|  |
| --- |
| Data Protection Policy |

|  |  |
| --- | --- |
| Policy Name | Data Protection Policy |
| Summary of Policy  | Teenage Cancer Trust is committed to respecting and protecting personal data of all individual who come in to contact with us, including staff, funded staff, job applicants, young people with their friends and family, volunteers, policy-makers, our supporters, potential supporters and other key stakeholders, We are honest, open and transparent about why we are collecting personal data and we always ensure that we are collecting and using personal data in accordance with the data protection laws, regulations and best practice.  |
| Policy Owner | Head of Fundraising Standards and Operations |
| Date of Issue | January 2022 |
| Review Date | January 2024 |
| Date of Next Review |  |
| Policy Type as per Policy Management Frameworkie one of the following:* *Policies linked to strategic risk and compliance requiring Board Sign off*
* *Operating Policies*
* *Staff Policies*
 | Operating Policy |
| Policy Type as per Policy Central | Data, All Policies |
| Key Audience | All staff, volunteers, trustees |
| Approved By (Director / Deputy Director) | Deputy Director, Supporter Experience and Engagement |
| RACI for Policy:* Responsible
* Accountable
* Consulted
* Informed
 |  |

|  |
| --- |
| **Policy Title** |

**CONTENTS**

1. **Policy Statement (to include purpose, overview and audience)**
2. **Principle of Policy (Data Protection Training and Resources)**
3. **GDPR principles**
4. **Individuals’ rights**
5. **Sensitive/special category data**
6. **Personal Data Breaches**
7. **Children and Data Protection**
8. **Sharing personal data**
9. **Other relevant policies and procedures (internal)**
10. **Relevant regulatory policies and guidelines (external)**
11. **Appendices (including key definitions)**
12. **Policy Statement**

Data protection is about safeguarding the fundamental right to privacy, which is enshrined in laws and regulations. Teenage Cancer Trust is committed to respecting and protecting **personal data** of all individuals who come in contact with us, including staff, funded staff, job applicants, young people with their friends and families, volunteers, policy-makers, our supporters, potential supporters and other key stakeholders. We are honest, open and transparent about why we are collecting personal data and we always ensure that we are collecting and using personal data in accordance with the data protection laws, regulations and best practice including the **General Data Protection Regulation (GDPR) and the UJ Data Protection Act (2018).**

Everyone within Teenage Cancer Trust will handle personal data at some stage in their role and it is therefore essential that we all understand the basic principles of data protection and our responsibilities in this regard.

Teenage Cancer Trust is committed to compliance with the EU General Data Protection Regulation

(“GDPR”), the UK Data Protection Act 2018 (“DPA”) and all other relevant laws in respect of personal data and the protection of the rights and freedoms of individuals whose information Teenage Cancer Trust collects and processes. Compliance with the GDPR is described by this policy and those policies and procedures listed below. Failure to ensure that the processing of personal data complies with legislation risks enforcement action, even prosecution, and compensation claims from individuals. There are also potentially serious reputational risk issues.

This policy is applicable to everyone within Teenage Cancer Trust regardless of location or role. It applies to all employees, affiliates, volunteers, consultants or representatives of Teenage Cancer Trust who require access to Teenage Cancer Trust servers and platforms in order to perform their functions

1. **Principle of Policy (Data Protection Training and Resources)**

Teenage Cancer Trust is committed to ensuring that all staff understand their obligations and responsibilities in connection with handling personal data. Data Protection Training is available and compulsory for **all** staff regardless of location within Teenage Cancer Trust. If you have any questions regarding data protection you should email the Data Protection Leads dataprotection@teenagecancertrust.org in the first instance.

