

Data Protection Policy and Procedures

Surrey Care Trust (SCT) is committed to safeguarding and promoting the welfare of its beneficiaries, along with their protection and expects all staff and volunteers to share this commitment.

In order to function properly as SCT needs to collect and use information about staff, beneficiaries and other individuals who come into contact with the Trust. Furthermore, SCT is obliged to collect and use personal information to fulfil its obligations to its funders and bodies. In whichever way this information is collected and used, SCT is bound by the safeguards that are legally binding in the latest legislation data.

Surrey Care Trust is registered with the Information Commissioner, registration number Z5497617, and with the Fundraising Regulator.

We have considered available advice on the appointment of a data protection officer and have decided that our 'Data and Supporter Liaison Officer' is the nominated person to deal with day to day issues, with overall responsibility resting with the Chief Executive. We will keep this under review.

1. Aims

To comply fully with the Data Protection principles enshrined in the General Data Protection Regulation 2018 (GDPR 2018), which state that personal information must be:

- a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- b) 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;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) 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;
- e) 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
- f) 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."

To ensure that such principles are reflected in both electronic and manual systems for keeping personal information.

To ensure that staff, beneficiaries and other individuals are made aware of:

- The nature of the information collected about them
- The purpose(s) for which personal information will be held
- What such information will be used for
- Who, other than internally, the information may be disclosed to

To ensure that, unless the information is subject to other enabling legislation or the possibility of sharing such information has been made explicit, informed consent must be obtained before such information can be passed to another organisation or individual.

Processing and Sharing Information

To ensure compliance with the Data Protection General Regulation 2018 (GDPR 2018) non-sensitive personal data shall be processed fairly and lawfully, and shall not be processed unless at least one of the following conditions is met:

(a) the individual has given clear **Consent** to process their personal data for a specific purpose.

(b) the processing is necessary for a **Contract** with the individual, or because they have asked us to take specific steps before entering into a contract.

(c) there is a **Legal obligation: ie** the processing is necessary to comply with the law (not including contractual obligations).

(d) because of **Vital Interests: ie** the processing is necessary to protect someone's life.

(e) for a **Public task:** the processing is necessary to perform a task in the public interest or for an official function, and the task or function has a clear basis in law.

(f) the processing is necessary for our **Legitimate Interests** or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Special Category Data

Special Category Data, as defined by the Data Protection General Regulation 2018, is information that relates to:

- Racial or ethnic origin
- Physical or mental health
- Sexual life or sexual orientation
- Genetics
- Biometrics (where used for ID purposes)

- Religious or other beliefs
- Politics
- Trade union membership

Special category Data shall be processed fairly and lawfully only if at least one of the following conditions is also met (in addition to the general conditions listed above):

- (a) the data subject has given explicit **Consent** to the processing of personal data for one or more specified purposes.
- (b) the Trust needs to hold the information **to Comply with Employment Law**.
- (c) to protect the **Individual's Vital Interests** in cases where consent cannot be given, or to protect the interests of another person where consent has been unreasonably withheld
- (d) processing of information by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union is needed, with appropriate safeguards, in the course of Surrey Care Trust's legitimate activities.
- (e) the personal data being processed has been manifestly made public by the individual.
- (f) processing of information is necessary to establish, exercise or defend legal claims.
- (g) processing of information is necessary because of substantial public interest, on the basis of EU or UK law, with the safeguards that it is proportionate, respects the essence of the right to data protection and provides suitable and specific measures to safeguard the rights and interests of the individual.
- (h) processing of information is necessary for preventive or occupational medical reasons.
- (i) processing of information is necessary for reasons of public interest in the area of public health.
- (j) processing of information is necessary for archiving information in the public interest, such as for statistical reasons.

Criminal Offence Data

Under the GDPR 2018, there are there are separate safeguards for personal data relating to criminal convictions and offences.

This concept of criminal offence data includes the type of data about criminal allegations, proceedings or convictions that would have been sensitive personal data under the 1998 Data Protection Act. However, it is potentially broader than this. In particular it specifically extends to personal data linked to related security measures.

Criminal Offence Data shall be processed fairly and lawfully only if Surrey Care Trust has specific legal authorisation to do so. We will not keep a comprehensive register of criminal convictions.

2. Procedures within the Trust

Between those employed by the Trust, and accountable to the Chief Executive, it is recognised that the fullest sharing of information between those responsible for the teaching, welfare and care of beneficiaries leads to the most benefit for the individual.

It is inherent that any and all such information should be kept confidential between members of staff within the Trust and not shared with others.

It is a matter of professional judgement as to whether information disclosed by a beneficiary is of necessity shared by all within the Trust. If uncertain, members of staff should consult with their senior manager.

Any information disclosed relating to physical, sexual or emotional abuse, or neglect of beneficiaries will be fully subject to the Trust's Safeguarding policy. Such information (in whatever form) will be retained in accordance with current legislation.

Any and all manual records kept by the Trust relevant to individuals, no longer required, must be shredded.

