children's hearings scotland

The Children's Panel – life changing.

INFORMATION SECURITY POLICY

Version	Date	Owner	Summary of Changes
V1.0	15/05/2013	Information Governance Lead	• N/A
V1.1	10/12/2013		• Addition of policies and procedures at section 4; amendment of the Government Classification Policy information at 6.1; amendment of 7.3.
V1.2	20/02/2014		• 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.
V1.3	03/06/2014		• Review period extended from 6 months to 2 years.
V1.4	29/07/2014		• Amendment of responsibilities at 5.3 and policies at section 4.
V1.5	19/08/2014		• Reviewed by Audit and Risk Management Committee (ARMC) – additional sections at 1.3 and 1.4. Clarification of roles and responsibilities at section 5.
V2.0	26/08/2014		• Final policy approved by the CHS Board.
V2.1	25/03/2015		• Minor amendments to reflect changes in job titles and additions to the legislative framework.
V3.0	31/03/2015		• Final policy approved by SMT.
V3.1			• Minor amendments made to terminology with a comprehensive review to take place prior to implementation of GDPR in May 2018.
V3.2			
V4.0	30/03/2018		• Review to be compliant with GDPR.
V4.1	18/02/2022	Information Governance & DPO	• Final policy approved by SIRO. • 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.
V5.0	28/02/2022		• Final policy approved by SIRO

Approvals	Approved by SIRO 28/02/2022

Date Approved: 28th February 2022
Date For Renewal: February 2024

1. Introduction

1.1 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.

1.2 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 National Team, Area Support Teams (ASTs), Clerks to the AST, panel members 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.

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

1.4 Our Publication Scheme[1] 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.

1.5 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.

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

2. Purpose and scope

2.1 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.

[1] The purpose of the Publication Scheme is to allow the public to see what information is available (and what is not available) 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.

2.2 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
- information relating to IT systems, manual systems, utilities and data used in the functioning of the organisation

2.3 This policy covers all CHS National team staff and Board members, panel and AST members, and Clerk to the ASTs (including their teams).

3. Legislative framework

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

3.2 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

3.3 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: 2013 - Information Security
- Government Security Classifications Policy

4. Relationship to other CHS policies, procedures and guidance

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

- *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*
- *Managing Information – Guidance for Staff, Managing Information – summary guidance for panel and AST members and Managing Information – Guidance for Clerks*
- *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*

5. Roles and responsibilities

5.1 The Chief Executive (CEO) of CHS, as Accountable Officer, has overall responsibility for information security. The CEO is responsible for ensuring that AST and panel members receive the appropriate level of training to support the implementation of this policy.

5.2 The Depute Chief Executive is designated as the Senior Information Risk Owner (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*.

5.3 The implementation of, and compliance with this policy, is delegated to the Information Governance and Data Protection Officer with the support of the Information Governance Records Officer and Digital Team. The Information Governance Team must support all panel and AST members as well as Clerks, CHS National team staff and Board members, to comply with their obligations under this policy;

- issue guidance and training
- monitor and report

5.4 Each CHS employee, Board member, AST member, Clerk and panel member is responsible for ensuring that they are familiar with and comply with all relevant policies, procedures and guidance[2]. Furthermore, they are expected to take all reasonable steps to protect CHS information from unauthorised use, modification, disclosure or destruction.

5.5 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

[2] 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*.

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*.

5.6 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 suspend the Board member from their duties whilst an investigation is carried out by The Standards Commission for Scotland in line with the *Board member's Code of Conduct*.

5.7 In the event of a serious information security incident or breach of this policy by a panel or AST member, 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/AST member from their duties whilst an investigation is carried out. Depending upon the outcome of the investigation, it may lead to a member being removed from the panel or AST[3].

6. Policy statement

6.1 CHS has identified overall information security objectives, which include:

- to ensure that all staff, Board members, AST members, Clerks and their teams, panel members and data processors are aware of their responsibilities in order to preserve information securely by providing appropriate awareness raising and training and contractual/service level agreements

- to ensure that confidentiality of information is maintained and is only accessible to authorised users when required and protected against unauthorised access (i.e. keep pin numbers separate from ID cards accessing buildings, securely store personal data in lockable cabinets, ensure shredding of documents no longer required, is carried out in a secure way)

- to ensure that integrity of information is protected from unauthorised modification and that information is not disclosed to unauthorised persons through deliberate or careless action, or files are moved/deleted in error

- to ensure availability of information and associated assets to authorised users when needed and to protect the information and systems from any threats which may occur

- to ensure that all physical and information assets are identified, risk assessed and control(s) identified, implemented, maintained and reviewed to ensure that control(s) are effective

- to ensure that regulatory and legislative requirements are identified and met

[3] Under the 2011 Act, the National Convener may with the consent of the Lord President of the Court of Session, remove a panel member during the 3 year appointment period if satisfied that a person is unfit to be a panel member due to conduct.

- to ensure that the Business Continuity Plan is produced, maintained and tested as far as practicable to mitigate against a disaster for loss of data due to fire, flood, theft and ransom ware, engaging with the Communications team

- to ensure that information governance training is available to all CHS staff, Board members, AST members, Clerks and panel members and that this training is refreshed on a regular basis

- to ensure that all breaches of information security and suspected weaknesses / incidents are reported within time limits, investigated, fed back and learnt from, introducing improved processes when required

- to take measures to ensure that information stored in the online portal is kept secure and in line with our statutory duties, with appropriate firewalls to protect against intrusion and prevent users within our organisation accessing websites that present a threat to CHS

- to have anti-virus or anti-malware products regularly scanning CHS networks to prevent or detect threats ensuring they are kept up to date, switched on and monitored

6.2 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

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

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

7. Managing our information assets

7.1 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.

7.2 Confidentiality and security rules continue to apply to all business conducted on behalf of CHS when a staff member 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. As with work in the office, breaches will be dealt with under the CHS Disciplinary Procedure. Staff members are

responsible for ensuring the security of the papers and equipment, and that basic levels of security are in place, such as locked windows and doors. Particular care must be taken when confidential papers are being transported to and from home.

7.3 CHS has identified its information assets (definable pieces of information, stored in any manner which is recognised as valuable to the organisation) and the owners of these assets. This information is contained in the Information Asset Register

From identification of the assets the following is ascertained:

- risks to those assets
- potential impact cause by those risks
- mitigating controls to safeguard this information

7.4 Please refer to the Information Asset Risk Register (reviewed and updated at least every six months) 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 risk management policy and the controls in place to limit exposure to risk.

Document Control

Title	Information Security Policy
Author	Danielle Metcalfe
Approved by	SIRO
Date of approval	Pending
Version number	5.0
Review frequency	Every two years
Next review date	February 2024