Data Protection Policy

1. Introduction

1.1 Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2018 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

1.2 Definitions used (mainly drawn from the GDPR)

Material scope (Article 2) **–** the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) **–** the GDPR applies to all controllers that are established in the UK who process the personal data of data subjects, in the context of that establishment.

Establishment **–** the main establishment of the Data controller in the UK is the place in which they make the main decisions as to the purpose and means of its data processing activities, e.g. head office.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of 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.

Data controller – The legal entity who determines the purposes and means of the processing of personal data, i.e. the charity. Referred to as 'controller' in this document.

Data processor – Any organization processing data on behalf of a Data Controller.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling **–** is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behavior. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach **–** 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. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent **-** 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.

Child **–** the UK GDPR defines a child as anyone under the age of 13 years old. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

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.

ICO – information commissioner's office – The organization responsible for the enforcement of GDPR and where data breaches are reported.

2. Policy statement

2.1 The Trustees and management of Cancer52 are committed to compliance with all relevant law in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information Cancer52 collects and processes in accordance with the General Data Protection Regulation (GDPR).

2.2 Compliance with the GDPR is described by this policy and other relevant policies such as the Information Security Policy along with connected processes and procedures.

2.3 The GDPR and this policy apply to all personal data processing functions, including those performed on beneficiaries, volunteers, staff, suppliers and partners personal data, and any other personal data the organisation processes from any source.

2.4 The Board of Trustees is responsible for reviewing the personal data audit annually in the light of any changes to activities and to any additional requirements identified by means of data protection impact assessments.

2.5 This policy applies to all those doing work for Cancer52, including staff, volunteers, and suppliers. Any breach of the GDPR or this Policy may be dealt with under the disciplinary policy.

2.6 No third party may access personal data held by Cancer52 without having first entered into a data confidentiality agreement, which imposes on the third-party obligations no less onerous than those to which The charity is committed, and which gives the right to audit compliance with the agreement.

3. Responsibilities and roles under the General Data Protection Regulation

3.1 Cancer52 is a Data Controller under the GDPR.

3.2 The Trustees are responsible for the implementation and maintenance of effective policy and process to ensure compliance with the GDPR.

3.3 The Board of Trustees has overall responsibility and accountability for the management of personal data and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

3.3.1 Development and implementation of the GDPR as required by this policy,

3.3.2 Information security and risk management in relation to compliance with the policy.

3.4 Compliance with data protection legislation is the responsibility of all Staff, Contractors and Volunteers of the charity.

3.5 Staff will receive training in data protection and use of personal data on appointment and update training annually.

3.6 Staff and volunteers are responsible for ensuring that any personal data about them and supplied by them to the charity is accurate and up-to-date.

4. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR.

4.1 Personal data must be processed lawfully, fairly and transparently

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

The specific information that must be provided to the data subject must, as a minimum, include:

4.1.1 the identity and the contact details of the controller and, if any, of the controller's representative;

4.1.2 the contact details of the Chair of the Board of Trustees;

4.1.3 the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

4.1.4 the period for which the personal data will be stored;

4.1.5 the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;

4.1.6 the categories of personal data concerned;

4.1.7 the recipients or categories of recipients of the personal data, where applicable;

4.1.8 where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;

4.1.9 any further information necessary to guarantee fair processing.

4.2 Personal data can only be collected for specific, explicit and legitimate purposes

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of the charity's GDPR register of processing.

4.3 Personal data must be adequate, relevant and limited to what is necessary for processing

4.3.1 The Board of Trustees is responsible for ensuring that The charity does not collect information that is not strictly necessary for the purpose for which it is obtained.

4.3.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be include a fair processing statement or link to privacy statement and approved by the Data Protection Officer.

4.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

4.4.1 Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

4.4.2 The Board of Trustees is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

4.4.3 It is also the responsibility of the data subject to ensure that data held by The charity is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

4.4.4 The Board of Trustees is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

4.4.5 The Board of Trustees is responsible for responding to requests for rectification from data subjects within one month. This can be extended to a further two months for complex requests. If the charity decides not to comply with the request, the Board of Trustees must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

4.4.6 The Board of Trustees is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

4.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

4.5.1 Where personal data is retained beyond the retention date for a legitimate business reason, it will be minimised and pseudonymised in order to protect the identity of the data subject in the event of a data breach.

