Data Protection Policy and Procedures

Surrey Care Trust (SCT) is committed to safeguarding and promoting the welfare of its staff, volunteers and beneficiaries, including protection of any of their personal data held by the Trust, and expects all staff and volunteers to share this commitment.

This policy describes how the Trust collects, stores, processes and shares personal data, whether belonging to staff, trustees, volunteers, beneficiaries or funders to ensure we meet the requirements of the Data Protection Act 2018 (the UK's implementation of the General Data Protection Regulation).

Personal data is information that relates to an identified or identifiable individual. [1]

In order to function properly, Surrey Care Trust needs to collect and use information about staff, beneficiaries and other individuals who come into contact with the Trust. Surrey Care Trust is also obliged to collect and use personal information to fulfil its obligations to its funders and bodies. The ways in which the trust collects and uses this information is legally bound by the safeguards in the latest legislation.

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

The Trust has considered available advice on the appointment of a data protection officer and have decided that: *'our Managers will have responsibility for dealing with day to day issues, with overall responsibility resting with the Chief Executive Officer.'* We will keep this under review.

1 Policy Aims

***i) To comply fully with the 7 Data Protection principles enshrined in the UK GDPR and Data Protection Act 2018*:**

1) LAWFULNESS, FAIRNESS AND TRANSPARENCY: personal data must be processed lawfully, fairly and in a transparent manner in relation to individuals;

2) PURPOSE LIMITATION: personal data is 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) DATA MINIMISATION: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4) ACCURACY: data must be 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 corrected without delay;

5) STORAGE LIMITATION: data must be 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;

6) INTEGRITY AND CONFIDENTIALITY: data must be 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; and

[1] What is personal data? | ICO and for more detailed guidance: What is personal data? | ICO

7) ACCOUNTABILITY: the Trust takes responsibility for what we do with personal data and how we comply with the other principles. To do this, we must have appropriate measures and records in place to be able to demonstrate compliance.

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

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

a) The nature of the information collected about them

b) The purpose(s) for which personal information will be held

c) What such information will be used for

d) Who, other than internally, the information may be disclosed to

iv) 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 is obtained before it can be passed to another organisation or individual.***

2 Types of personal data [2]

There are three categories of personal data which the Trust may need to process and store; non-sensitive personal data (from which an individual can be identified), special category data (which is more sensitive) and criminal records data (which is a specific type of special category data and governed by the Rehabilitation of Offenders Act).

Personal data

To ensure compliance with the Data Protection General Regulation 2018 (UK GDPR 2018) all personal data shall be processed fairly and lawfully. It may only be processed when at least one of the following six lawful conditions has been identified as having been met and that legal basis must be determined before processing the data and cannot be changed:

(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: i.e.** the processing is necessary to comply with the law (not including contractual obligations).

(d) because of **Vital Interests: i.e.** 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

[2] ICO interactive tool for determining lawful basis or processing personal data

Special Category Data, as defined by the UK GDPR as data that merits specific protection as it is more sensitive and its use could create a risk to an individual's fundamental rights and freedoms. It is information that relates to:

a) Racial or ethnic origin
b) Physical or mental health
c) Sexual life or sexual orientation
d) Genetic data
e) Biometric data (where used for ID purposes)
d) Religious or philosophical beliefs
e) Political opinions
f) Trade union membership

Special category Data can be processed fairly and lawfully once at least one of the following additional conditions has been identified as appropriate (***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 listed above.

(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, an association or any other not-for-profit body with a political, philosophical, religious or trade union aim, with appropriate safeguards.

(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 safeguard 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

Criminal offence data | ICO

Under the GDPR 2018, there are separate safeguards for personal data relating to criminal convictions and offences. Data protection law gives extra protection to criminal offence data or other security concerns because of the risk to the individual in sharing it. However, the rules are also different from those relating to sharing special category data; the need to protect people from criminal activity means that using this type of information can be justified in a wider variety of circumstances, despite the potential impact on the person who it's about.[3]

[3] Data storage, sharing and security | ICO

The Trust has a separate DBS policy, aligned to its Safeguarding policy and procedures, which defines the control, processing and safeguarding of criminal records data in its work.

Retention schedule
The Trust's retention schedule: SCT retention schedule by programme.xlsx (sharepoint.com) identifies the legal basis under which the Trust processes personal data. It also identifies the additional bases under which special category data is processed and the length of time for which data is retained by the Trust. The retention period may be based on statutory or contractual obligations, so it is important that managers are aware which takes precedence in any situation.

3 Data sharing procedures within the Trust

It is recognised by those employed by the Trust, and accountable to the Chief Executive, 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 to this principle 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 with whom information disclosed by a beneficiary is shared 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 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 which relate to individuals and are 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 to which the Trust is subject by other legislation, guidance or practice. Examples include inspection, audit, performance appraisal and target setting and monitoring. The Trust will be explicit about this with beneficiaries, though individuals should not be named in any publication or report resulting from such processes.

Information from which individuals could be identified can only be produced for any audience whereby the information may enter into the public domain with 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 bidding, 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.

