# Data Protection Policy

## 1. Introduction and purpose

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

1.2 The Data Protection Act 1998 (the DPA) places obligations on CHS employees (permanent and temporary, including contractors), Board members, Area Support Team (AST) members, Clerks to the AST (including their teams), and panel members, to protect the information of data subjects.

1.3 CHS (this includes panel and AST members) is a Data Controller, as defined in Section 1 of the DPA, and must ensure that all of the DPA requirements are implemented.

1.4 The purpose of this policy is to outline the key principles of the DPA and set out how CHS meets its legal obligations to ensure that all data is held and processed in compliance with the DPA. All staff, Board members, panel and AST members, and Clerks to the AST must read this policy. A summary guidance document is also available on the CHS website and CHIRP.

## 2. The Data Protection Act 1998

2.1 The DPA establishes a framework of rights and duties which is designed to safeguard personal data. It balances the needs of organisations to collect and use personal data for clear and legitimate purposes against the right of individuals to respect for the privacy of their personal data. 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 apply.

2.2 The DPA applies to paper and electronic records and audio and visual recordings, and does not differentiate between these different types of records.

2.3 Compliance with the DPA is regulated by the ICO who can issue an enforcement notice (breach of which is a criminal offence) and fine organisations up to £500,000 for failing to comply. If an individual unlawfully obtains or discloses personal data they could be committing a criminal offence.



*Date Approved: 26 August 2014*
*Date for Review: August 2016*

2.4 There are also wider implications for failing to comply with the DPA; 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

## 3. Definitions[1]

3.1 **Data** means 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 as defined by section 68 or
e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d)

3.2 A **relevant filing system** is defined as: *"any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible."*

The ICO's view is that this definition is intended to cover non-automated records that are structured in a way which allows ready access to information about individuals. As a broad rule, 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.

3.3 **Personal data** means information about a living individual who can be identified from that information and other information which is in, or likely to come into, the data controller's possession. This can include application forms, complaints records, contact details etc.

3.4 **Sensitive Personal Data** is information covering:

- the racial or ethnic origin of the data subject
- political opinions
- religious or other beliefs of a similar nature
- membership of trade unions
- physical or mental health or condition
- sexual life

[1] Further information about definitions is available from the Information Commissioner's website.

- the commission of any offence or criminal records

Sensitive personal data must be collected using an opt-in and should be carefully handled. Additional security measures may be necessary to protect sensitive personal data.

3.5 The **Data Controller** is 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.

3.6 The **Data Processor** means any person (other than an employee[2] of the data controller) who processes the data on behalf of the data controller.

3.7 The **Data Subject** is the living individual who is the subject of the personal information.

## 4. Data Protection Principles

The DPA sets out eight principles by which personal data must be processed. CHS must ensure that data is:

1. fairly and lawfully processed
2. processed for stated purposes
3. adequate, relevant and not excessive to the stated purposes
4. accurate and, where necessary, kept up to date
5. not kept longer than necessary
6. processed in accordance with the individual's rights
7. secure and safe from accidental loss, damage or destruction, and
8. not transferred to countries outside the European Economic Area unless there is adequate protection for the rights of the individual.

### 4.1 Principle 1 - Personal data shall be processed fairly and lawfully

In practice, the first principle means that CHS, ASTs, Clerks and panel members 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 privacy notices when collecting their personal data
- handle personal data only in ways individuals would reasonably expect
- make sure we do not do anything unlawful with the data

[2] In CHS' case, this also includes panel and AST members.

### 4.1.1 Conditions for processing

Processing means collecting, recording, using, disclosing, retaining 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 Schedule 2 and Schedule 3 of the DPA. The conditions for processing are more exacting when sensitive personal data is involved.

### 4.1.2 Privacy notices

When personal data is collected about individuals, they should be told exactly how that information is to be used. This is called a privacy notice. The notice should tell them:

- our identity
- the reasons (purposes) for which we intend to process the information
- who the information might be shared with (and what they will use the data for)
- how we will ensure that the information is kept securely
- how long we will keep the information for
- whether collection of the information is optional or mandatory and what the consequences might be of not collecting the information
- how they can access the information
- if the information is to be transferred overseas
- who they can contact for more info or to make a complaint
- how they can make a complaint with the ICO

If individuals are informed at the outset what their information will be used for, they will be able to make an informed decision about whether or not to provide their personal data.

CHS publishes a privacy notice on our website informing data subjects how we will use their personal information. It will be necessary to actively communicate this notice if we process an individual's personal data in a way that may be unexpected or in a different way from which it was originally collected. We will also actively communicate the notice when collecting sensitive personal data.

When making privacy notices available, the same medium will 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 privacy 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 (i.e. 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 such a request they must alert CHS at information@chs.gsi.gov.uk or 0131 244 3614.

