ROMSEY MILL

Data Protection Policy Information			
Version Number:	V3.6		
Policy History:	V3.2 - Policy updated and approved 09-2020 V3.3 - Policy updated and approved 10-2022 V3.4 - Policy updated and approved 07-2024 V3.5 – Policy updated and approved by Board of Trustees 07-2025		
Policy update prepared by:	Diane Hicks		
Policy reviewed by:	Operations & Resources Committee		
Policy approved by:	Operations & Resources Committee		
Sections updated:	Introduction; Additional section added – section 14		
Name Signature and Date:	Name: T. P. SMITH	Signed:	Date: 05/08/2026.
Next review date:	July 2027		

DATA PROTECTION POLICY

1. INTRODUCTION

The Data Protection Act 2018 ('DPA 2018') protects the rights of individuals to have their personal data collected and stored securely and used only for legitimate and lawful purposes for which their consent has been sought. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR) which became part of UK law from 25th May 2018.

This policy sets out how Romsey Mill collects, processes and protects personal data in compliance with the UK General Data Protection Regulation (UK GDPR), The Data Protection Act 2018 (DPA) and the Data (Use and Access) Act (DUAA) 2025. Romsey Mill is committed to a policy of protecting the rights and privacy of individuals including employees, programme participants, business contacts, funders, volunteers, and the other people the organisation has a relationship with or may need to contact, in accordance with the General Data Protection Regulation (GDPR). The new regulatory environment demands higher transparency and accountability in how charities manage and use personal data. It also accords new and stronger rights for individuals to understand and control that use.

The GDPR contains provisions that Romsey Mill needs to be aware of as a data controller, including provisions intended to enhance the protection of individual's personal data.

This policy should be read in conjunction with the following policies:

Safeguarding; Data Retention

Romsey Mill needs to collect and process certain information about employees, programme participants, business contacts, funders, supporters, volunteers, and other people the organisation has a relationship with or may need to contact for various purposes such as, but not limited to:

1. The recruitment and payment of staff
2. The recruitment of volunteers
3. The administration of our programmes
4. Programme participants contact and engagement
5. Recording outcomes and evaluations of programme for external funding bodies
6. Collecting fees
7. Donations

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation, Romsey Mill must ensure that all this personal information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully. The reasons for this are to ensure that Romsey Mill:

- Complies with the law and principles of the Data Protection Act 2018, the General Data Protection Regulation and the DUAA 2025.
- Aims to maintain consistently high levels of best practice in processing of personal and/or sensitive data.
- Protects employees, programme participants and other individuals.
- Protects itself as an organisation.
- Is open about how it stores and processes individuals' data.

2. COMPLIANCE

This policy applies to all staff and volunteers of Romsey Mill. Breach of this policy or of the Regulation itself will be considered an offence and Romsey Mill's disciplinary procedures will be invoked.

As a matter of best practice, other agencies and individuals working with Romsey Mill and who have access to personal information will be expected to read and comply with this policy. It is expected that staff who are responsible for dealing with external bodies will take responsibility for ensuring that such bodies sign a contract which will include an agreement to abide by this policy.

This policy will be reviewed annually and updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

3. DEFINITIONS

The following list of definitions of the technical terms we have used is intended to aid understanding of this policy:

Data Controller – The person who (either alone or with others) decides what personal information Romsey Mill will hold and how it will be held or used.

Data Protection Act 2018 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

General Data Protection Regulation – Regulates the processing of personal data and protects the rights and privacy of all living individuals. This legislation provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person(s) responsible for ensuring that Romsey Mill follows its data protection policy and complies with the Data Protection Act 2018 and the General Data Protection Regulation 2016 (GDPR). The responsibility of the Data Protection Officer (DPO) is as follows:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed.

Data Subject – The individual whose personal information is being held or processed by Romsey Mill (for example: a service user, an employee, volunteer, Organisation, Trust or a supporter).

Personal data – means data which relates to a living individual who can be identified –

a) from the data or

b) from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be "personal data". The more expansive definition in the General Data Protection Regulation includes online identifiers and provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

Special categories of personal data (Article 9)

Special categories of personal data under the GDPR relates to:

- Racial or ethnic origin of the data subject
- Political opinions
- Religious or philosophical beliefs
- Trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- Physical or mental health
- Sexual life
- Genetic or biometric data for the purpose of uniquely identifying an individual (e.g. Photos, fingerprints, facial recognition).

