Data Protection Policy

Date Approved: 11/06/2026
Approved by: SIRO
Version: 8.0

Next Review Date: 11/06/2027
Owner: Information Governance and Data Protection Officer

Document Version Control

Version Number	Change/Update	Author/Owner	Date
0.1	N/A	Sara Brodie	13/03/2013
1.0	N/A	Sara Brodie	20/03/2013
1.1	Additional references to ICO at 2.2; conduct process at 2.3; additional policies at 3.1; damage and distress at 4.4; DPOs at 7.3; e-learning at 7.12; alerting CHS at 8.1.3; notification responsibilities at 8.2.1; and Info mailbox at 8.6.1. New sections: 7.9-7.11 and 10.3. Changes to sections at 8.7.1.	Sara Brodie	10/12/2013
1.2	Additional references to Board member's conduct at 2.3; additional policies at 3.1; IAOs at 7.2; board member's responsibilities at 7.4; conditions for processing at 8.1.1; ISMS at 8.7.1 and board member's responsibilities at 10.1. New footnote at 5.6 and amendment to timescales at 8.6.1.	Ava Wieclawska	20/02/2014
1.3	Review period extended from 6 months to 2 years. Restructuring throughout.	Ava Wieclawska	02/06/2014
1.4	Additional references to statutory and regulatory obligations at 1.1, to summary guidance at 1.4; to examples of personal data at 2.1; and to contact email at 4.1.3.	Ava Wieclawska	23/07/2014
1.5	Reviewed by the Audit and Risk management Committee (ARMC) – changes made to section 5 to clarify roles and responsibilities.	Ava Wieclawska	19/08/2014
2.0	Final policy approved by the CHS Board.	Ava Wieclawska	26/08/2014
2.1	Minor changes to terminology and format throughout; additions to 4.7.1 re security measures.	Ava Wieclawska	08/07/2016
3.0	Minor changes to terminology	Callum Morrison	05/01/2017
3.1	Revised to take into account Data Protection law changes	Alice Wilson	13/11/2017
3.2	Final finishing for sign off with SIRO	Alice Wilson	04/05/2018
4.0	Final policy approved	Katie Crone Barber	24.05/2018
5.0	Updated in line with CHS current systems	Sophie-Elise Anker	18/02/2022
6.0	Revised in line with organisational changes and changes to CHS processes	Danielle Metcalfe	11/09/2024
6.1	Minor updates to terminology	Cedric Krummes	29/10/2025
6.2	Minor changes to clarify application of the legislation and revisions in line with organisational changes	Danielle Metcalfe	30/10/2025
6.3	Updated in line with revised CHS policy template	Danielle Metcalfe	30/10/2025
7.0	Final policy approved by SIRO	Danielle Metcalfe	31/10/2025

8.0	Minor updates in line with Data (Use and Access) Act 2025 and ISO 27001	Danielle Metcalfe	10/06/2026

CHS Data Protection Policy

Contents

.....1

1. Definitions.....4

2. Introduction and Purpose.....5

3. The Data Protection Legislation.....6

4. Data Protection Principles.....7

5. Data Subjects Rights.....15

6. Roles and Responsibilities.....17

7. Breaches of this policy.....19

8. Monitoring and Review.....19

1. Definitions

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

Data	information which: a) is being processed by means of equipment operating automatically in response to instructions given for that purpose b) is recorded with the intention that it should be processed by means of such equipment c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record or e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d)
Relevant filing system	The ICO considers that a relevant filing system exists where records relating to individuals (such as personnel records) are held in a sufficiently systematic, structured way as to allow ready access to specific information about those individuals.
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 of more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural personal (Article 4(1) of the UK GDPR) This can include application forms, complaints records, contact details etc.
Special Categories of Personal Data	information covering: the racial or ethnic origin of the data subject; political opinions; religious or philosophical beliefs; membership of trade unions; genetic data; biometric data; Data concerning health; Data concerning a natural person's sex life or sexual orientation; or the commission of any offence or criminal records. This type of data must be carefully handled. Additional security measures may be necessary to protect special category personal data.

