General Data Protection Regulation (GDPR), Policy and Procedure

1. Introduction

Community ConneX – formerly Harrow Mencap – as part of its business activities needs to gather and use certain information about individuals. These can include people we support and their families, employees, volunteers, trustees, contractors, partners and other people the organization has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the organisation's data protection standards – and comply with the GDPR law.

Community ConneX is fully committed to compliance with the requirements of the Data Protection Act 1998 ("the Act"). The organisation will therefore follow procedures that aim to ensure that all employees, trustees, contractors, volunteers, or consultants, who have access to any personal data (held about employees, trustees, volunteers, or people we support and their families) are fully aware of and abide by their duties and responsibilities under the Act.

2. Purpose

This data protection policy ensures Community ConneX:

- Complies with data protection law and follows good practice
- Protects the rights of clients, their families, staff and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of data breach.

3. Data protection risks

This policy helps to protect the organisation from some very real data security risks, including:

- Breaches of confidentiality – for instance, information being given out inappropriately
- Failing to offer choice – For instance, all individuals should be free to choose how the organization uses data relating to them

- Reputational damage – For instance, the company could suffer if hackers successfully gained access to sensitive data.

Everyone who works for or with the organisation (both staff, volunteers and contractors) has responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

4. Ancillary Supporting Policies, Procedure and Templates To ensure that our data protection policy is fully compliant with GDPR standards, there are other specific policies, procedures and templates that are designed to support Community ConneX's overarching GDPR policy. It is advised that these policies and procedures be read in full and for specific understanding of our data protection framework. The list includes the following:

Y:\HM Policies & Procedures NEW\GDPR\Approved Policies

a) Access Control Password Policy
b) Clear Desk Policy
c) Outsourcing Policy
d) Processor Notification Policy
e) Risk Management Policy and Procedure
f) Privacy Notice for Websites

Y:\HM Policies & Procedures NEW\GDPR\Approved Templates

a) Privacy Notice Template
b) Processor Agreement Template
c) Data Breach Incident Form
d) Subject Access Response Template
e) Outsourced Functions Register
f) Risk Management Corrective Action Plan
g) Staff GDPR acknowledgement Template

5. Definitions Terms

Charity	means Community ConneX, a registered charity.
GDPR	means the General Data Protection Regulation.
Responsible Person	means (Henry Anaele) the person responsible for data protection within the Charity].
Register of Systems	means a register of all systems or contexts in which personal data is processed by the Charity.
Data Protection Act 1998	The UK legislation that provides a framework for responsible behaviour by those using personal information.
Data Subject/Service User	The individual whose personal information is being held or processed by [Group] (for example: a service user or a supporter)
Explicit' consent	is a freely given, specific and informed agreement by a Data Subject (see definition) to the processing of personal information about her/him. Explicit consent is needed for processing sensitive data this includes the following: racial or ethnic origin of the data subject; political opinions; religious beliefs or other beliefs of a similar nature; trade union membership; physical or mental health or condition; sexual orientation; criminal record; proceedings for any offence committed or alleged to have been committed
Information Commissioner	The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.
Personal Information	Information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers of the Group

6. Data protection principles

The Charity is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. 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;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f. 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."

7. General provisions

a. This policy applies to all personal data processed by the Charity.
b. The Responsible Person shall take responsibility for the Charity's ongoing compliance with this policy.

c. This policy shall be reviewed at least annually.
d. The Charity shall register with the Information Commissioner's Office as an organisation that processes personal data.

8. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Charity shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to the charity shall be dealt with in a timely manner.

9. Lawful purposes

a. All data processed by the charity must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
b. The Charity shall note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Charity's systems.

10. Data minimisation

a. The Charity shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
b. Any other considerations relevant to the Charity's particular systems.

11. Accuracy

a. The Charity shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.
c. Any other considerations relevant to the Charity's particular systems

12. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the Charity shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why.

13. Security

a. The Charity shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

14. Handling of personal/sensitive information

Community ConneX will, through appropriate management and the use of strict criteria and controls: -

- Observe fully conditions regarding the fair collection and use of personal information;
- Meet its legal obligations to specify the purpose for which information is used;
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;

- Ensure that the rights of people about whom the 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 within the statutory 40 days The right to prevent processing in certain circumstances;
  - the right to correct, rectify, block or erase information regarded as wrong information.

In addition, Community ConneX will ensure that:

- There is someone with specific responsibility for data protection in the organisation;
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
- Queries about handling personal information are promptly and courteously dealt with;
- Methods of handling personal information are regularly assessed and evaluated;
- Performance with handling personal information is regularly assessed and evaluated;
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All trustees, employees, and volunteers are to be made fully aware of this policy and of their duties and responsibilities under the Act.

All of the above will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:-

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;

- Individual passwords should be such that they are not easily compromised.

15. Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Head of Group Services.

- When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it.
- These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:
- When not required, the paper or files should be kept in a locked drawer or filing cabinet
- Employees should make sure paper and printouts are not left where unauthorized people could see them, like on a printer
- Data printouts should be shredded and disposed of securely when no longer required.

16. Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. Community ConneX is registered as such. The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on

an annual basis. Failure to do so is a criminal offence. It is the Chief Executive's responsibility to ensure the timely renewal.

17. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Charity shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

Policy reviewed	February 2010 February 2013 February 2016 April 2019
Next review date	April 2022
Name or position of person responsible for this policy	Head of Group Services