4.6 Personal data must be processed in a manner that ensures the appropriate security

The Board of Trustees will carry out a risk assessment, using the DPIA procedure, which is available here taking into account all the circumstances of the charity's controlling or processing operations.

In determining appropriateness, the Board of Trustees should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or beneficiaries) if a security breach occurs, the effect of any security breach on the charity, and any likely reputational damage including the possible loss of public trust.

Organisational measures include following:

- Appropriate training
- Checking the reliability of employees and contractors (such as references etc.);
- Data protection in employment contracts;
- Monitoring of staff for compliance with relevant security standards.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

4.7 The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

The charity demonstrates compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design DPIAs, breach notification procedure and incident response plan.

5. Data subjects' rights

5.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:

5.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.

5.1.2 To prevent processing likely to cause damage or distress.

5.1.3 To prevent processing for purposes of direct marketing.

5.1.4 To be informed about the mechanics of automated decision-taking process that will significantly affect them.

5.1.5 To not have significant decisions that will affect them taken solely by automated process.

5.1.6 To sue for compensation if they suffer damage by any contravention of the GDPR.

5.1.7 To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.

5.1.8 To request the supervisory authority to assess whether any provision of the GDPR has been contravened.

5.1.9 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

5.1.10 To object to any automated profiling that is occurring without consent.

5.2 The charity ensures that data subjects may exercise these rights:

5.2.1 Data subjects may request access to their data in a way that complies with the requirements of the GDPR.

5.2.2 Data subjects have the right to complain to The charity related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled.

	Supervisory authority contact details	**Data Protection Representative contact details**
Contact Name:	Information Commissioner's Office	Jonathan Pearce Chair, Board of Trustees
Address line 1:	Churchill House	c/o Teenage Cancer Trust
Address line 2:	17 Churchill Way	93 Newman Street
Address line 3:	Cardiff	London
Address line 4:	CF10 2HH	W1T 3EZ
Email:	casework@ico.org.uk	jonathan.pearce@cancer52.org.uk
Telephone:	029 2067 8400	

6. Consent

6.1 The charity understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

The charity understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

6.2 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation.

6.3 For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

6.4 Where the data subject is a child, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16 (to be confirmed once legislation is enacted).

7. Security of data

7.1 All Staff, Contractors and Volunteers are responsible for ensuring that any personal data that they are responsible for is kept securely and is not, under any conditions, disclosed to any third party unless that third party has been specifically authorised to receive that information and has entered into a confidentiality agreement.

7.2 Personal data shall be accessible only to those who have a legitimate requirement to use it. Who has access to what will be determined by the DPIA covering the relevant business process.

7.3 All personal data shall be held securely.

7.4 All personal data should be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected; and/or
- stored on (removable) computer media which are encrypted.

8. Disclosure of data

8.1 Personal data shall not be disclosed to unauthorised third parties such as; family members, friends, government bodies, and in certain circumstances the Police. All Staff shall exercise caution when asked to disclose personal data to a third party. There must be a legitimate business reason for the transfer and appropriate NDA or Data processor agreements in place.

9. Retention and disposal of data

9.1 The charity will not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

9.2 Data may be stored for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

9.3 Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the “rights and freedoms” of data subjects.

10. Data transfer outside the UK

10.1 Cancer52 is a UK only charity and does not transfer personal information, as defined by the GDPR, outside of the UK.

10.2 In the exceptional circumstance that such a transfer is being contemplated, explicit, written, agreement must be obtained from the trustees, who must be assured that all requirements of the GDPR are met, particularly in the contract between the charity and the relevant 3rd party.

11. Risks associated with the processing of personal data

11.1 The charity is aware of any risks associated with the processing of particular types of personal data.

11.1.1 The level of risk to individuals associated with the processing of their personal data is assessed. Data protection impact assessments (DPIAs) are carried out in relation to the processing of personal data by The charity, and in relation to processing undertaken by other organisations on behalf of the charity.

11.1.2 Any risks identified by the risk assessment are actively managed in order to reduce the likelihood of a non-conformance with this policy.

11.1.3 Where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing, a DPIA will be undertaken to assess the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks. The DPIA must be signed off by the Board of Trustees before processing commences.

11.1.4 Appropriate controls will be selected and applied to reduce the level of risk to an acceptable level, in line with the charity's risk policy and the requirements of the GDPR.

12. Document Owner and Approval

The Board of Trustees is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.