Data Protection Policy

SLT Lead & Author Olivia Rowntree, Head of Audit Risk & Governance / Data Protection Officer	**Date Reviewed** February 2023 March 2025
Ratification Information Governance Working Group	**Date** May 2025
Published Date May 2025	**Next Review Date** May 2027

1 Purpose and Objectives

This policy describes the principles to be applied in relation to the collection, handling, processing, transferring or storing of personal data in the course of TCT's operational activities.

The objectives of the policy and this procedure are to:

- Establish and assign clear accountability for the protection of personal data;
- Ensure that all colleagues are aware of their individual responsibilities for data protection;
- Comply with all relevant data protection and e-privacy legislation and professional standards
- Manage the risk of personal data breaches

UK Legislative Framework

The two key pieces of legislation are the UK General Data Protection Regulation ("UK GDPR") and Data Protection Act 2018 ("DPA 2018")

The UK GDPR sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies. The DPA 2018 sits alongside and supplements the UK GDPR - for example setting out certain exemptions. It also sets out separate data protection rules for law enforcement authorities, extends data protection to some other areas such as national security and defence, and sets out the Information Commissioner's functions and powers.

Failure to comply with data protection legislation can lead to fines of up to €20m or 4% of income. However, the impact of negative media coverage on the charity's reputation and the loss of public confidence could be even more significant as The Children's Trust recognises that a lot of the personal data it holds is of a sensitive nature.

Being a health care provider, TCT must also have regard to the Department of Health and Social Care's National Data Guardian Standards and to the Common Law Duty of Confidentiality. TCT is required under its NHS England, contract to demonstrate compliance on an annual basis with NHS Digital's Data Security and Protection Toolkit.

The Children's Trust therefore takes the protection of personal data extremely seriously and mandates compliance with this policy and all related sub-policies at all times and across all areas.

2 Scope

This policy applies to all colleagues and the processing of all personal data during the course of charity business including that of; our beneficiaries, supporters, suppliers, partners and colleagues (whether employed or engaged on a voluntary or consultancy basis) both past and present and across the entire organisation.

3 Definitions

Unless otherwise stated, the words or expressions contained in this document shall have the following meaning:

the Charity/ organisation/ TCT	means The Children's Trust
SOP	Standard Operating Procedure
UK GDPR	UK General Data Protection Regulation

DPA	Data Protection Act
DPO	Data Protection Officer

The UK GDPR applies to the *processing* of *personal data*[1]. *Processing* is very broadly defined as carrying out "*any operation or set of operations*"[2] on the data, including:

- Collection
- Recording
- Organisation
- Structuring
- Storage
- Adaptation or alteration
- Retrieval
- Consultation
- Use
- Disclosure by transmission
- Dissemination or otherwise making available
- Alignment or combination
- Restriction (that is, the marking of stored data with the aim of limiting its processing in the future)[3]
- Erasure
- Destruction

The GDPR defines *personal data* as "*any information relating to an identified or identifiable natural person ('data subject')"*. The term "*natural person*" means a "living" person, therefore the GDPR does not apply to the deceased. Types of personal data include:

- Personal details
- Family and lifestyle details
- Education and training
- Medical details
- Employment details
- Financial details
- Contractual details (for example, goods and services provided to a data subject)

In effect, <u>any activity</u> involving <u>personal data</u> falls within the scope of the GDPR.

Other definitions relevant to this policy are as follows:

- *"consent"* - of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

- *"controller"* – the natural or legal person/ body which, alone or jointly with others, determines the purposes and means of the processing of personal data. The Children's Trust is a data controller. Most obligations under the GDPR fall on data controllers;

- *"filing system"* - any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

- *"personal data breach"* means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

- *"processor"* - a natural or legal person/ body which processes personal data on behalf of the controller. For example, if a separate organisation handles The Children's Trust's payroll function it would be doing so as a data processor;

[1] (Article 1(1) GDPR)
[2] (Article 4(2) GDPR)
[3] (Article 4(3) GDPR)

- *"profiling"* - any form of automated processing of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

- *"pseudonymisation"* - means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

- *"special categories of personal data"* – under the previous act this was known as "sensitive personal data" and is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. The GDPR imposes particular requirements regarding the processing of such data.

