Mirfield
Community
Centre
BRINGING THE COMMUNITY TOGETHER

UK GDPR

Policy for compliance with the UK General Data Protection Regulation

Introduction

Lots of data protection policies are unhelpfully long and simply reiterate large portions of the legislation. This policy aims to provide a concise and practical document that can be used as the foundation for a working Data Protection Policy. Any doubts about legal obligations should always be checked with the ICO.

Definitions

Trust	means Mirfield Community Trust, a registered charity.
UK GDPR	means the UK General Data Protection Regulation.
Responsible Person	means Anna Seabourne
Personal Data	means any information relating to an identified or identifiable natural living person. Information concerning a 'legal' rather than a 'natural' person is not personal data. Consequently, information about a limited company or another legal entity, which might have a legal personality separate to its owners or directors, does not constitute personal data and does not fall within the scope of the UK GDPR. Similarly, information about a public authority is not personal data. However, the UK GDPR does apply to personal data relating to individuals acting as sole traders, employees, partners, and company directors wherever they are individually identifiable and the information relates to them as an individual rather than as the representative of a legal person.
Register of Systems	means a register of all systems or contexts in which personal data is processed by the Trust.

1. Data protection principles

The Trust is committed to processing data in accordance with its responsibilities under UK GDPR.

UK 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.”

2. General provisions

a) This policy applies to all personal data processed by the Trust.

b) The Responsible Person shall take responsibility for the Trust’s ongoing compliance with this policy.

c) This policy shall be reviewed at least annually.

d) The Trust shall register with the Information Commissioner’s Office (IOC) as an organisation that processes personal data.

3. Lawful, fair and transparent processing

a) To ensure its processing of data is lawful, fair and transparent, the Trust 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 Trust shall be dealt with in a timely manner.

4. Lawful purposes

a) All data processed by the Trust 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 Trust records 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 Trust’s systems.

5. Data minimisation

a) The Trust 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) User and contractor details will be limited to those needed to contact them . Children details will be limited to those needed for safeguarding reasons.

6. Accuracy

a) The Trust 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) The personal data kept will be regularly checked to make sure the Trust has the relevant data needed to fulfil it's charitable objectives.

7. Archiving / removal

a) To ensure that personal data is kept for no longer than necessary, the Trust has in place an archiving policy for each area in which personal data is processed and reviews this process annually.

b) The archiving policy is that data will be deleted after a defined period of time which for each area in which personal data is processed is as follows:

- Accounting systems – 6 years
- Correspondence – 6 years
- Trustee details – 6 years following termination of appointment
- Employee details – 3 years following termination of employment
- Volunteer details – 3 years following termination of involvement
- Supporter details – on request
- Contractor details – 6 years following last work undertaken

8. Security

α) The Trust shall ensure that personal data is stored securely using modern software that is kept-up-to-date. Where paper records are stored, these will be kept in a locked office in the Trust's premises.

β) 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.

χ) When personal data is deleted this should be done safely such that the data is irrecoverable.

δ) Appropriate back-up and disaster recovery solutions shall be in place.

ε) CCTV use will be in accordance with the Trusts CCTV policy guidelines.

9. 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 Trust shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.

Appendix 1 – Register of Systems

	System/context	Type(s) of data held	Lawful basis for processing
1	Accounting software	Customer and contractor details	Contract
2	Email system	Email correspondence	Legitimate interest
3	Google cloud	Customer and contractor details	Contract
4	Google cloud	Trustee and staff details	Legal obligation
5	Google cloud	Supporter database	Consent
6	Paper files	Trustee details	Legal obligation
7	Paper file	Supporter consent forms	Consent