When beneficiaries are no longer involved with the Trust records held will be archived and stored securely for a maximum of 10 years or as otherwise specified in contracts. The relevant manager will be responsible for ensuring records are archived.

At times, individual information is required for illustrative purposes by processes that the Trust is subjected to by other legislation, guidance or practice. Examples include Inspection; Performance Appraisal and Target Setting. The Trust will be explicit to beneficiaries in this respect, though individuals should not be named in any publication or report resulting from such processes.

Information with respect to named individuals should not be produced for any audience whereby the information may enter into the public domain, without the express permission of the person involved. Trust based examples include:

- Newsletters to parents and the community
- Reports to the Board of Trustees
- Review and evaluation documentation for other than internal use
- Any and all documentation used for training or illustrative purposes to persons outside of the Trust
- Website and other internet based information

Other professionals or volunteers working on a temporary basis as a member of staff within the Trust and, accountable to the Chief Executive, will be required to adhere to the principles of information protection outlined.

3. Procedures outside the Trust

When exchanging or sharing data and information with other institutions, organisations, agencies or individuals the following principles are observed:

- Individuals (or in the case of young people under 18) parents or guardians should be made aware of the exchange or sharing of data and information with other institutions, organisations, agencies or individuals both through the website and by clear statements on data capture forms
- When sharing and exchanging information with other institutions, organisations, agencies or individuals the minimum amount of data or information should be provided, exchanged or shared, its purpose clearly identified and any further processing of such information by that institution, organisation, agency or individual reported to the Trust.
- Staff and volunteers should be aware that verbal exchange of data or information can be misunderstood, misinterpreted, or misrepresented, and it should be avoided

- The institutions, organisations, agencies or individuals receiving information from the Trust will undertake not to disclose, share or exchange such information with other institutions, organisations, agencies or individuals without first obtaining further informed consent from the Trust unless the original consent covered such eventualities
- Information shared or exchanged with other institutions, organisations, agencies or individuals should be first checked for accuracy and reliability by the Trust. Any information not based upon established fact should be clearly identified as opinion or hearsay
- It is the responsibility of the receiving institution, organisation, agency or individual to inform the Trust of any and all information and data that is discovered to be out of date, inaccurate or unreliable
- Institutions, organisations, agencies or individuals that have disclosed to them information relevant to the care and welfare, or the effective service for beneficiaries of SCT, should take the necessary steps to achieve the consent of the individual and/or parent/guardian to share such information with the Trust, which they should then undertake
- Institutions, organisations, agencies or individuals receiving information or data from the Trust must take all reasonable precautions to protect such personal information from unauthorised or unlawful processing or use, and against its accidental loss, destruction or damage
- Institutions, organisations, agencies or individuals unable to agree to these principles will not be made party to personal information concerning SCT beneficiaries except where this is covered by enabling legislation or associated Orders

Any breach of the procedures identified in this policy may lead to disciplinary action being taken against the member of staff involved.

4 Access to Information

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR 2018.

We will provide individuals with privacy information including: our purposes for processing their personal data, retention periods for that personal data, and who it will be shared with at the time that we collect personal data from them.

If we obtain personal data from other sources, we must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.

The information we provide to people should be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.

Staff and other individuals have the right to access information held on computerised or manual records which relates to them.

This also applies to parents/guardians or where appropriate a person legally acting on an individual's behalf, who have the right to access information held, including educational records, on computerised or manual records, which relates to themselves or their ward. Students can also request to see the personal information held about them about them.

Some information may be withheld from the individual. For instance, if it may cause harm to the physical or mental health of the pupil or a third party; information which may identify third parties (for example, other pupils), and information that forms part of court reports. Information may also be withheld if in that particular case it would hinder the prevention or detection of crime or the prosecution or apprehension of offenders to provide it

In addition, individuals, or where appropriate a person legally acting on a beneficiary's behalf, are also entitled to be given a description of the personal information which makes up the Trust record, together with details of the purposes for which the information is processed, the sources of the information, and the institutions, organisations, agencies or individuals to which the information may be disclosed

A parent seeking access to an educational record does not have a right of redress under the GDPR 2018 unless he/she is acting on behalf of their child. As parents have an independent right to access student records the students themselves have no right to prevent it.

If a request for information under the GDPR 2018 is ignored the matter may be referred to the Information Commissioner, or an application for disclosure can be made to the courts. The person requesting the information, unless acting on behalf of their child, in the first instance should contact the Board of Trustees, or, as a last resort, the courts

Further information about the GDPR 2018 can be obtained from the Commissioner's web site (www.ico.gov.uk), requested from an information line (0303 123 1113 or 01625 545745), or by post from:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
Tel: 08456 30 60 60 or 01625 54 57 45
Fax: 01625 524510

Individuals may make a complaint about the way in which information about them is held, processed or disclosed by writing to the Chief Executive, after that the Board of Trustees, the Information Commissioner, or as a last resort, the courts.

Policy Review

This policy will be reviewed and updated in line with our ISO 2015 guidelines in order to reflect best practice in information management, security and control and to ensure compliance with most recent Data Protection legislation