

Data Protection Policy

of the Community of the Holy Name (CHN)

Introduction

This document outlines the data protection policy of The U.K. Province of the Community of the Mission Sisters of the Holy Name of Jesus (CHN). It sets out a framework for the type of personal data we collect, why we keep it and how we store and use it.

CHN needs to collect and use certain types of information about the Individuals or Service Users who come into contact with CHN in order to carry on our work. This personal information must be collected and dealt with appropriately whether it is collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this under the Data Protection Act 2018.

2. Data Controller

CHN is the Data Controller under the Act, which means that it determines what purposes personal information held, will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

3. Disclosure

CHN may share data with other agencies such as the local authority and other voluntary agencies.

The Individual/Service User will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows CHN to disclose data (including sensitive data) without the data subject's consent.

These are:

- Carrying out a legal duty or as authorised by the Secretary of State;
- Protecting vital interests of a Individual/Service User or other person;
- The Individual/Service User has already made the information public;
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights;
- Monitoring for equal opportunities purposes – i.e. race, disability or religion; or
- Providing a confidential service where the Individual/Service User's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Individuals/Service Users to provide consent signatures.

CHN regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

CHN intends to ensure that personal information is treated lawfully and correctly.

To this end, CHN will adhere to the Principles of Data Protection, as detailed in the Data Protection Act 2018.

Specifically, the principles require that personal information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

CHN will, through appropriate management and strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information;
- Meet its legal obligations to specify the purposes for which information is used;
- Collect and process appropriate information, and only to the extent that it is needed to fulfill its operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:
 - The right to be informed that processing is being undertaken;
 - The right of access to one's personal information;
 - The right to prevent processing in certain circumstances; and
 - The right to correct, rectify, block or erase information which is regarded as wrong information.
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information;
- Set out clear procedures for responding to requests for information.

4. Data collection

Informed consent is when

- An Individual/Service User clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data,
- And then gives their consent.

CHN will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, CHN will ensure that the Individual/Service User:

- Clearly understands why the information is needed;
- Understands what it will be used for and what the consequences are should the Individual/Service User decide not to give consent to processing;
- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed;
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress; and
- Has received sufficient information on why their data is needed and how it will be used.

5. Data Storage

Information and records relating to service users will be stored securely and will only be accessible to authorised CHN Sisters, staff and volunteers.

Information will be stored for only as long as it is needed or is required by statute and will be disposed of appropriately.

It is CHN's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

Note

Some personal data especially relating to staff and volunteers is now being kept for lengthy periods in order to comply with Safeguarding requirements and conditions applied by insurance providers.

6. Data access and accuracy

All Individuals/Service Users have the right to access the information CHN holds about them. CHN will also take reasonable steps to ensure that this information is kept up to date by asking data subjects whether there have been any changes. In addition, CHN will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection;
- Everyone processing personal information understands that they are contractually responsible for following good data protection practice;
- Everyone processing personal information is appropriately trained to do so;
- Everyone processing personal information is appropriately supervised;
- Anybody wanting to make enquiries about handling personal information knows what to do;
- It deals promptly and courteously with any enquiries about handling personal information;
- It describes clearly how it handles personal information;
- It will regularly review and audit the ways it holds, manages and uses personal information;
- It regularly assesses and evaluates its methods and performance in relation to handling personal information; and
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them.

7. Other documents relating to this policy

Other documents relating to this policy include:

- Safeguarding policy of the Community of the Holy Name
- Volunteering policy of the Community of the Holy Name
- CHN data mini-audit 2017

8. Communication

This policy will be communicated generally and to those whose personal data is collected, stored and used.

In case of any queries or questions in relation to this policy please contact the CHN Data Protection Officer who is:

Sister Bursar CHN, Quarry Bank, Woodfield Lane, HESSLE, East Yorkshire, HU13 0ES, or bursarsofficechn@gmail.com

9. Review

This policy will be reviewed every three years and updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 2018.

Signed
on behalf of the Trustees

Adopted on:

Review date:

APPENDIX 1: Glossary of Terms

Data Controller – The person who (either alone or with others) decides what personal information CHN will hold and how it will be held or used.

Data Protection Act 2018 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person(s) responsible for ensuring that CHN follows its data protection policy and complies with the Data Protection Act 2018.

Individual/Service User – The person whose personal information is being held or processed by CHN for example: a visitor, an employee, a volunteer or a member of the Fellowship of the Holy Name.

Explicit consent – is a freely given, specific and informed agreement by an Individual/Service User in the processing of personal information about her/him. Explicit consent is needed for processing sensitive data.

Notification – Notifying the Information Commissioner about the data processing activities of CHN, as certain activities may be exempt from notification.

The link below is to the ICO website where a self assessment guide will help you to decide if you are exempt from notification: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/>

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 2018.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees within CHN.

Sensitive data – refers to data about:

- Racial or ethnic origin
- Political affiliations
- Religion or similar beliefs
- Trade union membership
- Physical or mental health
- Sexuality
- Criminal record or proceedings