4 Policy Statement

4.1 The Charity shall appoint individuals with the requisite skills and knowledge to oversee and guide organisational compliance with all relevant data protection legislation and related standards set by the Department of Health and Social Care and other government departments from time to time. Notably, TCT shall appoint:

- Data Protection Officer (Head of Audit Risk & Governance)
- Senior Information Risk Officer (Director Resources)
- Caldicott Guardian (Medical Director)
- Information Asset Owners (IAOs)

4.2 An Information Governance Working Group shall be established to oversee policy development and the ongoing programme of compliance activity and to provide assurance to the Finance, Investments & Resources Committee that processes and controls are designed and operating effectively.

5 Roles and responsibilities

The Data Protection Officer (DPO)

The Data Protection Officer is responsible for the ongoing review and maintenance of the Data Protection Policy, related sub-policies and procedures and for ensuring there is adequate training across the organisation to support the implementation of the same.

Under the GDPR, the Data Protection Officer's primary objective is ensuring The Children's Trust's compliance with the GDPR. The Data Protection Officer's other tasks are set down by the GDPR[4] and include:

- maintaining The Children's Trust's Notification (essentially The Children's Trust's entry in the Information Commissioner Office Register of Data Controllers);
- advising colleagues on our GDPR compliance and acting as point of expertise for any data

[4] (Article 39)

protection issues which may arise within The Children's Trust;
- working with colleagues across the organisation to ensure there is effective compliance monitoring;
- advising regarding privacy impact assessments; and
- co-operating with data protection supervisory authorities, in the UK, the Information Commissioner's Office.

The Data Protection Officer must be informed about all data protection issues/ incidents within The Children's Trust in a proper and timely manner.

The contact details of the DPO are; dpo@thechildrenstrust.org.uk and details of the current role holder can be found on the Information Governance page of The Loop.

If you have any queries in relation to this policy or its related sub-policies, or are concerned about a breach of policy, please contact the DPO as detailed above.

Senior Information Risk Officer

The SIRO's role is to take ownership of TCT's information security policy and associated risk management strategy and processes and act as champion for information risk at board meetings.

Other key responsibilities include:

- Overseeing the development of an information risk management process;
- Developing an information security strategy and approval of the information security budget;
- Taking ownership of the risk assessment process for information and cyber security;
- Reviewing and approving action in respect of identified information risks;
- Ensuring that the organisation's approach to information is communicated to all colleagues;
- Approval of information security policies;
- Ensuring the board is adequately briefed on information risks and issues;
- Providing leadership and guidance to Information Asset Owners;
- Signing off the charity's annual self-assessment (alongside Director IT and Facilities) against the NHS Data Security and Protection Toolkit, Cyber Essentials and PCI DSS;
- Monitoring compliance with this policy.

Caldicott Guardian

The Guardian plays a key role in ensuring that the organisation satisfies the highest practical standards for handling patient identifiable information.

- Act as the 'conscience' of The Children's Trust, by actively supporting work to enable information sharing where it is appropriate to share and advising on options for lawful and ethical processing of information;
- Represent and champion confidentiality and information sharing requirements and issues at all levels of the organisation;
- Help embed the Caldicott principles when determining whether identifiable information should be used or disclosed;
- Work collaboratively with the Senior Information Risk Owner (SIRO) and Data Protection Officer on information governance matters.
- Ensure the confidentiality and data protection work programme is successfully co-ordinated and implemented across frontline clinical services;
- Ensure compliance with the principles contained within NHS Digital's: *"Code of practice on confidential information"* (2014) and that staff are made aware of individual responsibilities through policy, procedure and training;

- Provide advice and assurance to senior management, the Information Governance Working Group and the board on confidentiality and data protection issues;
- Identify and address any barriers for sharing for care.

Information Asset Owners (IAOs)

With a dotted line to the SIRO, IAOs have the following key responsibilities which are detailed further in "Information Assets Management Procedure":

- Lead and foster a culture that values, protects and uses information in the interests of TCT's beneficiaries and other stakeholders;
- Understand the data flows to and from the asset;
- Understand who has access to each asset and why and monitor their use of the asset;
- Identify, assess and mitigate risks to each asset, provide assurance to the SIRO and lead on any data loss incidents, ensuring these are reported in a timely manner and investigated and resolved appropriately.

IAOs may delegate their day-to-day responsibilities to Information Asset Administrators but will remain fully accountable.

