Data Protection Policy

Lead Director Liz Sell, Director of Finance	**Date Reviewed** February 2023
Lead Author(s) Olivia Rowntree, Head of Audit Risk & Governance / Data Protection Officer	**Date Drafted** September 2020
Recommending Committee Information Governance Committee	**Endorsed Date** September 2020
Approval Body Audit & Risk Committee	**Ratified Date** February 2023
Published Date February 2023	**Next Review Date** February 2024

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. It's main objective being to ensure organisational-wide compliance with all relevant data protection legislation.

UK Legislative Framework

Data protection law in the UK has changed significantly over the last few years and more recently post-Brexit. 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 is a UK law which came into effect on 1st January 2021 at the end of the Brexit transition phase. It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies. It is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679) which applied in the UK before that date, with some changes to make it work more effectively in a UK context.

The DPA 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018. It was amended on 1st January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU. It sits alongside and supplements the UK GDPR - for example by providing 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 could lead to fines of up to €20m or 4% of turnover. 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

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 a:

- Data Protection Officer (Head of Audit Risk & Governance)
- Senior Information Risk Officer (Chief Executive)
- Caldicott Guardian (Medical Director)

4.2 The Data Protection Officer's (DPO's) duties shall include all those mandated under prevailing data protection legislation, including responsibility for the development and ongoing review and maintenance of this policy, all related sub-policies and procedures required under the UK GDPR/ DPA 2018 and for ensuring there is adequate training and compliance monitoring across the organisation to support the implementation of the same.

4.3 An Information Governance Committee (IGC) shall be established to oversee the ongoing programme of compliance activity and to provide assurance to the Audit & Risk Committee that control measures are designed and operating effectively.

4.4 Mandatory information governance training shall be developed and implemented in line with regulatory requirements and/ or statutory guidance. The training shall be delivered with such frequency as is required by the relevant regulatory authorities and compliance will be monitored and reported to the Audit & Risk Committee via the Information Governance Committee.

4.5 All data processing undertaken by TCT will comply with the data protection principles of; lawfulness, fairness and transparency; purpose limitation; data minimisation, accuracy; storage limitation; confidentiality integrity (and availability) and accountability.

4.6 The DPO shall develop and keep up to date a privacy policy which complies with the requirements of the UK GDPR/ DPA 2018, shall be published on TCT's external website and made accessible to data subjects when they share their data with TCT.

4.7 The DPO shall develop and maintain a record of TCT's data processing activities in accordance with the UK GDPR/ DPA 2018.

4.8 The DPO shall develop a policy and process to ensure that data subjects' rights are upheld in line with data protection legislation and that statutory timeframes for responding to data subject requests are met.

4.9 The Charity will adopt a risk-based approach to the design, development and implementation of appropriate organisation and technical measures in order to preserve the confidentiality, availability and integrity of personal data.

4.10 In line with data protection legislation, TCT shall adopt the principle of "privacy by design" ensuring that information security requirements are defined at the earliest stage of any process to procure, develop or modify IT software which will be used for data processing purposes.

4.11 The DPO will ensure that prior to any high risk data processing being undertaken, there is a policy and procedure in place to ensure that a Data Protection Impact Assessment (DPIA) is satisfactorily completed.

4.12 When engaging data processors to process personal data on TCT's behalf, suitable contractual agreements/ clauses, as required under data protection legislation, are put in place and agreed before processing commences.

4.13 The DPO will ensure that there is a policy and process in place for reporting and investigating data breaches and for assessing whether they require notification to the supervisory authority. The Data Protection Office shall be the designated point of contact with the supervisory authority (ICO). However, all decisions to notify the ICO, or the affected data subjects, shall require the prior approval of the SIRO and Chief Executive. No other staff member shall be authorised to make statutory data breach notifications to any regulator or data subject.

4.14 All data processing (including that undertaken by cloud-service providers and other suppliers) must take place within the EEA and ideally within the UK to avoid complicated contractual arrangements and additional administrative compliance burden. Any exceptions to this policy must be discussed with the DPO and approved by the IGC.

4.15 A policy and procedure shall be developed, implemented and maintained to ensure high standards of record keeping and data quality, particularly across the clinical areas to support high quality, timely and safe care.

5 Stakeholder Consultation

Appendix 1 details the stakeholders who were consulted in the development of this policy.

6 Related Policies and Procedures

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

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

7 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

8 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

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	