Data Protection

Introduction

Sue Ryder complies with laws and regulations relating to the privacy and protection of personal data and takes these obligations seriously. This policy sets out the principles which we apply in processing the personal data of employees, contractors/consultants, volunteers, suppliers, service providers, supporters, contacts, customers, and service users.

This policy is prepared in compliance with the Data Protection Act 2018 and the General Data Protection Regulations. Any breach of this policy will be taken seriously and may result in disciplinary action.

What is personal data?

Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

Special Categories of Personal Data is any data that by its nature is particularly sensitive, including data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data concerning health, or data concerning a natural person's sex life or sexual orientation.

Data protection principles

Personal data must be processed in accordance with six data protection principles. It must be:

1. Processed lawfully, fairly, and in a transparent manner.
2. Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; this means that you can't collect it for one purpose and use it for another.
3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed; you must not collect or share more personal data than is required.
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay.
5. Kept in a form that allows identification of individuals for no longer than is necessary; you must not keep personal data for longer than you need it.
6. Processed in a way that ensures the security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

For more detailed information about following these principles, please refer to our full-length Data Protection Policy which can be provided by your line manager or Volunteer Coordinator.

Data Breaches and Notification

Data breaches must be reported immediately to your line manager, Company Secretary or the Data Protection Officer at data.protection@suerydercare.org

A data breach includes but is not limited to the following:

- Unauthorised disclosure of special category / personal data - this includes giving personal data to someone who is not authorised to receive it, providing health information to a third party without consent, sending personal data to the wrong person via email, phone or fax
- Loss or theft of confidential or special category data
- Loss or theft of equipment on which personal data is stored (e.g. loss of laptop)
- Unauthorised use of, access to, or modification of IT, data or information systems (e.g. via a hacking attack)
- Attempts (failed or successful) to gain unauthorised access to IT, data or information systems

When reporting the breach, please give details of the breach including when you became aware of it, where it occurred, and any action that you have taken.

Where there is any risk to the rights and freedoms of data subjects, we must notify the Information Commissioners Office without undue delay and, when possible, within 72 hours. If this is not done, the maximum fine the ICO can levy is £ 8.7 million. It is therefore very important that breaches are reported, however trivial they may seem.

If you need to send personal data to someone (and they have the right to see it) then you must consider the most secure way of sending it, which includes sending the minimum amount requested and the options of anonymisation or pseudonymisation. The more 'sensitive' the data, the more secure the delivery method has to be. If in doubt, seek advice.

Individual Rights and Requests

Data Subjects have the following rights in relation to their personal data. If you receive a request from an individual who wishes to exercise any of these rights then pass on the request to your line manager.

- **The right to be informed** - Data subjects have a right to know about our personal data protection and data processing activities.
- **The right of access** - Data subjects can make what is known as a Subject Access Request to request information about the personal data we hold about them.
- **The right to correction** - Data subjects have a right to require that any incomplete or inaccurate information is corrected.
- **The right to erasure (the 'right to be forgotten')** - Data subjects have a right to ask that we remove data we hold about them unless we have reasonable grounds to refuse.
- **The right to restrict processing** - Data subjects can request that we no longer process their personal data in certain ways, whilst not requiring us to delete the same data.
- **The right to data portability** - Data subjects can ask us to provide copies of personal data we hold about them in a commonly used and easily storable format.
- **The right to object** - Unless we have overriding legitimate reasons, data subjects may object to us using their data for marketing purposes, research, or statistical purposes.
- **Rights with respect to automated decision-making and profiling** - Data subjects have a right not to be subject to automated decision-making if those decisions have a legal (or similarly significant effect) on the subject.
- **Right to withdraw consen**t - If we are relying on consent as the basis on which we are processing personal data, the data subject can withdraw their consent at any time.

Subject Access Rights

It is a criminal offence to conceal or destroy personal data which is part of a Subject Access Request. This conduct would also amount to gross misconduct which could result in dismissal.

Accountability and Responsibility

All charity personnel are likely to be dealing with personal data in some form or another and must

comply with this policy. Dependent upon your role in the Charity you may have further and specific responsibilities around data protection, especially when you have access to 'Datasets' or deal with specific category information eg health records.

A manager of a dataset will be responsible for ensuring that access is restricted to those who need access and that access is removed when no longer required, also for ensuring that the information is accurate where appropriate.

Personnel Records

Access to the people database or volunteer database is strictly controlled by security protocols. The People Directorate is responsible for ensuring that all employee and/or volunteer data held by them is relevant, retained, and destroyed.

Any paper records will be destroyed by shredding or through a confidential waste service. Data held in electronic form will be deleted when no longer required.

Health Records

Anyone who has access to health records needs to be even more vigilant when considering their responsibility under GDPR and also needs to be aware of patient confidentiality. Apart from life and death situations, consent will be needed to share confidential information/health records with a third party.

Personal Data Update

All employees, volunteers, and contractors have a responsibility to notify the Charity of any changes to the following personal data; name, address, telephone number, home email address, person to notify in case of an emergency and their telephone number, and bank details.

Volunteers should inform their Line Manager who will update the database accordingly.

Training and Induction

All charity personnel must be made aware of this policy as part of their induction process.

There are additional data protection resources available via your line manager which you may find helpful and there is mandatory Data Protection E-Learning for all staff and key volunteers, dependent upon role.

Sending Personal Data

Information must not be sent outside of the UK. Please refer to the Legal Department if there is a requirement to do this.

Before sending personal data and specifically special categories of personal data consider:

a) Whether consent is required - see the Charity's Confidentiality Policy and Consent Procedure;

b) The best way to send the information

c) That you have included the minimum amount of information required (consider pseudonymising).

If you need to send personal information by email address, fax, or post, consider the sensitivity of the information. The more confidential or sensitive it is, the more care needs to be taken. You

need to consider the risk of it going to the wrong person, or being accessed by someone who shouldn't be able to see it – accidentally or deliberately.

a) **Sending by email**: **internally** emails sent between one Sue Ryder email address and another, and between nhs.net emails cannot be intercepted in transit, but you should always bear in mind the risks of transmitting very confidential or sensitive information, and you may decide that encryption is still appropriate given the sensitivity of the information.

You cannot encrypt or password-protect the actual email, so data must not be included in the body of the email but instead put in a document and sent as an attachment. Contact the IT Department if you are not sure how to do this. The encryption code/password must be provided separately by telephone or text. If you cannot password-protect the information then you must look at other forms of transmission. If in doubt contact the Company Secretary or IT.

c) **Sending by fax**: ensure that you have the correct number and have asked the recipient to be at the fax machine to collect the fax immediately after it is transmitted. If using a number for the first time, consider sending a test page first. If you are sending health information, consider sending two faxes, with the personal information in one and the clinical information in the other.

d) **Sending by pos**t: Copies of health records must always be sent by special/recorded delivery and marked 'Private and Confidential'. Original service user records should never be sent by post but always be hand-delivered.

Providing information over the telephone

Any member of staff or volunteer dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular, they should:

a) Check the caller's identity to make sure that information is only given to a person who is entitled to it.

b) Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

c) Refer to the Company Secretary for assistance in difficult situations. No one should be bullied into disclosing personal information.

d) Check the Confidentiality Policy, particularly if health care information is being requested.