Data Controller	A person (usually an organisation) who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data Processor	Any person or organisation (other than an employee of the data controller) who processes the data on behalf of the data controller.
Data Subject	The living individual who is the subject of the personal data.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing of data relates to the entire lifecycle of data.

2. Introduction and Purpose

Children's Hearings Scotland (CHS) is required to collect and maintain certain personal data about individuals for the purpose of satisfying our statutory, operational and regulatory obligations.

Data Protection legislation[1] places requirements on the CHS Community which includes National Team members (permanent and temporary, including contractors and agency), Board members, volunteers, Experts by Experience, Clerks (including their teams), and third parties processing personal data on CHS' behalf. It is the responsibility of all CHS Community members to protect the personal data of data subjects by following this policy and the associated guidance.

CHS (this includes Board and Panel Members and Panel Practice Advisors) is a Data Controller, as defined in Article 4(7) of the UK General Data Protection Regulation (GDPR), and must ensure that all of the data protection requirements are implemented.

[1] Data Protection legislation includes the UK General Data Protection Regulation, the Privacy and Electronic Communications Regulations, the Data Protection Act 2018, and the Data (Use and Access) Act 2025.

The purpose of this policy is to outline the key principles of data protection legislation and set out how CHS meets its legal obligations to ensure that all data is held and processed in compliance with data protection legislation. All members of the CHS Community must read this policy.

3. The Data Protection Legislation

Data Protection legislation provides a framework of rights and duties which is designed to safeguard personal data. The legislation balances the needs of organisations to collect and use personal data for clear, legitimate purposes against the individuals' rights to privacy. Wherever data is held, whether it is panel papers, complaints records, emails or any other records relating to the Children's Hearings System (the System), the rights of the individual to privacy and access to their personal data apply.

The legislation applies to paper and electronic records and audio and visual recordings and does not differentiate between these different types of records. If an individual is identifiable in a record, then the record contains personal data, and therefore the data protection obligations apply.

Compliance with data protection legislation is regulated by the Information Commissioner's Office (ICO) which has various powers, including issue of an enforcement notice (breach of which is a criminal offence) and the ability to fine organisations up to £17.5 million (or 4% of total worldwide annual turnover, whichever is higher) for failing to comply. If an individual unlawfully obtains or discloses personal data, they could be committing a criminal offence.

There are also wider implications for failing to comply with data protection legislation. Disclosure of personal data can cause real harm, damage or distress to individuals; there is a risk of compensation claims by those affected; the ICO can publicise security breaches leading to reputational damage; and stakeholders may lose trust in the way CHS manages personal data. We are all individually responsible for protecting personal data.

4. Data Protection Principles

Data Protection legislation sets out six principles by which personal data must be processed. Along with the 6 Principles there is an overarching Accountability requirement. CHS must ensure that personal data is:

1. Processed fairly, lawfully and transparently
2. Collected for explicit and lawful purposes and processed in a manner compatible with those purposes (purpose limitation)
3. Adequate, relevant and not more than necessary for those purposes (data minimisation)
4. Accurate and up to date, inaccuracies should be changed without delay
5. Kept only as long as is necessary (storage limitation)
6. Processed securely and protected against unauthorised or unlawful processing, loss or destruction

4.1 Principle 1 - Personal data shall be processed fairly, lawfully and in a transparent manner in relation to the data subject

In practice, Principle 1 means that the CHS Community must:

- have legitimate grounds for collecting and using personal data
- not use personal data in ways that have unjustified adverse effects on individuals
- be transparent about how we intend to use personal data, and give individuals appropriate fair processing notices (privacy notices) when collecting their personal data
- handle personal data only in ways individuals would reasonably expect
- Not do anything unlawful with the data

4.1.1 Conditions for processing

Processing means collecting, recording, organising, storing, using, disclosing, transferring, sharing, retaining, archiving or disposing of personal data or carrying out any operation or set of operations on the personal data, including –

- organisation, adaptation or alteration of the data
- retrieval, consultation or use of the data
- disclosure of the data by transmission, dissemination or otherwise making available
- alignment, combination, blocking, erasure or destruction of the data

If any aspect of processing is unfair, there will be a breach of this principle.