All directors, heads of, senior managers and other people managers

These roles are responsible for:

- Monitoring compliance with all information governance and security policies and mandatory training requirements;
- Ensuring that users are set up on corporate systems and given access to information assets on a 'need to know' basis aligned with their job description;
- Consulting with the DPO about any significant proposals for new processes or systems, or changes to existing ones, that involve the processing of personal data and ensuring a Data Protection Impact Assessment is completed as necessary;
- Consulting with the DPO before appointing a new third-party data processor or making any changes to arrangements with an existing data processor;
- Consulting with the DPO and/or Caldicott Guardian before any non-routine sharing of confidential patient information with third parties;
- Notifying the DPO without delay in the event that a suspected or actual data breach is identified;
- Notifying the DPO of any subject access requests in a timely manner;

6 Data Processing Principles & Requirements

The GDPR sets out seven data protection principles which all colleagues will adhere to, summarised as follows:

- **Lawfulness, fairness and transparency** - personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject;
- **Purpose limitation** - personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- **Data minimisation** - personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

- **Accuracy** - personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay;
- **Storage limitation** - 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;
- **Confidentiality, Integrity (& Availability)** - personal data shall 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;
- **Accountability** - the controller shall be responsible for, and be able to demonstrate compliance with, the six principles above.

6.1 Lawfulness (and Fairness) of Processing

Personal data must be processed lawfully, fairly and in a transparent manner and we will communicate our legal basis for personal data processing in our privacy policy on our website and in other prominent notices at the point of data collection.

6.1.1 Lawful Bases

The legal bases for processing *personal data* at The Children's Trust are set out below:

- **Consent** - the data subject has given us their consent one or more specific purposes. If relying on consent as our lawful basis for processing, we will make this clear in our Privacy Policy and will inform the data subjects that they have the right to withdraw consent at any time.
- **Performance of a contract** – it is necessary for the performance of a contract with the data subject, or in order to take steps initiated by the data subject before entering into a contract;
- **Legal compliance –** we have a legal obligation to process certain personal data;
- **Vital interests** – it is essential for reasons of life or death of the data subject or of another individual;
- **Public interest** - 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; and
- **Legitimate Interests –** it is necessary for the purposes of our legitimate interests or those of a third party, provided those interests are not outweighed by the fundamental rights and freedoms of the data subject, in particular if the data subject is a child.

In addition, where ***special categories of personal data*** *are processed*, an additional specific legal basis must apply. The most relevant of these for The Children's Trust will be:

- **"Explicit" consent** - the data subject has given explicit consent to the processing of those personal data for one or more specified purposes (except where the law provides that the prohibition for processing special categories of data may not be lifted by the data subject);
- **Vital interests** – it is essential for reasons of life or death of the data subject or of another individual;
- **The provision of healthcare** - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or UK law or pursuant to contract with a health professional and subject to certain conditions and safeguards.

The detailed legal bases for the main activities of the Children's Trust are set out in the Record of Processing Activities.

Please note that in order for the use of health data to be lawful, confidentiality and consent to treatment rules must also be followed: GDPR does not affect the law on lawful consent to treatment for patients which is covered in detail by the GMC Guidance on Confidentiality https://www.gmc-uk.org/professional-standards/the-professional-standards/confidentiality.

6.2 Transparency

We will ensure we are transparent and explicit with our beneficiaries, supporters, partners, colleagues and other data subjects about the processing of personal data that we undertake. We will make sure this information, captured in our privacy notices is readily accessible and easy to understand using clear and plain language, particularly when such information is addressed to a child.

Data obtained from the data subject

Specifically, when we collect data from a data subject, we will include information in our privacy policy about our purpose and legal basis for processing that data, who we share it with, the security measures we have in place, how long we keep the data for and the data subject's rights under the UK GDPR.

Data obtained from a third party

If we collect personal data indirectly, i.e. from third parties, we will provide all the above information to the data subject (as if we had obtained the data directly) as well as information about the origins of the personal data and whether these were publicly accessible.

We will provide this information to the data subject within one month of receiving the personal data. In cases where the personal data will be used to communicate with the data subject, the information will be provided at the latest at the time of the first communication to that data subject, or if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

Our privacy policy for data subjects external to The Children's Trust can be found on our website along with data subject-specific privacy notices as follows:

- Beneficiaries
- Supporters
- Professionals and Corporate Partners
- Candidates and Prospective Volunteers

We also have a People Privacy Policy (on TheLoop) which covers how we collect, use, store and share the personal data of colleagues working at The Children's Trust (whether they are employees, volunteers, contractors or any other type of worker).

6.3 Rights of the Data Subject

Individuals have a number of rights as *data subjects* under the GDPR. The Data Subject Rights Policy and Procedure sets out how The Children's Trust helps data subjects exercise these rights and responds to requests from data subjects in accordance with the GDPR. This includes helping colleagues recognise when an individual is attempting to exercise their data subject rights, as this may not always be immediately obvious.