Fundraising and Marketing
There is a defined policy in relation to personal data held by Fundraising and Marketing which is appended to this policy.

4 Data sharing procedures outside the Trust

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

a) 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.

b) 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.

c) Where personal information is shared electronically with other agencies, some form of password protection or encryption must be used. This will sometimes be dependent on the agency that is the data controller.

d) Staff and volunteers should be aware that verbal exchange of data or information can be misunderstood, misinterpreted, or misrepresented, and it should therefore be avoided.

e) 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.

f) 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.

g) 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.

h) 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.

i) 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

j) 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.

5 <u>Working with data at home or away from the Trust's premises</u>

Data protection is not a barrier to increased and different types of homeworking, but we'll need to consider the same kinds of security measures for homeworking that you'd use in normal circumstances.

Working from home entails taking data home, in digital or print format, meaning that staff and volunteers will have information that pertains to the organisation around people that are not SCT employee. It may seem unlikely that a friend or family member would even be interested in personal data held by your organisation. Regardless, make sure that data is kept away from non-employees. This means locked drawers, password protected computers and shredding any paper that holds confidential information. Data is vulnerable to loss or theft wherever we are.

Managers should review their data security practices as part of a change to flexible working. They should monitor what employees are accessing sensitive data, when they're accessing it, and what they're accessing. This applies equally to hard-copy and soft-copy data so that information is kept securely and not put into peril, lost or stolen.

All staff and volunteers must refer to the Trust's policy on Working with Display Screen Equipment and Surrey Care Trust IT systems and in particular:

· Avoid working in an area frequented by family, friends or other visitors

· If there are other people in close proximity, try to position your device screen so it cannot be seen by them when looking at any personal or confidential data.

· If you leave your device unattended initiate the screensaver, and/or exit the file you're accessing, and/or lock the screen

· Keep your system login/password private

· Do not allow family or friends to use your work device that accesses company systems

· Do not download any company data or information to your personal home device unless you have had specific permission to do so and there are deletion control measures in place.

· Do not use public Wi-Fi to access company systems

· Do not upload any software to company systems without permission

· Ensure all portable devices are password protected

· If your device is lost, stolen or misplaced, advise us and the Trust's IT provider immediately

· If any telephone discussion involves the exchange of personal data, make sure you cannot be overheard

· Print document containing personal data only when necessary, and make sure the document is destroyed when no longer needed

· Observe a "clean desk" policy as much as possible – do not leave documents containing personal or confidential information lying around

· Lock any personal data (e.g. bank details, names, DOBs, addresses, ethnicity/disability data) securely in a locked drawer or in a secure online facility

· Report any breach, or suspected breach in data in the usual way.

6 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.

At the time that we collect personal data from them, 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.

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 they are 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.

Related policies:
Code of Conduct. Complaints policy. Disclosure Barring (DBS) policy, Recruitment policy.

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 **Last review November 2024. Next Review November 2025**

ANNEX 1 – FUNDRAISING AND MARKETING

In relation to the Data Protection Act 2018, the General Data Protection Regulation (GDPR), and the Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003 Surrey Care Trust's Fundraising and Marketing team (F&M) will:

a) Keep up to date with guidance from the ICO. This includes the ICO's direct marketing guidance, its GDPR consent guidance, and legitimate interests guidance.

b) Pay the data protection fee to the ICO

When processing personal data (including information that is available to the public) for any purpose F&M will:

- have a lawful basis (a valid legal reason) for collecting, using and keeping the personal data (for more information on the grounds (or 'conditions') for processing personal data
- give people concise, open, understandable and easily accessible information about how we will process their personal data, including who our organisation is, what we will do with their personal data and who (if anyone) we will share it with
- only process personal data in ways that the person whose data it is would reasonably expect
- **not** do anything unlawful with personal data.
- Meet any duties we have to keep data confidential, unless there is an overriding legal reason to do so

We will make sure that all materials, in particular filled-in donor forms, are stored securely and in line with our obligations under data protection law.

We will make sure that data we keep about donors is accurate and reflects their communication preferences, and only keep it for as long as is necessary for:

- the purpose or purposes you are processing it for
- purposes compatible with these stated processing purposes
- a purpose that is allowed by law and is in the public interest

We will take all reasonable steps to make sure that:

- databases are accurate and, where necessary, up to date
- we don't send direct marketing to people who have told us they don't want to receive it
- we will stop sending communications addressed to people we know have died

We will have appropriate systems or procedures in place (such as a list of people not to contact) to make sure that we do not send direct marketing to people who have asked not to receive it.