### 4.1.4 Information Sharing

CHS will produce Data Processing Contracts, Information Sharing Protocols and Data Access Agreements where necessary in order to ensure the secure and lawful transfer of information between parties.

### 4.1.5 Privacy Impact Assessments (PIAs)

CHS will conduct PIAs prior to initiating a project which will involve the collection/use of personal data, in order to assess the privacy risks to individuals.

## 4.2 Principle 2 - Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

In practice, the second principle means that CHS, ASTs, Clerks and panel members must:

- be clear from the outset about why we are collecting personal data and what we intend to do with it
- comply with the DPA's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data
- comply with what the DPA says about notifying the Information Commissioner
- ensure that if we wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair

### 4.2.1 Notification

CHS must provide an annual notification to the Information Commissioner, summarising the purposes for which personal data is used by the organisation. Failure to submit the annual notification or to keep it up to date is a criminal offence. The notification covers processing undertaken by CHS (or on our behalf by Clerks), ASTs and panel members. CHS is responsible for submitting this notification.

### 4.2.2 Incompatible re-use of information

CHS will 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.

### 4.2.3 CCTV

Personal data in the form of images is collected by CCTV cameras in operation at the entrances to Ladywell House and in the car park. These cameras are owned by National Records of Scotland and the images are monitored by the Scottish Government. The images are held in line with Scottish Government policies and procedures.

## 4.3 Principle 3 - Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

In practice, the third principle means that CHS, ASTs, Clerks and panel members should:

- only hold personal data about an individual that is sufficient for the purpose we are holding it for in relation to that individual
- not hold more information than we need for that purpose

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

## 4.4 Principle 4 - Personal data shall be accurate and, where necessary, kept up to date

In practice, the fourth principle means that CHS, ASTs, Clerks and panel members 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 information
- consider whether it is necessary to update the information

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

Each Information Asset Owner will undertake a regular audit of their information asset to ensure that it is accurate and up to date.

#### 4.4.1 Panel Pal database

It is the responsibility of each panel member to ensure that their name, contact details, availability and certain training information are accurate and up to date. They may update their own record or notify CHS of any changes, and we will update their record on their behalf.

CHS and ASTs are responsible for ensuring that the remaining record is accurate and up to date. The Panel Database Administrator will undertake regular audits of the panel member database.

For the purposes of communications with panel and AST members, contact details must be downloaded from the relevant database on the day of the communication. Out of date contact lists must not be used.

### 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, the fifth principle means that CHS, ASTs, Clerks and panel members must:

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

CHS staff, AST members, Clerks and panel members 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 accordance with the rights of data subjects

This is the sixth principle, and the rights of individuals that it refers to are:

- a right of access to a copy of the information comprised in their personal data
- a right to object to processing that is likely to cause or is causing damage or distress
- a right to prevent processing for direct marketing
- a right to object to decisions being taken by automated means
- a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed

- a right to claim compensation for damages caused by a breach of the Act.

### 4.6.1 Subject Access

Individuals have a right to request any personal data held by CHS in whatever form. CHS has a procedure to deal with requests for access to information (known as Subject Access Requests - SARs). SARs will be handled by CHS centrally. If a SAR is received by an AST or by the Clerk's office, CHS should be notified by email at information@chs.gsi.gov.uk within 2 working days.

SARs will be acknowledged by CHS within 2 working days of receipt by CHS (a request for proof of identification can be made at this time). The SAR will be responded to within 40 calendar days of receipt of the request/identification. If any delays occur, CHS will write to the data subject explaining the reason.

CHS can charge a fee of £10 for each occasion that access is requested.

## 4.7 Principle 7 - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

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

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

### 4.7.1 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 information.
- CHS highlights information risks on its strategic risk register which is considered by the Audit and Risk Management 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 staff and volunteers must undergo mandatory data protection training and complete refresher training on a regular basis.

- CHS staff and volunteers must read, understand and comply with this policy and accompanying policies, procedures and guidance for managing information.
- Personal information must not disclosed, accidentally or otherwise to any unauthorised third party.

Physical security:

- 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 office shredding bin and a member of CHS or NRS staff must witness paperwork being shredded.
- CHS operates a clear desk policy.
- Personal information in the form of manual records must be kept in a locked filing cabinet, drawer or other secure area.
- Personal information must not be taken out of the CHS office in the form of hard copy.

IT Security:

- IT equipment must be disposed of in a secure manner in line with CHS guidance.
- Access to sensitive personal data is provided extra protection by controlled access.
- Personal information in the form of computerised records will be kept on a secure IT system which is password protected.
- Personal information 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 (ctrl alt del) when away from their desks.
- CHS staff must lock their laptops to their docking station when in the office.
- Mobile phones must be locked with a PIN/password.