Under the GDPR, a *data subject* has the right to:

- **INFORMATION** about The Children's Trust's data collection and data processing activities (i.e. information about how we as a charity handle an individual's personal data – whether the individual be a patient, a visitor to our website etc.);
- **ACCESS** their own personal data (the **right of subject access**) (i.e. the individual has the right to obtain a copy of their personal data that we hold);
- **RECTIFICATION** (i.e. the individual can in certain circumstances request that we correct personal data which is inaccurate or out of date);
- **ERASE** personal data (the **right to be forgotten**) (i.e. the individual can in certain circumstances ask TCT to erase their personal data – so that he or she is 'forgotten');
- **RESTRICT** data processing (i.e. the individual can ask us to restrict the processing of their personal data in certain circumstances);
- **OBJECT** to data processing (i.e. the individual can object to our processing of their personal data in certain circumstances);
- **PORTABILITY** (i.e. the individual can ask to receive a copy of their personal data or for us to transfer their personal data to another data controller);
- **not** be subject to **AUTOMATED DECISION-MAKING** or **PROFILING** (i.e. the individual can ask us not to subject their personal data to automated decision-making / profiling). Automated decision-making and profiling must not be used in relation to a child;
- be **NOTIFIED** of a data security breach (i.e. the individual can expect that we notify him or her about a data security breach involving their personal data).

Data subjects also have the following rights:

- where our lawful basis for processing is “consent”, to withdraw consent at any time;
- to request a copy of an agreement under which personal data is transferred outside of the EEA;
- to prevent processing that is likely to cause damage or distress to the data subject or anyone else;
- to make a complaint to the supervisory authority. In the UK this is the Information Commissioner's Office.

IMPORTANT! You must immediately forward any data subject request you receive to your line manager and the DPO and comply with Data Subject Rights Policy and Procedure found on the Information Governance pages of The Loop.

6.4 Responsibilities of the Data Controller

6.4.1 Data Protection by Design and Default

At The Children's Trust we will ensure that by default we design and implement appropriate technical and organisational measures, commensurate with the level of risk to the data subjects, which satisfy the data protection principles. E.g. pseudonymisation which relates to the data protection principle of data minimisation.

6.4.2 Data Protection Impact Assessment

Data Protection Impact Assessments (DPIA) are a tool to help us identify and minimise the data protection risks of new projects or data processing activities. They are part of our accountability obligations under the GDPR, and an integral part of 'data protection by default and by design' approach. An effective DPIA helps organisations fully consider- and actively seek to mitigate the risks to personal data when designing and architecting new systems and data processing operations. It ensures problems are identified and fixed at an early stage and helps demonstrate compliance with data protection obligations; meet individuals' expectations of privacy and avoid reputational damage which might otherwise occur. In some cases, the GDPR mandates a DPIA, but they can be a useful tool in other cases too.

For more information about when a DPIA is needed and how it should be undertaken, see the Data Protection Impact Assessment Policy & Procedure.

6.4.3 Use of Data Processors

When engaging outsourced service providers and other suppliers to undertake data processing activities on our behalf, those third-party data processors must provide sufficient guarantees to implement appropriate technical and organisational measures and to comply with data protection regulations. You must consult the DPO before any new data processors are appointed or before any changes to existing data processing arrangements are made. This is to ensure the necessary safeguards, including the requisite contractual clauses, are in place.

6.4.4 Record of Processing Activities

The Children's Trust must maintain a record of its data processing activities in compliance with the GDPR. This will cover:

- the name and contact details of the data controller (TCT) and, where applicable, the joint controller, the controller's representative and the data protection officer;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, where applicable, the documentation of suitable safeguards;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures

All departments are required to support an annual 'information audit' to ensure the Record of Processing Activity is kept up to date. The DPO must be informed of any new processing activities or significant changes to existing processing activities as and when they are *planned*.

A record of data subjects' consents (where applicable) must be retained in accordance with our Record Retention and Disposal Policy.