We will either stop sending direct marketing to a person within a reasonable period (as soon as possible, but in any case within 28 days) or not begin to process a person's personal data for the purpose of sending them direct marketing if we receive notice from, or on behalf of, that person telling you that they don't want to receive direct marketing. For example:

- a notice from (or sent on behalf of) a person through the Fundraising Preference Service telling us that a request to stop contact has been made
- any other clear indication from a person (or made on their behalf) that they do not want us to contact them for direct marketing purposes. This indication may include giving you their contact preferences or

We will **not** share personal data with any other organisation unless we have a lawful basis to share it and can prove that we meet the processing requirements 3.3.2.

a) If personal data is shared between organisations e.g. under a data-processing arrangement (where one organisation acts on behalf of another organisation under a written contract, such as professional fundraisers, data-management companies or printing houses) the organisational structure or arrangement and the reason for processing the data **will** be clear in the privacy information we give to the person in order to meet their right to be informed.

b) We will **not** share a person's personal data with any other organisation for that organisation's marketing purposes unless we are allowed to do so by law, either because we have the person's consent to do so or through any exceptions

c) We will not sell a person's personal data to any other organisation, unless we can show that we have that person's freely given, specific, informed and unambiguous consent to sell their data.

d) If we plan to use a real-life example of a person in a case study, we will only process that person's personal data in line with the law.

Direct Marketing

Direct marketing is defined in law as 'The communication (by whatever means)…of any advertising or marketing material…which is directed to particular individuals…' The ICO states that fundraising activity, as well as charities' promotional and campaigning work, is covered by the definition of direct marketing.

In practice, fundraising messages which are sent electronically (for example, phone calls, faxes, texts and emails) or by addressed mail are likely to be directed to a specific person, and so are covered by this definition. The marketing must be directed to particular people. Some marketing is not directed to specific people (for example, unaddressed mail) and so is not covered by this definition.

a) Alongside data protection legislation that applies when processing personal data for direct marketing purposes, the Privacy and Electronic Communications Regulations (PECR) will apply when sending marketing electronically, such as by email or text message and in recorded phone calls. In these cases, we will always need the person's consent to send them direct marketing, unless:

   - we meet the 'soft opt-in' condition which allows businesses who have received a person's contact details when selling a product or service to them (or during negotiations relating to a possible sale) to market similar products and services to that person
   - we are marketing to businesses or organisations (including where you contact an individual using a corporate email address such as firstname.surname@companyname.com).

b) We will have a lawful basis for processing personal data in order to send direct marketing communications to people (typically 'consent' or 'legitimate interest')

c) When using Consent as a lawful basis for processing personal data in order to send direct marketing communications, the consent **will be**:

   - be a freely given, specific, informed and unambiguous indication of the person's wishes
   - be given through a clear positive action from the person concerned to show they have given consent (for example, using active methods, such as ticking an unticked opt-in box or answering 'yes' to a question)
   - give options for different levels of consent for different types of processing if you plan to process the person's data for more than one purpose

- be separate from your other terms and conditions and not be something the person has to give when signing up to a service (unless you need the consent to be able to provide that service)
- name your organisation and any others who will be relying on the consent
- tell people about their right to withdraw their consent and make it as easy for them to withdraw consent as it is to give it
- be recorded in a way that allows your organisation to show who gave consent, when they gave consent, how they gave consent, and what they were told in connection with giving consentElectronic requests for consent **will** be clear and concise and not unnecessarily disrupt the use of the service the consent is for. For example, you can achieve this by breaking a longer privacy notice into shorter pieces of privacy information which pop up only at the point where a person is asked for their personal data.

b) If we have a person's consent to send them direct marketing communications, we will:

- offer them an easy way to withdraw their consent (such as an 'unsubscribe' button in any communications you send)
- remind the person, as often as our organisation reasonably decides, of their contact preferences and offer them an easy way to change these if they want to (such as an 'update your communication preferences' button)
- update the person's record as necessary to reflect changes to their consent or contact preferences

c) Make sure that all consent statements (wording to gain consent for marketing purposes) displayed in your fundraising materials are at least the same font size as:

- any text which asks for personal data
- any text which states the donation amount

d) If there is no text asking for personal details or stating the donation amount, our consent statements will be in a font size of at least 10.

When Legitimate interest is used as a basis for direct marketing communications

a) When we use legitimate interest as the basis for processing data for the purpose of direct marketing by live phone call or by post, we will show that we:

- Have identified a legitimate interest
- need to process the data to achieve that interest (under ICO guidance, if the same result can reasonably be achieved in another, less intrusive way, legitimate interests will not apply)
- have balanced our interest in processing the personal data against the interests, rights and freedoms of the person to make sure that your interests are not overridden by theirs 3.5.8.

b) When we rely on the legitimate interest condition as the lawful basis to process data, we will have a record of our decision-making to help show that we meet the conditions set out above.

c) When we rely on the legitimate interest condition as the lawful basis to process data for the purpose of direct marketing by phone or post, our privacy notice will:

- explain what we will use the personal data for
- explain our legitimate interests
- offer, in the privacy notice and in any other direct marketing communication we send, a clear and simple way for the person to tell us that they do not want to receive direct marketing in future.

Requests from people to access their personal data

a) When we process a person's personal data, we will, if that person asks us to, give them a copy of the personal data we hold about them and details of how we use it in line with the person's right of access

b) If we hold or use a person's personal data to fulfil a contract or because we have their consent to process it, we will make sure that the personal data can be easily moved, copied or transmitted from one computer system to another if the person asks us to do this (whether this is to their own systems, or to the systems of another organisation or new data controllers).