Before we can process any individual's personal data we must ensure that conditions for processing are met. The conditions for processing are set out in the Schedules of data protection legislation. When processing special category (sensitive) personal data, we must be able to demonstrate that there are two conditions that apply under the appropriate two Schedules detailing conditions for processing. The Information Governance team must be contacted prior to the undertaking of any processing personal data that is new for CHS.

4.1.2 Privacy Notices

When personal data is collected about individuals, they should be told exactly how that data is to be used. This is called a privacy notice. It is important that such notices are concise, transparent, intelligible and easily accessible. It must be written in clear and plain language, especially if the notice is for a child. So it is important that any privacy notices specifically for children is clear and in a language that they will understand. The notice should tell them:

- Who CHS is, including name and contact details
- Contact information of the Data Protection Officer (DPO)[2]
- why we need their data, and that this must be done fairly and lawfully
- what purpose we will use their data for (and that it will not be used for any purpose incompatible with the original purpose)
- the categories[3] of personal data obtained and the source of the data (if the data has not been collected directly from the individual)
- if the collection of data is consensual, contractual, a legal obligation, or part of CHS' public task and, if it is consent-based, how to withdraw consent
- who we will share their data with (and what these third parties will use the data for);
- about their rights under data protection legislation, including the right to access, amend, restrict and erase the information we hold about them
- the details of the existence of automated decision-making, including profiling (if applicable)
- how they can make a complaint to CHS and to the Information Commissioner's Office (ICO)
- how we will ensure that the data is kept secure, accurate and up to date
- how long we will keep the data[4] and that we will dispose of data securely
- if the information is to be transferred out with the European Economic Area (EEA)

If the data is collected by another organisation, it is important to provide the individuals with the notice when we receive the data. A record of the privacy notice should be held for as long as the data itself is held.

[2] The DPO in CHS is the Information Governance and Data Protection Officer (IG&DPO)
[3] See CHS Privacy Notices for further information
[4] Please refer to the CHS *Retention and Disposal Schedule* for guidance.

If you think someone would not know about the use of their data or would find it objectionable in any way that causes detriment to an individual, then it is necessary to tell them about it. This is 'actively communicating' a privacy notice and means that we will tell an individual about the collection and processing of their personal data. This is different to having a privacy notice available for individuals to access if they want to find out more about how we handle personal information. We will also actively communicate a privacy notice when collecting sensitive personal data.

CHS has a privacy notice on our corporate website for members of the public. There is one specifically for volunteers, staff, applicants, and individuals with lived experience working with CHS, including a separate notice for children. If there is a change to how we process personal data, please speak to the IG Team for advice to ensure that individuals are fully informed of how we use their data.

When making privacy notices available, the same medium should be used to deliver the notice as is used to collect the information. For example, if the information is being collected through a website, the notice will also be available on the website.

4.1.3 Disclosure of personal information to third parties

Information about identifiable individuals should only be disclosed on a need-to-know basis. The validity of all requests for disclosure of personal data without consent from the data subject must be checked. The identity of those requesting data and their legal right to request or demand information must be validated. The reasons for any disclosure made without consent must be documented.

Police officers or others requesting information for the purposes of a criminal investigation should be asked to put their request in writing. The request should include:

- what information is required
- why it is needed
- how the investigation will be prejudiced without it

This requirement can be set aside where the request is made in an emergency and a person is in immediate and imminent risk of serious harm.