6.4.5 Security of Processing

Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

- We will develop, implement and maintain safeguards appropriate to our size, scope and organisation, our available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable).
- We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.
- We will implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data.
- We will exercise particular care in protecting special categories of personal data from loss and unauthorised access, use or disclosure.
- Colleagues at The Children's Trust must follow all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction.
- The transfer of personal data to third-party service providers is only permissible if those third parties agree to comply with our policies and procedures including putting in place adequate measures, as requested.
- All colleagues must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

  (a) **Confidentiality** means that only people who have a need to know and are authorised to use the personal data can access it.
  (b) **Integrity** means that personal data is accurate and suitable for the purpose for which it is processed.
  (c) **Availability** means that authorised users are able to access the personal data when they need it for authorised purposes.

- All colleagues must comply with all applicable aspects of our data protection and information security policies and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect personal data.

6.4.6 Training and Compliance Monitoring

All colleagues (employees, volunteers and contractors) must undergo adequate training to enable them to comply with this policy, related sub-policies and all relevant data privacy laws.

- All colleagues must complete mandatory information governance induction training upon joining The Children's Trust and annually thereafter
- All colleagues must regularly review the systems and processes they use day-to-day to ensure they comply with this policy.

6.5 Personal Data Breach Notification

A personal data breach is a type of information security incident that carries particular regulatory obligations. These are security breaches that lead to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data, even if only temporarily.

The UK GDPR requires us to notify personal data breaches to the ICO without undue delay and, where feasible, **within 72 hours** of first awareness **if** they are likely to result in risks to people's rights and freedoms. If a notification is later it must be accompanied by an explanation for the delay.

Personal Data Breaches must also be notified to data subjects if the breach is "likely to result in a high risk" to the data subject's rights and freedoms. The ICO gives the accidental disclosure of patient records as an example of the type of data breach that would need to be notified to individuals.

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so. Information security incidents have the potential to significantly limit The Children's Trust's ability to function, and can damage its reputation.

IMPORTANT! If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO (dpo@thechildrenstrust.org.uk) by following the Data Breach Management Policy & Procedure. You should preserve all evidence relating to the potential personal data breach.

6.6 Sharing Personal Data

Generally, we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the personal data we hold with another employee, agent or representative of The Children's Trust if the recipient has a job-related need to know the information.

You may share patient information with other healthcare providers to facilitate safe and coordinated care, subject to strict rules and regulations, and individuals can object to their records being shared between services. You may only share the personal data we hold with third parties, such as NHS organisations, local authorities, partners and our service providers if:

- they have a need to know the information for the purposes of providing the contracted services;
- sharing the personal data complies with the privacy notice provided to the data subject and, if required, the data subject's consent has been obtained;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross border transfer restrictions; and
- a fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

Sharing Children's Data for Safeguarding Purposes

Data protection law allows you to share information when required to identify children at risk of harm and to safeguard them from harm. **Data protection law doesn't prevent you from doing this**. It simply helps you to share information in a fair, proportionate and lawful way. **It can be more harmful not to share information that is needed to protect a child or young person**.

Appropriate information sharing is central to effectively safeguarding children from harm and promoting their wellbeing. There have been many reviews of cases where children have died or been seriously harmed through abuse or neglect. The case reviews frequently identify gaps in information sharing as a factor contributing to failures to protect the children involved.

If there is an immediate risk of harm to a child, you should share the information that is **proportionate and necessary** to safeguard the child. Ideally, if time permits you should check with a line manager, the Named Nurse for Safeguarding or the Caldicott Guardian first but if that is not possible, go ahead and share.

Otherwise, when deciding whether to share personal data for safeguarding purposes follow these key steps:

- **Step 1**: Complete a risk assessment. When you are making a decision about sharing information about a child, it is very important to assess the risks. You can use the DPIA form to do this (see section 6.4.2). A DPIA can help you plan for the information sharing and assess and mitigate the risks to children's rights and freedoms. It helps you to ensure your sharing is done safely, lawfully and with accountability.

- **Step 2:** Be clear about transparency and individuals' rights (ref section 6.3). If you're sharing information for safeguarding purposes, you might not be obliged to allow people to exercise all these rights. For example, if giving access to a person to information you hold about them would be likely to cause serious harm to a child. There are exemptions and restrictions under the DPA 2018 that you may use in some circumstances to limit these rights. The DPA 2018 lists the exemptions relating to health, social work, education and child abuse, and the circumstances where they can be applied. This includes cases of information being processed by a court, requests made by someone with parental responsibility or in cases where compliance would be likely to cause someone serious harm. Be sure you know which exemption applies in each case before sharing. Seek advice from the DPO if in doubt.

- **Step 3:** Always share information following the seven data protection principles (see section 6).

