Privacy statement for staff

This privacy notice tells you what Children's Hearing Scotland (CHS) does with the personal data that you provide. This notice is for the information of staff employed directly by CHS. If you are a volunteer, or a member of the public, further information can be found on the CHS website and CHIRP. If you are a secondee, please refer to your original employer's privacy statement. If you are currently employed through an agency, please refer to the agency's privacy notice.

Some key phrases

Personal Data: this is any piece of data that either by itself or when taken with another piece of data makes you identifiable. It can be in any format.

Data Controller: this is the organisation or authority that takes ultimate responsibility for the data you provide. They can ask other parties to help process it, but they are responsible for ensuring that it is securely and properly managed.

Data Processor: this is any third party or agency that is brought in to process data on behalf of the Data Controller.

Data Subject: this is you, the person that the data is about.

1. Who is the Data Controller?

Children's Hearing Scotland (CHS) is the Data Controller for the data we hold about you. This means that once you have provided us with the information listed in the next section, CHS is ultimately responsible for ensuring its security, who sees it, where it goes, and when (and how) it is destroyed. Where you see "we," or "us," it refers to CHS as the Data Controller. You can find more information on how to contact us in Section 7.

2. What information do we collect from you?

Personal data refers to any piece of information about you which makes you identifiable. It can be in any format, digital or paper, and for details on how we store your data, please see sections 5 and 6

Employment

Before you start working with us, you will be asked to provide the following types of personal data:

- Name
- Contact information (postal and email addresses, phone numbers)
- Education history (including relevant certificates or transcripts
- Details of family circumstances (next of kin, their contact information)
- Employment history
- Financial details (bank account information for salary payment)
- A recent image or 'selfie,' along with any audio visual materials produced in the course of your employment
- Criminal history
- Gender

Whilst you are employed at CHS, you are expected to keep this information up to date. If you spot an inaccuracy, or cannot update the information yourself, please see section 7.

Special Categories of data

We also gather more sensitive types of information on staff. These types are called Special Categories of data, and may include:

- Race and ethnic origin
- Religion
- Sexual orientation
- Physical health
- Mental health
- Trade Union membership
- Biometric data

When you are asked to provide this data, it will be made clear whether it is a requirement or an optional question. Where you provide these pieces of information, additional safety measures are put in place to protect them.

Where information is provided in a digital format, it is stored on CHS' own IT systems. When information is provided in a paper format, it will be digitised (scanned), and moved onto our systems. We do not hold paper documentation for long periods of time and once they have been digitised, they are destroyed in an appropriate manner. Where information is held by anyone other than CHS, such as partners or IT providers, we have contracts in place to ensure that they store all information in a secure manner that meets our very high standards.

More information on how long we hold your information, and how we dispose of our records, can be found in Section 5.

3. Why do we collect this data, and what do we do with it?

As an employer, and as a Public Authority, CHS is required by law to maintain certain data and report on other types. Here we list the different reasons we have for collecting your data. These are called our 'legal bases for processing', and these are clarified in the speech bubbles below. We are required to tell you this; you do not need to remember it. They are simply for your reference.

We use it for administrative and financial management purposes

Q: What is our legal basis?

A: We need to process your personal data to fulfil the contract you have entered into with us.

We process your data:

- To meet our contractual obligations to you that are laid out in your contract
- To enrol you on our systems (including HR management and pension providers)
- To provide you with access to IT systems, training programmes, archives, and other services, as per the requirements of your specific role
- To administer financial rewards and remuneration

We use it to meet our duty of care to you and our legal obligations

We process your data:

- To meet our legal duty of care to you under health and safety and safeguarding laws
- To provide health services
- To protect your vital interests or someone else's (e.g. in a medical emergency)
- To comply with our statutory obligations (e.g. immigration and right to work laws)
- To comply with our obligations under the UK Equality Act (2010)

Q: What is our legal basis?

A: We will process your data when it is necessary to comply with a legal obligation, protect vital interests in an emergency, exercise or defend legal claims or comply with court judgements, provide medical and health services, or protect public health.

We gather sensitive data from you, which is held in strictest confidence. It is only disclosed to agencies with a statutory duty to collect it. You are not required to disclose this information to us.

If you disclose that you have a disability, we have a duty to disclose this information on a need-to-know basis to ensure reasonable adjustments are considered to enable you to work without barriers.

We use it for public safety and the prevention and detection of crime

Q: What is our legal basis?

A: We need to process your data where it is necessary for the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against and the prevention of threats to public security.

We process your data:

- To apply welfare, security and other measures where they are necessary for the safety and security of staff members and the wider public under health and safety and other relevant laws (e.g. you will be issued with a photo ID for entry into secured office spaces)
- To comply with court ordered actions involving the police (e.g. a search warrant)
- When it is necessary for IT monitoring purposes

We use it to promote our activities:

We will process your data:

- To produce marketing materials that promote the function and services provided by CHS, this is most likely to involve the use of audio visual images.

- When this is the case, you will be informed that filming/photography/recording is taking place, and where possible your consent will be gathered

Q: what is our legal basis?

A: Where we have your consent and/or where necessary for archiving purposes in the public interest.

Sometimes we use it for research and archiving:

Q: What is our legal basis?

A: We will process your data when it is necessary for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes.

We will process your data:

- To retain any promotional materials that include data, such as images of staff
- To keep a record of your period of employment with us
- To support research on CHS and the Children's Hearing System
- To produce management and statistical information to monitor and improve our performance and service provision to you

4. Who do we share this information with?

In order to meet our obligations to you we will, from time to time, share your information with selected partners. We will only share your data when there is a legal requirement to do so, and all partners and processing agencies are carefully vetted to ensure that they are GDPR-compliant as well. Where possible, we sign *Data Processor Agreements* with them that carefully spell out what data will be shared, for what purpose and for how long. These agreements hold our partners to a very high standard, and are used to ensure that they process your data securely, and only for the purposes that we have requested.