Decisions related to the disclosure of information to third parties must be taken at an appropriately senior level within CHS. If an AST member, Panel Member or Clerk, receives an information request they must alert the CHS National Team.

Any member of CHS staff, volunteer, or Clerk who is required to send personal identifiable data in any format to countries outside the European Economic Area (EEA), must discuss

this with the Data Protection Officer (DPO) as the levels of protection for the information may not be as comprehensive as those in the UK.

4.1.4 Information Sharing

CHS produces, contributes to and signs Data Processing Contracts, Information Sharing Protocols and Data Access Agreements where necessary in order to ensure the secure and lawful transfer of personal data between parties.

4.1.5 Data Protection Impact Assessments (DPIAs)

CHS conducts DPIAs prior to initiating a project or process and prior to making changes to an existing process which will involve the collection/use of personal data, in order to assess the privacy risks to individuals. There are guidance and templates available for the CHS National Team to complete these impact assessments and the IG Team will provide assistance and guidance where necessary.

4.2 Principle 2 - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

In practice, Principle 2 means that the CHS Community must:

- be clear from the outset about why we are collecting personal data and what we intend to do with it
- ensure that the reasons for processing the personal data are clear and specified – including in privacy notices
- pay an annual notification fee to the regulator, the UK Information Commissioner's Office (ICO)
- ensure that if we wish to use or disclose personal data for any purpose that is additional to the originally specified purpose, the new use or disclosure is fair and lawful and is compatible with the original purpose

4.2.1 Notification

CHS must provide an annual notification fee to the UK Information Commissioner's Office. The ICO requires the name and address of the controller, staff numbers, financial turnover and contact information of the DPO, and if applicable the individual completing the fee registration.

4.2.2 Incompatible re-use of information

CHS should be open and transparent about the way in which we process personal data. Personal data must not be re-used for any purpose that is incompatible with the original purpose for which it was collected (e.g. personal data collected for the purpose of responding to a complaint must not be reused for sending marketing emails).

4.2.3 CCTV

CCTV cameras collect personal data in the form of images, as such if CCTV footage is to be collected by CHS individuals should be appropriately notified of its use through privacy notices (see section 3.1.2)

CCTV cameras are in operation at the entrances to Thistle House and in the car park. These cameras are owned by Scottish Legal Aid Board (SLAB) and the images are held in line with Scottish Government policies and procedures.

4.3 Principle 3 - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Data Minimisation)

In practice, Principle 3 means that the CHS Community must:

- only hold personal data about an individual that is sufficient for the purpose we are holding it for in relation to that individual
- ensure that we hold enough data that is adequate for the purposes we are holding it for
- not hold more data than we need for that purpose (data minimisation)

Personal data should not be held on the off-chance that it may be useful in the future. However, it is permissible to hold personal data for a foreseeable event that may never occur.

Where special category (sensitive) personal data is concerned, it is particularly important to make sure that we collect or retain only the minimum amount of data we need.

4.4 Principle 4 - Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

In practice, Principle 4 means that the CHS Community must:

- take reasonable steps to ensure the accuracy of any personal data we obtain
- ensure that the source of any personal data is clear
- carefully consider any challenges to the accuracy of data held
- consider whether it is necessary to update the data

The law recognises that it may not be practical to double-check the accuracy of every item of personal data we process. The law makes special provision about the accuracy of information that individuals provide about themselves, or that is obtained from third parties.

Each Information Asset Owner (IAO) will undertake a regular audit of their information assets to ensure that they are accurate and up to date.

4.4.1 Panel Member and Panel Practice Advisor (PPA) contact details

It is the responsibility of each Panel Member and PPA to ensure that their name and contact details are accurate and up to date. Panel Members and PPAs should update their own record in CSAS, or notify their Clerk if they are unable to.

CHS are responsible for ensuring that the remaining record is accurate and up to date.