Personal data relating to criminal convictions and offences or related security measures based Criminal record can only be processed if there is a lawful basis for doing so (Article 6(1) of GDPR) and the processing is authorised by law providing for appropriate safeguards for the rights and freedoms of data subjects (Article 10)

Personal data that has been pseudonymised – e.g. key coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Consent – is a freely given, specific and informed agreement by a Data Subject to the processing* of personal data* about them. Consent under the GDPR must be freely given, specific, informed and an unambiguous indication of an individual's wishes. There must be some form of clear affirmative action – a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions, and there must be a simple way for people to withdraw consent.

* See definition

Processing – means collecting, amending, handling, storing, or disclosing personal information.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 2018 and the General Data Protection Regulation 2016

4. GENERAL DATA PROTECTION REGULATION

This piece of legislation came into force on the 25th May 2018. The General Data Protection Regulation describes how organisations must collect, handle, and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be in hard or soft copy (paper/manual files; electronic records; photographs; CCTV images) and may include facts or opinions about a person. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR) which became part of UK law from 25th May 2018

5. RESPONSIBILITIES UNDER THE GENERAL DATA PROTECTION REGULATION

Romsey Mill will be the 'data controller' under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of the personal data and determines what purposes personal information held will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

Romsey Mill appoints a Data Protection Officer (DPO), currently the Operations and Resources Manager, who will ensure that any concerns regarding the data held by Romsey Mill including how it is stored, processed, and used are addressed.

The Operations & Resources Manager is responsible for all day-to-day data protection matters, including ensuring that all members of staff, volunteers and relevant individuals abide by this policy, and for developing and encouraging good information handling within Romsey Mill.

The Operations & Resources Manager is also responsible for ensuring that Romsey Mill's notification is kept accurate. Details of Romsey Mill's notification can be found on the Office of the Information Commissioner's Website. Our data registration number is Z714228X.

Compliance with the legislation is the personal responsibility of all individuals within Romsey Mill who process personal information. Individuals who provide personal data to Romsey Mill are responsible for ensuring that the information is accurate and up to date.

Romsey Mill also has a nominated Trustee who oversees this policy and ensures policy reviews are undertaken annually and policy updates are made in-line with changes to legislation and risk factors. The Trustee will also receive compliance reports from the Data Protection Officer when required.

6. DATA PROTECTION PRINCIPLES

Romsey Mill regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal. The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles. Data shall be obtained only for one or more of the purposes specified in the Act and shall not be processed in any manner incompatible with that purpose or those purposes. To this end, Romsey Mill will adhere to the Eight Principles:

1. **Process personal data fairly, lawfully and in a transparent manner**

   Romsey Mill will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

   This means that we must:

   - Have legitimate grounds for collecting and using personal data.
   - Not use the data in ways that have unjustified adverse effects on the individuals concerned.
   - Be transparent about how we intend to use the data and give individuals appropriate privacy notices when collecting their personal data.
   - Handle the personal data of individuals only in ways they would reasonably expect.
   - Make sure we do not do anything unlawful with data.

2. **Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose.**

Romsey Mill will ensure that the reason for which it collected the data originally is the only reason for which it processes that data, unless the individual is informed of any additional processing before it takes place.

3. **Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.**

   Romsey Mill will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this in mind. If any irrelevant data is given by individuals, it will be destroyed immediately.

4. **Keep personal data accurate and, where necessary, up to date.**

   Romsey Mill will review and update all data on a regular basis and at least annually. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify Romsey Mill if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of Romsey Mill to ensure that any notification regarding the change is noted and acted on. Every reasonable step will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.

5. **Only keep personal data for as long as necessary.**

   Romsey Mill undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means Romsey Mill will undertake a regular annual review of the information held and implement a process for deleting and discarding of data.

   Romsey Mill will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste).

6. **Process personal data in accordance with the rights of the data subject under the legislation.**

   Individuals have various rights under the legislation including a right to:

   - Be told the nature of the information Romsey Mill holds and any parties to whom this may be disclosed.
   - Prevent processing likely to cause damage or distress.
   - Prevent processing for purposes of direct marketing.
   - Be informed about the mechanics of any automated decision making process that will significantly affect them.

- Not have significant decisions that will affect them taken solely by automated process.
- Sue for compensation if they suffer damage by any contravention of the legislation.
- Take action to rectify, block, erase or destroy inaccurate data.
- Request that the Office of the Information Commissioner assess whether any provision of the Regulation has been contravened.

Romsey Mill will only process personal data in accordance with individuals' rights.

7. **Put appropriate technical and organisational measures in place against unauthorized or unlawful processing of personal data, and against accidental loss or destruction of data.**

   All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorized third parties.

