Information Sharing/GDPR

Policy Statement

Rotherfield St Martin is committed to protecting the rights and privacy of individuals. To carry out our work of supporting older members of our community we need to collect and use certain types of data. All information will be collected and handled securely. The Data Protection Act 2018 governs the use of information about people (personal data). Within our organisation personal data will be held on computers, laptops and mobile devices, or in manual files and includes email, minutes of meetings and photographs.

Rotherfield St Martin is the named data controller for information held and is responsible for processing and using personal information in accordance with the Data Protection Act and GDPR. Collectively this is staff, trustees and volunteers (who have been fully vetted and have organisational reasons for handling personal data). Collectively as the Data controller we decide what personal information will be held and how it will be held or used. Volunteers of RSM who have access to personal information will therefore be expected to read and comply with this policy.

Purpose

The purpose of this policy is to set our commitment to keeping personal data protected. We recognise the risks to individuals of identity theft and financial loss if personal data is lost or stolen.

The Data Protection Act

This contains 8 principles for processing personal data with which we must comply

Personal Data:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met.
2. Shall be obtained only for one or more purposes specified in the Act and shall not be processed in any manner incompatible with that purpose or those purposes.
3. Shall be adequate, relevant and not excessive in relation to those purposes.
4. Shall be accurate and where necessary, kept up to date.
5. Shall not be kept longer than necessary.
6. Shall be processed in accordance with the rights of the data subjects under the Act.

7. Shall be kept secure by the data controller who takes appropriate measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information.
8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

Applying the Data Protection Act

We will let people know why we are collecting their data, which is for the purpose of supporting our members' health and wellbeing. Our 'lawful basis' and purpose for processing is 'consent' and 'vital interests'. It is our responsibility to ensure that data is only used for this purpose. Access to personal information will be limited to staff, trustees and fully vetted volunteers. We are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against us.

Procedures for Handling Data and Data Security

We have a duty to ensure that appropriate technical and organisational measures and training are taken to prevent:

- Unauthorised or unlawful processing of personal data
- Unauthorised disclosure of personal data
- Accidental loss of personal data

We therefore must ensure that personal data is dealt with properly no matter how it is collected, recorded or used. This applies whether or not the information is held on paper or electronically.

Privacy Notice and consent

The 'privacy notice' is included on our annual membership forms which are the main source of information about members. These forms will be stored securely in paper form.

Operational Guidance

Email:

Staff should consider whether an email (both incoming and outgoing) will need to be kept as an official record. If an email needs to be retained it should be saved to an appropriate electronic file or printed and stored securely.

Emails that contain personal information that are not required for operational use should be deleted permanently.

Phone Calls:

Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:

- Personal information should only be given verbally if there are no doubts to the callers' identity and the information request is innocuous. Members, staff, trustees and volunteers information will not be shared unless there is an operational reason for doing so, for example a VDS driver needing to contact a member or a safeguarding concern.
- If there are any doubts, ask the caller to put their enquiry in writing.
- We are alert to the fact that a caller may be impersonating someone with right of access, therefore if we have any doubts to a callers true identity we will call them back on the publicised telephone number of that organisation or known number of the individual.

Laptops and Portable Devices:

All laptops and portable devices that hold data containing personal information are password protected.

If left unattended, portable devices will be stored out of sight.

Portable devices are never left in vehicles overnight.

Portable devices are never left unattended in public places.

Data Security and Storage:

As a general rule we keep as little personal data as possible on computers and laptops. Personal data received on disk or memory stick will be saved onto a relevant file on the server or laptop/desktop and the information will be wiped from the memory stick.

Passwords:

We use passwords that are not easy to guess and that contain both letters and numbers. We do keep a written record of all passwords but this is not stored electronically and is kept in our safe.

Data Storage:

Personal data will be stored securely and is only accessible by staff and fully vetted volunteers who have an operational need to do so. Our main source of personal information comes mainly from our membership forms which are kept securely in the office. Some of the data from the forms is extracted and input onto a database 'Access' which is on password protected PC's/laptops. This is to aid the management of our membership. Information will only be stored for as long as it is needed or required by law and will be disposed of appropriately. For financial records this is 7 years. Archival material relating to

the charity such as minutes and legal documents will be archived and stored for the length of the charity in accordance with charity law. Other correspondence and emails will be disposed of when no longer required.

All personal data held for the organisation must be non-recoverable from any device that has been passed on/sold to a third party.

Sensitive Data

Sensitive data such as accidents, safeguarding and general notes on members will be kept securely and will not leave the office. This data will only be shared with regularity bodies as required and within the best interest of our members, i.e. we are concerned that they are being harmed or are at risk of being harmed.

We hold key codes for some of our members in the case of emergencies only. These codes are kept in our safe.

Data Subject Access Requests:

We may have to share data with other agencies such as local authority, funding bodies and other voluntary agencies. The circumstances where the law allows us to disclose data (including sensitive data) without the data subjects consent are:

- Carrying out a legal duty or as authorised by the Secretary of State, protecting vital interests of a Data Subject or other person e.g. safeguarding
- 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.

We regard the lawful and correct treatment of personal information as very important to successful working and to maintain the confidence of those to whom it deals. Therefore we ensure that personal information is treated lawfully and correctly.

Risk Management:

The consequences of breaching Data Protection can cause harm or distress to service users if their information is released to inappropriate people, or they could be denied a service to which they are entitled. This policy is therefore designed to minimise the risks and to ensure that the reputation of the charity is not damaged through inappropriate or unauthorised access and sharing.

This policy was written/reviewed by	Charity Manager Vicky Cheeseman
Adopted by	Trustees of Rotherfield St Martin
Date	16 July 2018
Last Reviewed	6th April 2022 - SJ
Next Review Due	5th April 2023 or sooner if legislation dictates.

For further information please visit: Information Commissioners Office (ICO)

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/Additional Information