Information Security Policy

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.

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. The requirement to keep information secure will be balanced with the need for CHS, Area Support Teams (ASTs), Clerks to the AST, panel members and the Children's Panel to operate effectively.

1.3 CHS are committed to openness, transparency and accountability within the framework of the Data Protection Act 1998 (DPA) and the Freedom of Information (Scotland) Act 2002 (FOISA).

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' integrity in our dealings with all our stakeholders.

2. Purpose and scope

2.1 The purpose of this policy is to set out CHS' 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.

Date Approved: 26 August 2014 and 31 March 2015
Date for Review: March 2017

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 collect, holds, uses and destroys information.

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

- Children's Hearings (Scotland) Act 2011
- The Children's Hearings (Scotland) Act 2011 (Rules of Procedure in Children's Hearings) Rules 2013
- Public Records (Scotland) Act 2011
- Equality Act 2010
- The Environmental Information (Scotland) Regulations 2004
- Communications Act 2003
- Freedom of Information (Scotland) Act 2002
- Regulation of Investigatory Powers Act 2000
- Data Protection Act 1998
- Human Rights Act 1998
- Employment Rights Act 1996
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988
- Prescription and Limitation Acts 1973 and 1984

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

- BS ISO 27001: 2005 - Information Security
- BS ISO 15489: 2001 – Information and Documentation – Records Management (Parts 1 & 2)
- 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:

- *Managing Security Incidents Procedure* and *Reporting Information Security Incidents – summary guidance*

- *Security Classifications Policy* and *Classifying sensitive documents and emails – summary guidance*
- *Secure Transfer of Information Guidelines*
- *Keeping Information Safe – key tips* for panel members, AST members, Clerks, and Board members

4.2 This policy relates to the following CHS policies, procedures and guidance:

- *Data Protection Policy* and *Data Protection – Guidance for Staff*
- *Acceptable Use Policy* and *Acceptable use – summary guidance*
- *Records Management Policy*
- *Managing Information – Guidance for Staff*, *Managing Information – summary guidance for panel and AST members* and *Managing Information – Guidance for Clerks*
- *Retention and Disposal Schedule* and *Retention and Disposal – Guidance for Clerks*
- *Business Continuity Plan* and *Vital Records Strategy*

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 Director of Finance and Corporate Services is designated as CHS' Senior Information Risk Owner (SIRO). The SIRO 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' *Retention and Disposal Schedule*.

5.3 The implementation of, and compliance with, this policy is delegated to the Information Governance Officer with the support of IT colleagues. The Information Governance Officer 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 and monitor and report on compliance with this policy.

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 Hearings System, it may be 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*.

[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*.

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, it may be 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, it may be 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.
- 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.
- 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.
- To ensure that the Business Continuity Plan is produced, maintained and tested as far as practicable.
- 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 and investigated.

[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 take measures to ensure that information stored in the online portal is kept secure and in line with our statutory duties.

- To adopt the Government Security Classifications Policy for the classification of records from 02 April 2014. This policy defines three levels of protective markings: TOP SECRET, SECRET, OFFICIAL. These markings define how documents should be stored and handled. Please refer to the *Security Classifications Policy* for further information.

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
- 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 will use physical, personnel, technical and procedural means to achieve appropriate security measures.

7.2 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

7.3 Please refer to the Information Asset Register (reviewed and updated at least every six months) for more information about how CHS will manage its information assets and assess the risks associated with these assets.

Document Control

Title	Information Security Policy
Author	Ava Wieclawska, August 2014 and March 2015
Approved by	CHS Board and Senior Management Team
Date of approval	26 August 2014 and
Version number	3.0
Review frequency	Every two years
Next review date	March 2017

Status Control

Version	Date	Status	Author(s)	Amendments to policy	Approved by
1.0	15/05/2013	Final	Sara Brodie	N/A	CHS Board
1.1	10/12/2013	Draft	Sara Brodie	Addition of policies and procedures at section 4; amendment of the Government Classification Policy information at 6.1; amendment of 7.3.	SMT
1.2	20/02/2014	Draft	Ava Wieclawska	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.	
1.3	03/06/2014	Draft	Ava Wieclawska	Review period extended from 6 months to 2 years.	
1.4	29/07/2014	Draft	Ava Wieclawska	Amendment of responsibilities at 5.3 and policies at section 4.	
1.5	19/08/2014	Draft	Ava Wieclawska	Reviewed by Audit and Risk Management Committee (ARMC) – additional sections at 1.3 and 1.4. Clarification of roles and responsibilities at section 5.	ARMC
2.0	26/08/2014	Final	Ava Wieclawska	Final policy approved by the CHS Board.	CHS Board
2.1	25/03/2015	Draft	Ava Wieclawska	Minor amendments to reflect changes in job titles and additions to the legislative framework	SMT
3.0	31/03/2015	Final	Ava Wieclawska	Final policy approved by SMT	SMT