CHS information, which has the potential to cause damage or distress to individuals, CHS or the Children's Hearings System, this will be handled in line with the terms of the contract to ensure contractual obligations are met.

10.7 In the event of a serious information security incident or breach of this policy by a third-party contractor/supplier with access to CHS information, which has the potential to cause damage or distress to individuals, CHS or the Children's Hearings System, this may lead to a review or termination of CHS' contract with the third-party.