For the purposes of communications with Panel Members and PPAs, contact details must be extracted from CSAS on the day of the communication. It is important that out of date contact lists are not used and that the CHS Community update CSAS when there is a change in address. If old contact lists are used, or if CSAS is not kept up to date, this can result in a breach of data protection legislation.

4.5 Principle 5 - Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes

In practice, Principle 5 means that the CHS Community must:

- review the length of time we keep personal data
- consider the purpose or purposes we hold the data for in deciding whether (and for how long) to retain it
- securely dispose of data that is no longer needed for this purpose or these purposes
- update or securely dispose of data if it goes out of date

CHS National Team and Clerks must ensure that they are aware of, and comply with, CHS' Retention and Disposal Schedule.

4.6 Principle 6 - Personal data shall be 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

In practice Principle 6 means that CHS must have appropriate security measures to prevent the personal data held being accidentally or deliberately compromised. In particular, CHS:

- designs and organises our security to fit the nature of the personal data we hold and the harm that may result from a security breach
- is clear about who is responsible for ensuring information security
- makes sure we have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff
- is ready to respond to any breach of security swiftly and effectively

4.6.1 Keeping personal information safe and secure

Organisational security:

- CHS has an Information Governance Policy Framework in place with four overarching policies: Information Security, Data Protection, Acceptable Use and Records Management.
- CHS has a suite of policies, procedures and guidance which support the above policies and govern the processing of personal data.
- CHS has an Information Security Management System containing a suite of policies, procedures and training in alignment with the ISO 27001 standard
- CHS highlights information risks on its strategic risk register which is considered by the Audit and Risk Committee and CHS Board on a regular basis.
- Only authorised people can access, alter, disclose or destroy personal data and those people only act within the scope of their authority.
- CHS Community members must undergo mandatory data protection training and complete refresher training on a regular basis.
- CHS Community members must read, understand and comply with this policy and accompanying policies, procedures and guidance for managing information.
- Personal information must not be disclosed, accidentally or otherwise to any unauthorised third party.
- CHS has data processing contracts in place with data processors across the country and carries out audits of these data processors, in line with Principle 6.

Physical security:

CHS National Team and Board members:

- Access to the CHS office is governed by Scottish Government's *Security Policy*.
- Visitors must be signed in and out and escorted whilst on the premises.
- Confidential paper waste must be disposed of in the confidential waste bin.
- CHS operates a clear desk policy.
- Personal data in the form of hard copy records must be kept in a locked filing cabinet, drawer or other secure area.
- Personal data must not be printed at home except in exceptional circumstances where this has prior approval from the Information Governance team for a limited and specific purpose.

Panel Members, PPAs and Clerks:

- Confidential paper waste must be disposed of using a cross-cut shredder or by handing to the Clerks for secure destruction.
- Volunteers must ensure when handling personal data at home that it is kept out of sight and in a safe place and that no other members of the household can access the personal data.
- Volunteers must ensure that personal data is placed within a zipped/locked bag when travelling to a hearing/meeting.
- When travelling to a hearing/meeting by car volunteers must lock the zipped/locked bag in the boot of the car or another secure area (e.g. glove box) and this must never be stored in a car overnight.
- Personal data must not be accessed/read/discussed while on public transport or when in public places.
- Personal data must not be left unattended at any time – this includes information on a computer screen and information on paper documents.
- Clerks must keep information relating to the Childrens' Hearings System separate from local authority information on electronic systems.

IT Security:

- IT equipment must be disposed of in a secure manner in line with the ISMS Data Retention and Erasure Policy. To arrange disposal of ICT equipment please contact digital@chscotland.scot
- Access to special category (sensitive) personal data is protected by placing additional controls on access.
- Personal data in the form of computerised records are kept on a secure IT system which is either password protected, encrypted or has additional device security.
- Personal data must not be kept on unsecure portable data storage devices.

- Laptops must be kept in a secure location at all times
- CHS staff must lock their computer screens (Windows key + L) when away from their desks.
- Devices must be locked with a password in accordance with the password requirements detailed in the Acceptable Use Policy.