- **Step 4:** Make sure you have identified the relevant lawful/ legal basis for sharing the information in each circumstance (see section 6.1.1)

6.7 Data Transfer Outside the UK

The UK GDPR restricts data transfers to countries outside the UK in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You may only transfer personal data outside the UK if one of the following conditions applies:

(a) the UK government has issued a decision confirming that the country to which we transfer the personal data ensures an adequate level of protection for the data subjects' rights and freedoms;

(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the UK government, an approved code of conduct or a certification mechanism,

a copy of which can be obtained from the DPO;

(c) the data subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the data subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent and, in some limited cases, for our legitimate interest.

Note, post-Brexit the UK government has ruled that transfers of data from the UK to the European Economic Areas (EEA) EA are permitted. The UK has issued a *partial* adequacy decision for transfers to the United States of America (further rules here: https://www.gov.uk/government/publications/uk-us-data-bridge-supporting-documents/uk-us-data-bridge-factsheet-for-uk-organisations).

If you are considering any third country transfers, please consult the DPO.

6.8 Data Quality General Principles

Data quality is a key part of any information system. Colleagues are responsible for timely and accurate record keeping and for preserving the confidentiality, integrity and availability of personal data. These obligations are enforced; legally under the Data Protection Act 2018, contractually under the contract of employment and TCT's policies and procedures and ethically under professional codes of practice across the various disciplines.

All staff should be aware of the importance of good data quality and their own contribution to achieving it, and The Children's Trust will endeavour to provide appropriate training in relation to the same.

Information Asset Owners also have an important role to play in ensuring that, where appropriate, systems are in place to validate the completeness, accuracy, relevance and timeliness of data/information.

6.9 Marketing

We are subject to certain rules and privacy laws when marketing to our supporters. Accordingly, we will only send electronic direct marketing (for example, by email, text or automated calls) with a data subject's consent. The right to object to marketing should be presented at the time of the first communication with the supporter, clearly and separately from any other information.

A data subject's objection to direct marketing should be actioned promptly by adding their name and email address or contact phone number (as applicable) to TCT's marketing suppression list. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

7 Related Policies and Procedures

The following procedures stated below support the effective application of this policy:

- Data Breach Management SOP
- Data Subjects Requests SOP
- Information Assets Management Policy & SOP
- Information Security Policy
- Record Retention & Disposal Policy & SOP
- Record Keeping Policy

8 External References and Guidance

The following external resources and guidance were consulted in drafting this policy:

- UK General Data Protection Regulation
- Data Protection Act 2018
- ICO website

9 Document Change Control

Version	Status	Description (of changes)	Reviewed by	Reviewed/ Issued Date
0.1	Draft	Change to new document format	IGC	09/2020
1.0	Final			11/2020
1.1	Final	Updated section 1 to reflect Brexit changes	OR	06/2021
2.0	Final	Changes to 4.14 to allow processing outside the EEA, but only where the UK has issued an adequacy decision.	OR	02/2024
2.1	Draft	Updated to include information from SOP including roles and responsibilities	OR	03/2025
3.0	Final	Approved	IGC	05/2025

Appendix 1 – Stakeholder Engagement Checklist

Review and complete the following checklist to indicate which stakeholders were consulted in the development of this policy.

#	Question	Yes/ No	Stakeholder(s) to be consulted
1	Is there a statutory requirement to have in place this particular policy/ does the policy need to comply with detailed legislation?	Yes	Audit, Risk and Governance team
2	Is implementation of the policy (or any element of it) dependent on the use of new or existing information technology?	No	Head of IT
3	Does implementation of the policy (or any element of it) place any demands on/ or affect the activities of the Estates and Facilities teams (e.g. does it impact the provision or maintenance of premises, equipment, vehicles or other TCT assets)?	No	Head of Estates
4	Does implementation of the policy or any element of it involve/ impact the processing of personal data?	Yes	Data Protection Officer
5	Does implementation of the policy require significant unbudgeted operational or capital expenditure?	No	Finance Director
6	Does implementation of the policy (or any element of it) directly or indirectly impact on the delivery of services / activities in other areas of the organisation? E.g. a policy written by a clinical lead in CF&S might impact on the delivery of care for CYP attending the School.	No	Relevant, impacted OLT members
7	Is there a need to consider Health and Safety or potential environmental impacts in developing and implementing the policy?	No	Health and Safety Manager
8	Have you consulted with a representative of those who will be directly impacted by the policy?	N/A	
9	Please detail any other stakeholder groups consulted, if applicable.	N/A	