### 4.7.2 Data Processors

Where CHS uses a contractor to process personal data on its behalf, the contractor must sign a Data Processing Contract which ensures that they are taking adequate steps to comply with Principle 7 (and all other DPA requirements) on CHS' behalf. CHS retains legal responsibility for the actions of processors, and so those managing contracts must ensure that all security procedures necessary are specified in the contract, and it is subsequently monitored to ensure that they are in place.

## 4.8 Principle 8 - Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

Any member of CHS staff, AST member, Clerk or panel member who is required to send personal identifiable information in any format to countries outside the EEA, must discuss this with CHS as the levels of protection for the information may not be as comprehensive as those in the UK.

# 5. Roles and responsibilities

## 5.1 CHS staff and Board members

- The Chief Executive Officer (CEO) has overall responsibility for data protection and information security. The CEO is responsible for ensuring that AST and panel members processing personal data receive the appropriate level of training to support the implementation of this policy. The CEO is also responsible for ensuring that all collection and processing of personal data complies with the DPA and its principles.

- The Director of Finance and Corporate Services 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 staff, Board members, Clerks, AST and panel members, familiarise themselves with the content of this policy.

- The implementation of this policy is delegated to the Data Protection Officer(s) (DPOs). The DPOs are responsible for identifying and publicising data protection responsibilities across the CHS community.

- Staff and Board members are responsible for ensuring that they are familiar with and comply with this policy.

## 5.2 Area Conveners

- Area Conveners are responsible for raising awareness of data protection responsibilities at a local level and highlighting any data protection issues or concerns to CHS at information@chs.gsi.gov.uk. 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 CHS. They are also expected to support CHS in the investigation of any breaches of the policy or the DPA and to disseminate key IG messages at local AST events and meetings.

## 5.3 Area Support Team members

- All AST members processing personal data are responsible for ensuring that they are familiar with and comply with this policy and other guidance issued by CHS. AST members are expected to assist their Area Convener in raising awareness of the importance of data protection and keeping information safe. Data protection training will be provided to AST members through an eLearning package, to be completed annually.

### 5.4 Clerks to the AST

- Clerks and their teams provide support to AST members and panel members at local level. This support arrangement is governed by the Partnership Agreements between local authorities and CHS.

- CHS has put in place Data Processing Contracts to govern the processing of personal data by local authorities on behalf of CHS.

### 5.4 Panel members

- Data protection training will be delivered by the national training provider at pre-service stage and on a refresher basis through an eLearning package. All panel members will be required to complete the eLearning training on an annual basis.

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

## 6. Breaches of this policy

6.1 All personal data recorded in any format must be handled securely and appropriately in line with the DPA. CHS staff and Board members, panel and AST member, and Clerks must not disclose information for any purpose outside their normal role.

6.2 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 CEO will investigate (or appoint a member of staff to investigate) any breaches of this policy by an AST or panel member. A breach of this policy by a Clerk or a member of their team will be handled in line with the terms of the Data Processing Contract.

## 7. Monitoring and Review

7.1 This policy will be reviewed every two years or as appropriate to take into account changes to legislation that may occur, and/or guidance from the Scottish Government and/or the UK Information Commissioner.

**Document Control**

| | |
|---|---|
| **Title** | Data Protection Policy |
| **Author** | Sara Brodie and Ava Wieclawska, August 2014 |
| **Approved by** | CHS Board |
| **Date of approval** | 26 August 2014 |
| **Version number** | 2.0 |
| **Review frequency** | Every two years |
| **Next review date** | August 2016 |

**Status Control**

| Version | Date | Status | Author | Amendments to policy | Approved by |
|---|---|---|---|---|---|
| 0.1 | 13/03/2013 | Draft | Sara Brodie | N/A | SMT |
| 1.0 | 20/03/2013 | Final | Sara Brodie | N/A | CHS Board |
| 1.1 | 10/12/2013 | Draft | Sara Brodie | 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.<br>New sections: 7.9-7.11 and 10.3.<br>Changes to sections at 8.7.1. | SMT |
| 1.2 | 20/02/2014 | Draft | Ava Wieclawska | 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.<br>New footnote at 5.6 and amendment to timescales at 8.6.1. | |
| 1.3 | 02/06/2014 | Draft | Ava Wieclawska | Review period extended from 6 months to 2 years. Restructuring throughout. | |
| 1.4 | 23/07/2014 | Draft | Ava Wieclawska | 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. | |
| 1.5 | 19/08/2014 | Draft | Ava Wieclawska | Reviewed by the Audit and Risk management Committee (ARMC) – changes made to section 5 to clarify roles and responsibilities. | ARMC |
| 2.0 | 26/08/2014 | Final | Ava Wieclawska | Final policy approved by the CHS Board. | CHS Board |