In addition to the measures highlighted above, CHS has an Information Governance Policy Framework (containing this policy, the Information Security Policy, the Records Management Policy and the Acceptable Use Policy) and Information Security Management System policies in place that identify each of the IG and information security related policies and procedures in existence and to whom it applies to in the CHS Community. Guidance on managing information appropriately and in line with our statutory obligations can be found in the relevant policies and procedures.

4.6.2 Data Processors

Where CHS uses a third party to process personal data on its behalf, the contractor becomes a data processor for CHS and must sign a Data Processing Contract which ensures that they are taking adequate steps to comply with Principle 6 (and all other data protection requirements) on CHS' behalf. Data Processors have legal obligations under data protection legislation, as well as the explicit instructions contained within the data processing contract. Data Processors must report any security incident to CHS immediately. CHS retains legal responsibility as data controller and it is important that the contracts are detailed and clear on what the data processors can and cannot do. Therefore, it is important that those who manage the contracts must ensure that all security procedures necessary are specified in the contract, and they are subsequently monitored to ensure that they are in place. This includes carrying out audits regularly to ensure that the contract obligations are being met.

5. Data Subjects Rights

5.1 As well as the 6 Principles under data protection legislation, every data subject has additional rights under the data protection legislation:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (commonly known as the right to be forgotten (RTBF)
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

5.1.1 The Right to be Informed

This links with Principle 1 and the transparency requirement to actively communicate privacy notices to the individuals. As referenced in section 4.1.2, individuals must be provided with a privacy notice detailing what we do with the personal data, how long it is kept, if it is shared, who it is shared with, their rights under data protection legislation, including how to complain to CHS and the ICO, etc.

5.1.2 Right of Access

Individuals have a right to make a request orally or in writing to receive a copy of their personal data held by the CHS Community. CHS has a procedure to deal with requests for access to personal data known as 'Subject Access Requests' (SARs). SARs are handled by the CHS Information Governance Team. If a SAR is received by staff, the Clerk's office, or by anyone in the CHS Community, that person or team should notify the CHS Information Governance Team within 2 working days.

SARs are acknowledged by CHS within 3 working days of receipt by CHS (a request for proof of identification can be made at this time). Every SAR is responded to within one month of receipt of the request/identification/fee where applicable. If any delays occur, CHS writes to the data subject explaining the reason.

5.1.3 The Right to Rectification

This is the right for inaccurate personal data to be rectified or completed if it is incomplete. An individual can make a request for this in writing or verbally. As with the right of access, CHS have one month to respond. This links with principle 4 and the data controller's obligations to keep personal data accurate and up to date.

5.1.4 The Right to Erasure (Right to be Forgotten)

This is a right which means individuals can request that the personal data held about them is erased. It is known commonly as the 'Right to be Forgotten'. Individuals can make the request to erase verbally or in writing. CHS has one month to respond to a request. It's important to note that the right is not absolute and only applies in certain circumstances.

5.1.5 The Right to Restrict Processing

Individuals have the right to request the restriction or suppression of their personal data. As with the Right to Erasure this is not an absolute right and only applies in certain circumstances. CHS has a calendar month to respond to the request. It links closely to the Right to Rectification (see section 4.1.3). When processing is restricted, a data controller can store the data but not use it.

5.1.6. The Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy, or transfer their data from one IT system to another in a safe and secure way without affecting its usability. Doing this enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits. As with the other rights, this is not an absolute right, it only applies to information the individual has provided to the organisation.

5.1.7. The Right to Object

Individuals have the right to object to specific processing, based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.

5.1.8 Rights in relation to automated decision making and profiling

The rights for individuals in relation to automated individual decision-making (making a decision solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process. The rights mean that where automated processing occurs the privacy notice explains exactly how the decision making is made, how to request human intervention or challenge a decision.