   Romsey Mill will ensure that all personal data is accessible only to those who have a valid reason for using it.

8. **Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.**

   Romsey Mill will not transfer data to such territories without the explicit consent of the individual. This also applies to publishing information on the internet – because transfer of data can include placing data on a website that can be accessed from outside the EEA – so Romsey Mill will always seek the consent of individuals before placing any personal data (including photographs/videos) on its website.

   If Romsey Mill collects personal data in any form via its website; it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

7. INFORMATION SECURITY

Security is a critical part of keeping information confidential. Romsey Mill takes steps to ensure that all information is held securely both physically and electronically.

Romsey Mill will have in place appropriate security measures e.g. ensuring that hard copy personal data is kept in lockable filing cabinets/cupboards with controlled access (with the keys then held securely in a key cabinet with controlled access):

- Keeping all personal data in a lockable cabinet with key-controlled access.

- Password protecting personal data which is held electronically.
- Archiving personal data which is then kept securely (lockable cabinet).
- Placing any PCs or terminals that show personal data so that they are not visible except to authorised staff.
- Ensure that PC screens are not left unattended without a password protected screen-saver being used.

In addition, Romsey Mill will put in place appropriate measures for the deletion of personal data – manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PC's will be wiped clean before disposal of and if that is not possible destroyed physically. A log will be kept of the records destroyed.

8. DATA COLLECTION

Lawfulness of processing (Article 6(1)):

For processing to be lawful at least one of the following must apply:

a) The data subject has given consent to the processing of his or her personal data for one or more specific purposes.

b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

c) Processing is necessary for compliance with a legal obligation to which the controller is subject.

d) Processing is necessary in order to protect the vital interests of the data subject or of another individual.

e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the subject is a child.

Consent as a basis for processing (Article 7)

Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and

transparent manner. Consent is especially important when Romsey Mill is processing any sensitive data, as defined by the legislation.

Romsey Mill understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

Romsey Mill will ensure that any forms used to gather data on an individual will contain a statement (fair collection statement) explaining the use of that data, how the data may be disclosed and also indicate whether or not the individual needs to consent to the processing.

Romsey Mill will ensure that if the individual does not give consent for the processing, and there is no lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

Informed consent is when:

- A Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data
- and then gives their consent.

Romsey Mill will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, Romsey Mill will ensure that the Data Subject:

- Clearly understands why the information is needed.
- Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing.
- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed.
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress.
- Has received sufficient information on why their data is needed and how it will be used.

9. DATA SHARING

There are two types of data sharing: systematic and exceptional. 'Systematic' means a routine sharing of data or pooling of data. 'Exceptional' is one-off sharing (which might have

to happen in an emergency). When deciding whether to share data, Romsey Mill will consider the following:

- What is the sharing meant to achieve? We will have a clear objective or set of objectives. Being clear about this allows us to work out what data we need to share and who with. Any sharing of information will be documented.
- What information needs to be shared? We will not share all the personal data we hold about someone if only certain data items are needed to achieve our objectives.
- Who requires access to the shared personal data? We employ 'need to know' principles, meaning that other organisations should only have access to data if they need it, and that only relevant staff within those organisations should have access to the data. This will also address any necessary restrictions on onward sharing of data with third parties.
- When should it be shared? Is this an on-going, routine process or should it only take place in response to particular events?
- How should it be shared? This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security.
- How can we check the sharing is achieving its objectives? We will judge whether it is still appropriate and confirm that the safeguards still match the risks.
- What risk does the data sharing pose? For example, is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine individuals' trust in us?
- Could the objective be achieved without sharing the data or by anonymising it?
- Do we need to update our notification?
- Will any of the data be transferred outside of the European Economic Area (EEA)?

Data Sharing Agreements

These will document the following issues:

- The purpose, or purposes, of the sharing.
- The potential recipients or types of recipient and the circumstances in which they will have access.
- The data to be shared.
- Data quality – accuracy, relevance, usability etc.
- Data security.

- Retention of shared data.
- Individuals' rights – procedures for dealing with access requests, queries and complaints.
- Review of effectiveness/termination of the sharing agreement.
- Sanctions for failure to comply with the agreement or breaches by individual staff.
- Common retention and destruction arrangements for the data sent and received will be agreed.