When we share your data you will be informed, and where possible we will seek your consent to share it. This is not always possible though.

Example: If you have a serious accident at work that leaves you unable to communicate, we would be required to share your data with the emergency services. We do not get your consent to do this, but are allowed to by law, as it is considered to be in your vital interest (life or death).

We share your information with IT and Communications service providers. This is to enable them to provide IT and communications systems for CHS.

CHS uses Microsoft Office 365 to provide the CHIRP services. This is because Microsoft complies with the Privacy Shield framework, a certification programme that ensures that participants based in the United States (and all of their subsidiary and partner businesses) are following UK and EU regulations when it comes to the security of personal data.

We share your information with National and Local Government agencies and partners. This is to ensure security measures are in place, and that you are able to fulfil the requirements of your contract.

CHS provides your personal data to the Scottish Government IT team to assign you a secure email address and allow you access to the required systems. We will also give your information to Disclosure Scotland, to allow them to check that you are allowed to work with children, young people, and vulnerable groups. The Scottish Children's Reporters Administration (SCRA) requires access to some of your data to provide HR and payroll services and support. We also share your information with our selected pension provider, but you can 'opt-out'.

We share your information with training providers when necessary. This is to make sure that you have adequate training materials, practice opportunities and support.

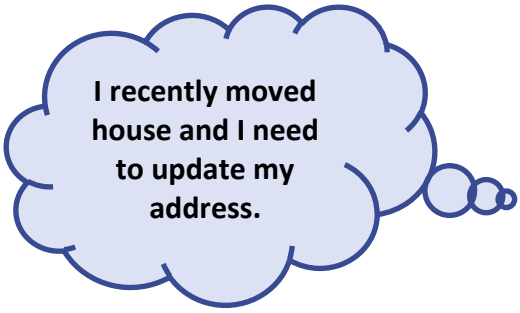
5. How long do we keep hold of your information?

We only keep information for as long as it is needed. For the majority of your data, this means that we destroy it after a specific period of time. There are some pieces of information that we must keep permanently, for either business continuity or historical value.

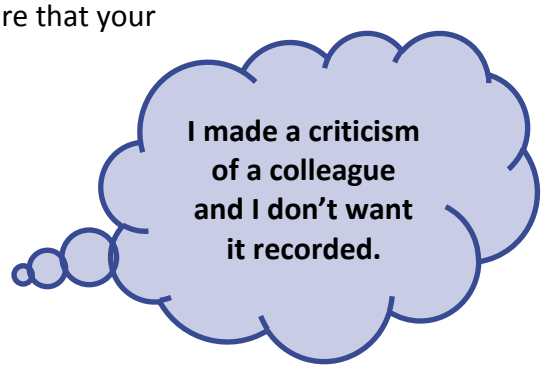
CHS operates a *Retention and Disposal Schedule* that shows exactly how long we can keep different types of information. This document also explains how we destroy different types of information, and the reason for processing the information in this way. To read this, please click here.

6. Your rights

Under the law you, as the *Data Subject*, have rights that can be exercised at any time in relation to your personal data:

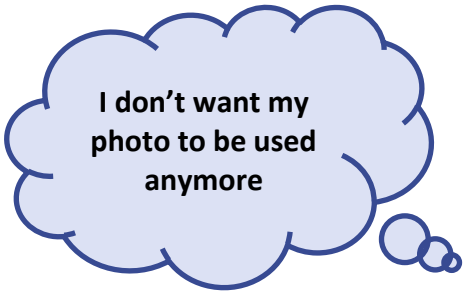


You have the right to request that the *Data Controller* rectifies any inaccuracies in the data held about you. If you change banks, for example, CHS is required to ensure that your information is kept up to date.



You have the right to request the erasure of your data. This is more commonly known as *'the right to be forgotten'*. For example, you may wish to have an email exchange you were involved in removed, or ask to be removed from a mailing list.

***NOTE:** due to our statutory obligations listed above, it is not always possible to completely erase an individual's data. Where this is the case, you will be informed as soon as possible.*



You have the right to request the restriction of processing of your data for a given purpose, or to object to the process taking place altogether. For example, if you do not wish to have your data included in equality monitoring reports, or wish to have a quote attributed to you on the CHS website removed.

You do not need to quote your rights, or any part of the legislation, to enact them. To make sure that your request is processed properly, or to find out more you should contact the *Data Protection Officer*, whose details are listed below. You can also contact the representative of the Data Controller- the Chief Executive of CHS.

Data Protection Officer:

Information Governance Team
information@chs.gsi.gov.uk
T: (0131) 244 3614
Area 2/1/1 Ladywell House
Ladywell Road
Edinburgh
EH12 7TB

Representative of the Data Controller:

Boyd McAdam
National Convenor and Chief Executive
Boyd.mcadam@chs.gsi.gov.uk
T: 0131 244 3698
Area 2/1/1 Ladywell House
Ladywell Road
Edinburgh
EH12 7TB

Information Commissioner's Office:
If you feel that CHS has mishandled your information to an extent that cannot be adequately investigated or resolved 'in house' you can always contact the Information Commissioner directly.

To report the organisation, or register a concern about how your data has been managed, you can use the ICO's web forms: https://ico.org.uk/concerns/

For advice on data protection and your rights, you can send all queries to:
Information Access Team
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Or email them at: accessinformation@ico.org.uk