**Privacy Policy**

**1. Introduction**

To be able to provide the support to clients, members, employ staff and carry out the finance functions Community First Yorkshire holds a wide range of data about individuals. Since it relates to identifiable individuals all of the activities using this data fall under the General Data Protection Regulations. The GDPR applies to personal data in computerised, manual or any other format, as long as the data is in a system that allows the information to be readily accessible. Community First Yorkshire has processes, documentation and records which are designed to ensure that it complies with the regulations and has set up the procedures set out in this policy and procedure in order to meet the requirements of the Act and accompanying employment practices code. CFY is registered with the Information Commissioner’s Office as an organisation that processes personal data.

This policy sets out the procedures, processes, policies and documents that Community First Yorkshire has in place to meet the principles of GDPR.

Overall responsibility for Data Protection rests with the Community First Yorkshire Board of Trustees and Community First Yorkshire has a member of staff with the responsibility of data protection officer who is in charge of all aspects of information, including the GDPR and FOI Act (Freedom of Information). Their duties include in accordance with Community First Yorkshire Policies:

* + - Auditing information systems to find out who holds what data, and why.
		- Providing guidelines for managers about how to gather, store and retrieve data.
		- Ensuring that all information collected complies with the GDPR Act 2018.
		- Checking the security of information stored.
		- Reviewing practice in respect of references.
		- Reviewing the private use of telephones, email and post.

**2. Procedures**

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

* Processed lawfully, fairly and in a transparent manner in relation to individuals;
* 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;
* Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
* 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;
* Kept in a form which permits identification of data subjects for no longer than is necessary for the purposed for which the personal data are processed; persona 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
* 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.

**3. Privacy Notices**

Community First Yorkshire has privacy notices for each project or service. The notices explain the reasons for processing individual data, how it is used, the legal basis for processing, if it will be transferred or shared, how it is stored, archived and how long it will be kept before being destroyed.

Privacy Notices are available on our website.

**4. Lawful and Transparent processing/ Record of processing activities**

To ensure its processing of data is lawful, fair and transparent Community First Yorkshire will maintain a Data Audit System/register of data processing activities for each project or service /department. This will identify the following:

* Types of data processes
* Personal data processed
* Purpose
* Lawful basis for processing
* Consent for processing (if required) and how obtained
* How data is processed and stored
* Security measures and access
* Retention periods

This will be reviewed annually.

All data processed by CFY must be done on one of the following lawful bases:

* Consent
* Contract
* Legal Obligation
* Vital interests
* Public Task
* Legitimate Interest

Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept.

Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent will be clearly available and systems in place to ensure such revocation is reflected accurately in CFY’s systems.

**5. Individual Rights**

Individuals have the right to access their personal data. These rights are:

* Right to be informed
* Right to access of data
* Right to the rectification of any inaccurate data
* Right to the erasure or stop processing of the data
* Right to the restriction of processing
* Right to object
* Right to data portability
* Right to automated decision making including profiling

Any individual wishing to make a Subject Access Request should contact the Data Processor at Community First Yorkshire. Any such requests will be dealt with in a timely manner within 1 month from the date of the request. CFY has the right to extend on notice to 2 months if the request is complex. To request a Subject Access Request form please emailing info@communityfirstyorkshire.org.uk

The data provided will be in a secure electronic format unless agreed otherwise. Identity checks will be conducted on the individual requesting the information before the data is provided.

Should any request be unfounded or excessive, CFY is not required to comply and may choose to request a fee to cover administration costs and we will inform the individual of this decision.

**6. Data Security**

Community First Yorkshire will ensure that personal data is stored securely using modern software that is kept up to date with back up and disaster recovery solutions in place.

Where you data is stored in paper format we have secure storage and processes for this.

Access to personal data is limited to personnel who need access and employees are responsible for protecting their passwords and maintaining confidentiality and security of data they are processing as part of their job.

When personal data is deleted this is done to such an extent that the data is irrecoverable.

**7. Breach of security**

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to and individuals personal data, CFY will access the risk to the individuals rights and freedoms and if appropriate report the breach to the ICO promptly.

**8. Data Accuracy**

Community First Yorkshire will take reasonable steps to ensure personal data is accurate and kept up to date. The Data Processor will ensure that regular maintenance and housekeeping processes take place which include archiving, disposal and deletion of data in accordance with the requirements of GDPR and as per Community First Yorkshire’s data retention policy.

The data audit system shows us what data should/must be retained, for how long and why.

**9. Unique Category Data**

Unique data such as criminal records, health conditions, ethnic origin will be processed in accordance with the GDPR requirements for such data.

**10. Responsibilities of Individuals**

Individuals are responsible for notifying CFY of any changes to their personal data in order for CFY to maintain the accuracy of the data held.

Employees or volunteers working for CFY who process or have access to personal data as part of their job are required to follow the procedures in place to meet the requirements of GDPR also:

* To access only data they have authority to access
* To disclose data to only those authorised to receive it
* Keep data secure by protecting passwords, locking away hard copy files, not storing personal data on memory sticks or personal devices.
* Not removing any personal data in any format without adopting appropriate security measures.