Exceptional data sharing

Romsey Mill complies with statutory guidelines on sharing information including compliance with the Prevent duty under the counter-terrorism and Security Act 2015. Information will be shared with the right people at the right time to:

- Prevent death or serious harm.
- Co-ordinate effective and efficient responses.
- Enable early interventions to prevent the escalation of risk.
- Prevent abuse and harm that may increase the need for care and support.
- Maintain and improve good practice in safeguarding programme participants.
- Reveal patterns of abuse that were previously undetected and that could identify others at risk of abuse.
- Identify low-level concerns that may reveal people at risk of abuse.
- Help people to access the right kind of support to reduce risk and promote well being.
- Help identify people who may pose a risk to others and, where possible, work to reduce offending behaviour.
- Reduce organisational risk and protect reputation.

10. DATA STORAGE

Information and records relating to programme participants will be stored securely and will only be accessible to authorised staff and volunteers.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

It is Romsey Mill's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

11. DISCLOSURE

Romsey Mill may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows Romsey Mill to disclose data (including sensitive data) without the data subject's consent.

These are:

- Carrying out a legal duty or as authorised by the Secretary of State.
- Protecting vital interests of a Data Subject or other person.
- The Data Subject has already made the information public.
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights.
- Monitoring for equal opportunities purposes – i.e. race, disability or religion.
- Providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.

12. SUBJECT ACCESS REQUESTS (SARs)

Romsey Mill will make sure that only people that need personal information can have access to it. All Data Subjects have the right to access any personal data relating to them which are held by Romsey Mill. Any individual wishing to exercise the right should apply in writing to the Chief Executive Officer with a Subject Access Request (SAR). The SAR must be made by the individual (the data subject) unless they have authorised a third party to make the request. Approval from the data subject must be verified. Any member of staff receiving a SAR should forward this to the CEO. Under the terms of the legislation, any such requests must be complied with within 40 days of receipt of the request in writing.

Subject Access Request entitles an individual to more than just a copy of their personal data. An individual is also entitled to be:

- Told whether any personal data is being processed. If no personal data is held about the requester, Romsey Mill must respond to let the requester know whether personal data is being processed.

- Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people.

- Given details of the source of the data (if known).

Personal information held on employees will only be disclosed to trustees, members of the Leadership and Management Team (LMT) and other staff as authorised by a member of the LMT, where specific action is required. If an employee accesses another employee's records without authority, this is deemed an act of gross misconduct under our disciplinary policy and is a criminal offence under section 55 of the DPA 2018.

In addition, Romsey Mill will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection.

- Everyone processing personal information understands that they are contractually responsible for following good data protection practice.

- Everyone processing personal information is appropriately trained to do so.

- Everyone processing personal information is appropriately supervised.

- Anybody wanting to make enquiries about handling personal information knows what to do.

- It deals promptly and courteously with any enquiries about handling personal information.

- It describes clearly how it handles personal information.

- It will annually review and audit the ways it holds, manages and uses personal information.

- It regularly assesses and evaluates its methods and performance in relation to handling personal information.

- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them.

13. CHILD PROTECTION AND DATA ACCESS

Child protection information will be stored and handled in line with the Data Protection Act 2018 and General Data Protection Regulation 2016 (GDPR) principles. The GDPR does not prevent staff from sharing information with relevant agencies, where that information may help to protect a child.

Child protection records are normally exempt from the disclosure provisions of the General Data Protection Regulation 2016, which means that children and parents do not have an automatic right to see them. If any member of staff receives a request to see child protection records, they should refer this to the Designated Safeguarding Lead who in turn will seek advice from Cambridgeshire County Council's Information Governance Team. Together a decision will be made about what information to share. This decision will consider the balance between the potential risk to the child and the principle of working openly and honestly with parents.

For further information regarding Safeguarding, please see Romsey Mill's Safeguarding Policy.

14. Complaints Handling Procedure

If an individual has a complaint regarding how their data is handled, they can make a complaint using Romsey Mill's Complaints Procedure. The complaint should be marked for the attention of the Data Protection Officer by email to info@romseymill.org or by post to Romsey Mill, Hemingford Road, Cambridge CB1 3BZ. Romsey Mill will acknowledge receipt of the complaint within 3 workings days. The complaint will then be fully investigated in line with our complaints policy. Romsey Mill's Complaints Policy can be found on our website - https://www.romseymill.org/policies

If an individual is not satisfied with the outcome of the Complaints Procedure, they can escalate their complaint to the Information Commissioner's Office - https://ico.org.uk/global/contact-us

This Data Protection policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the General Data Protection Regulation (GDPR) May 2016, Data Protection Act 2018 and Data (Use and Access) Act 2025.

In case of any queries or questions in relation to this policy please contact Romsey Mill's Data Protection Officer: Romsey **Mill's Operations & Resources Manager.**