6. Roles and Responsibilities

6.1 CHS National Team and Board members

- The National Convener (NC) of CHS has overall responsibility for data protection and information security. The NC is responsible for ensuring that CHS Community members processing personal data receive the appropriate level of training to support the implementation of this policy. The NC is also responsible for ensuring that all collection and processing of personal data complies with data protection legislation.

- The Director of Business and Finance is designated as CHS' Senior Information Risk Owner (SIRO). The SIRO is a 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*. The SIRO must also ensure that all CHS Community members familiarise themselves with the content of this policy.

- The designated Data Protection Officer (DPO) is responsible for identifying and publicising data protection responsibilities across the CHS Community.

- Regional team members are responsible for raising awareness of data protection responsibilities at a local level and highlighting any data protection issues or concerns to the IG team. In particular, they are expected to monitor compliance with this policy and other guidance issued by CHS and report any suspected or known vulnerabilities and incidents in relation to the management of information, to IG. It is important that they report any incidents or vulnerabilities immediately to ensure that where applicable CHS can meet the required deadline of reporting a breach to the ICO within 72 hours. They are also expected to support in the investigation of any breaches of the policy or data protection legislation and to disseminate key IG messages at local AST events and meetings.

- CHS National Team, Experts by Experience and Board members are responsible for ensuring that they are familiar with and comply with this policy.

- Data protection training is provided to all staff, Board Members and Experts by Experience through an eLearning package, to be completed on appointment and annually.

6.2 PPAs and volunteers with additional responsibilities (e.g. Panel Engagement Leads)

- All PPAs and volunteers with additional responsibilities processing personal data are responsible for ensuring that they are familiar with and comply with this policy and other guidance issued by CHS. They are expected to assist their Regional Teams in raising awareness of the importance of data protection and keeping information safe. They are also expected to assist their regional teams if a security incident occurs and should report any incidents to the Tribunal Delivery Manager and the IG Team immediately. Data protection training is provided to all volunteers through an eLearning package, to be completed at pre-service/appointment and every two years.

6.4 Clerks to the AST

- Clerks and their teams provide support to the National team, PPAs and panel members at local level. This support arrangement is governed by the Collaborative Agreement between local authorities and CHS.

- CHS has put in place Data Processing Contracts (DPC) to govern the processing of personal data by local authorities on behalf of CHS. As data processors, they have additional legal obligations, including reporting information security incidents.

- Clerks must report incidents to the National Team immediately when they become aware of an incident. This is important, as there is a duty to report serious breaches to the ICO within 72 hours of discovery.

6.5 Panel Members

- Data protection training is delivered by the national training provider at pre-service stage and on a refresher basis through an eLearning package. All Panel Members are required to complete the eLearning training every two years.

- All Panel Members are responsible for ensuring that they are familiar with and comply with this policy and other policies and guidance issued by CHS.

- All Panel Members must inform the Information Governance Team immediately at information@chs.gov.scot if an information security incident occurs.

7. Breaches of this policy

7.1 All personal data recorded in any format must be handled securely and appropriately in line with the Data Protection legislation. CHS staff, Experts by Experience, and Board members, volunteers, Clerks, and third party contractors/suppliers with access to CHS information must not disclose information for any purpose outside their normal role with CHS.

7.2 Breaches of this policy by a member of CHS staff will be considered as a disciplinary issue and will be investigated in line with the *Staff Code of Conduct*. Breaches of the policy by a Board member may lead to investigation by The Standards Commission for Scotland in line with the *Board member's Code of Conduct*. The NC will investigate (or appoint a member of staff to investigate) any breaches of this policy by a PPA or panel member. A breach of this policy by a Clerk or a member of their team or any other third party contractor/supplier will be handled in line with the terms of the Data Processing Contract.

8. Monitoring and Review

7.1 This policy will be reviewed annually or as appropriate to take into account changes to legislation that may occur, and/or guidance from the Scottish Government and/or the Information Commissioner's Office.