



Data Protection Policy

Policy statement

MCFT are committed to managing, storing and processing information minimally, securely and in line with the principles of all relevant legislation. All of the below set out the legislative requirements for organisations processing personal data:

- The Data Protection Act 2018 (DPA), which governs how personal information is used by organisations, businesses or the government.
- The UK General Data Protection Regulation (UK GDPR)
- and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)

Policy Scope

MCFT processes personal data relating to potential, existing and previous staff and volunteers, website users, as well as personal data collected for the successful delivery of individual projects, collectively referred to in this policy as data subjects. When processing personal data, MCFT is obliged to fulfil individuals' reasonable expectations of privacy by complying with UK GDPR and other relevant data protection legislation (data protection law).

- This policy applies to all personal data processed by MCFT.
- The Responsible Person shall take responsibility for MCFT's ongoing compliance with this policy. The MCFT manager is the Responsible Person for data management.
- The Data Protection Legislation is overseen and enforced by the Information Commissioner's Office (ICO), who is an independent public body responsible directly to Parliament. MCFT have undertaken the self assessment on the Information Commissioner's Office website and are not required to pay a fee or register at this time. This will be checked each time a review of this policy is undertaken.
- See also MCFT's privacy policies.

Commitments

MCFT undertakes to ensure that personal data will 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 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 DPA in order to safeguard the rights and freedoms of individuals
- 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.

Lawful, fair and transparent processing

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

Lawful purposes

- All data processed by MCFT 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](#)).
- MCFT will note the appropriate lawful basis in the Register of Systems which is a record of all systems or contexts in which personal data is processed by MCFT.
- Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
- 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 MCFT's systems.

Data held will be:

- **Minimised** – MCFT will ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **Accurate** – MCFT will take reasonable steps to ensure personal data are accurate and kept up to date where necessary for the lawful basis on which data are processed, steps shall be put in place to ensure that personal data are kept up to date.
- **Archived / removed** –in accordance with MCFT’s data archiving policy which includes guidance on how long data should be retained and will ensure that personal data is kept for no longer than required

Data Security

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

Data protection breach

- The UK GDPR introduces a duty on all organisations to report certain personal data breaches to the relevant supervisory authority, in this case the Information Commissioner’s Office (ICO). This must be done by the Responsible person within 72 hours of becoming aware of the breach, where feasible.
- 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, MCFT will 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](#)).
- If the breach is likely to result in a high risk of adversely affecting individuals’ rights and freedoms, the individuals will also be informed without undue delay.
- A record is kept by the Responsible person of any personal data breaches, regardless of whether you are required to notify.

MCFT will notify all staff and volunteers that a Data Protection Policy is in place and their responsibilities in regards to this. Staff will received training in managing information and how to manage and report breaches of data protection . Breaches of information must be notified to the Responsible Person; for MCFT this is the MCFT Manager, who will record the breach, determine the level of impact of the breach and whether the individual and/or relevant supervisory authority should be notified.

The MCFT Data Protection and Information Governance policy is fully supported by the Trustees. Our policy will be monitored and reviewed annually to ensure that we continue to meet our obligations under the law and protect such personal data as it is necessary for MCFT to collect in order to carry out its charitable and other activities.

Signed:

A handwritten signature in black ink, appearing to read 'D. Allen', with a long horizontal stroke extending to the right.

Chair of Trustees

Date: 19.7.24

Date approved by Trustees: