

# PRIVACY POLICY

# Introduction

The definition of Data Protection is: the process of safeguarding important information from corruption, compromise or loss. The [Data Protection Act](http://www.legislation.gov.uk/ukpga/1998/29/contents) (1998) controls how personal information is used by organisations, businesses or the government.

Eskdale Mill & Heritage Trust has a legitimate interest in acquiring and storing data and therefore has to follow strict rules called ‘data protection principles’. The Trust must make sure the information it keeps is:

* used fairly and lawfully
* used for limited, specifically stated purposes
* used in a way that is adequate, relevant and not excessive
* accurate
* kept for no longer than is absolutely necessary
* handled according to people’s data protection rights
* kept safe and secure
* not transferred outside the [European Economic Area](https://www.gov.uk/eu-eea) without adequate protection

On the 25th May 2018 new legislation called the General Data Protection Regulation (GDPR) comes into force (and will continue post Brexit) and covers all companies that deal with the data of EU citizens. GDPR is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the [European Union (EU)](https://www.investopedia.com/terms/e/europeanunion.asp). The GDPR sets out the principles for data management and the rights of the individual, while also imposing fines that can be revenue-based on companies who misuse this information.

GDPR has a focus on protecting people and the Trusts relationship with them. As soon as the Trust records any information about any person the following safeguarding procedures must be followed.

# Eskdale Mill & Heritage Trust Data protection principles

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

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

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. 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;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. 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;
5. 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
6. 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.

# General provisions

1. This policy applies to all personal data processed by the Trust.
2. The Responsible Person shall take responsibility for the Trust’s ongoing compliance with this policy.
3. This policy shall be reviewed at least annually.
4. The Trust holds personal data and has carried out an information audit of what personal data it holds, where it comes from and who it is shared with.
5. The Trust is registered with the Information Commissioner’s Office (ICO) as an organisation that processes personal data.

# Lawful, fair and transparent processing

1. To ensure its processing of data is lawful, fair and transparent, the Trust shall ensure data is only collected for legitimate purposes and keep a Register of Systems (appendix 3).
2. The Register of Systems shall be reviewed at least annually.
3. 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. The Trust uses Hotmail for group emailing and hence some data may be held overseas.

# Lawful purposes

1. 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.
2. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept on a password protected excel spreadsheet.
3. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should made to the membership secretary. Once the Trust has been notified of a persons wish to opt-out they will be removed from the database by the Membership Secretary. For verbal communications a record of the conversation must be kept.

# Data minimisation

1. 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.

# Accuracy

1. The Trust shall take reasonable steps to ensure personal data is accurate.
2. 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.
3. The Trusts database will be updated as and when required.

# Archiving / removal

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

# Security

1. The Trust shall ensure that hard copies of personal data is stored securely in a locked filing cabinet and electronic data uses modern software that is kept-up-to-date by our IT services.
2. Access to personal data shall be limited to personnel who need access and appropriate security (passwords) are in place to avoid unauthorised sharing of information.
3. Trust membership secretary has a personal laptop which is moved from place to place. This ‘Data in Transit’ is protected by encrypted passwords on all laptops.
4. When personal data is deleted, hard copies will be shredded and electronic copies deleted in a way such that the data is irrecoverable. The Trust’s back-up systems are automatically deleted after three months.
5. Appropriate back-up and disaster recovery solutions are in place with a daily back up of business data and weekly data back-up stored in a safe.

# 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 within 72 hours. The affected people must also be contacted. All procedures and actions taken must be documented in case of further investigation by the ICO. ([See the ICO website](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/) for examples of a breach of information). Near misses should also be documented and recorded.