1. **GDPR Principles**

The GDPR is underpinned by a number of data protection principles which drive compliance and set out the main responsibilities of organisations. These principles are listed below and can be easily adhered to by following the do’s and don’ts of each principle.

|  |
| --- |
| **Principle 1**: **Lawfulness, fairness and transparency**  |
|  **Definition**:  *Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.*   |
| **J**  | * When collecting personal data, make sure you tell supporters and other stakeholders how their data will be used. **Be open and honest** about who we are and why we are collecting their data, the GDPR is much more specific about this requirement. This can be achieved by presenting them with our [Privacy Policy](https://www.teenagecancertrust.org/about-us/privacy-policy) at the earliest convince.
 |
| * **When you want to use personal data for marketing communication in the future, including our e-newsletter, always make sure you obtain consent** (opt-in) when collecting personal data and **be transparent**about how we intend to use it. Consent/opt-in must be freely given, specific and informed and we must be keep a record of the consent given on an individual’s record onto our organisational database, CARE.
 |
|   |
| * Use one of Teenage Cancer Trust's [Data Protection statements](https://teenagecancertrust759.sharepoint.com/%3Aw%3A/s/FundraisingStandardsandOperationsTeams/EQ9QxxeLi2BJiSm-1JQicbABHCKdEJM2bJy1uRl-k31iFQ?e=yJAkxo) when asking for consent (opt-in). Please speak to our Data Protection Leads at dataprotection@teenagecancertrust.org if the consent you need is not covered by the statements.
* We must have a valid lawful reason for processing and using an individual’s personal data. Please refer to the [Lawful Basis for Processing Personal Data Process map](https://teenagecancertrust759.sharepoint.com/%3Ab%3A/s/FundraisingStandardsandOperationsTeams/EUIm507UYohEj5JTYDslMM8B-bK-dNc7eltEnXW_mgKHuw?e=WeK8fv) to confirm that you have a lawful basis for processing an individual’s personal data, **this is very useful! If you are still unsure, please contact our Data Protection Leads to discuss.**
* If you have determined that you will use legitimate interest as your lawful basis for processing data for Direct Marketing (DM) purposes via post and telephone, you will need to work with the Data Protection Leads to complete a [Legitimate Interest Assessment Form](https://teenagecancertrust759.sharepoint.com/%3Aw%3A/r/sites/BackstageFundraising/_layouts/15/Doc.aspx?sourcedoc=%7B011EEF29-914C-429E-9C3E-B285D63E81F9%7D&file=Legitimate%20Interest%20Assessment.docx&action=default&mobileredirect=true) prior to processing any personal data.
* Always speak to the Data Protection Leads when planning a group communication, including those to cold contacts/non-supporters, they can be contacted via dataprotection@teenagecancertrust.org.  The Data Protection Leads are responsible for ensuring our compliance with Data Protection laws and regulations and they must be satisfied that all planned activities involving our supporters, key stakeholders, potential supporters and the general public are carried out fairly and lawfully and we have a valid basis for processing personal data.
 |
| * **Always treat other people's data in the same way you would like your own data to be treated!**
 |
| **L**   | * Never collect and/or use personal and/or sensitive data without having a lawful reason to do so. N.B.  You don’t need an explicit consent to send administrative communication, for example to send a thank you letter for a donation which has been received or to make a phone call to your supporter about their upcoming event but you need it for sending any type of marketing communication, including our e-newsletter. For more information, refer to the [Lawful Basis for Processing Personal Data Process Map.](https://teenagecancertrust759.sharepoint.com/%3Ab%3A/s/FundraisingStandardsandOperationsTeams/EUIm507UYohEj5JTYDslMM8B-bK-dNc7eltEnXW_mgKHuw?e=WeK8fv)
 |
|   |

|  |
| --- |
| **Principle 2**: **Purpose Limitations**  |
|  **Definition**:*When collecting personal data, this must be done so for specified, explicit and legitimate purposes and individuals must be aware of how we will process their personal data.*   |
| **J**  | * Make sure you always have a specific reason for collecting data and use this data for the specified purpose only, for example, an individual signs up to volunteer at the RAH, we can then only use their data to contact them about that opportunity and our volunteering programme.
 |
| * Make sure the individual is aware of the purposes for which their data will be used and always refer them to our [Privacy Policy](https://www.teenagecancertrust.org/about-us/privacy-policy) on our website when collecting their data. This ensures we are transparent about personal data use and individuals feel informed.
 |
| * Ensure you add the correct suppressions onto the individual’s record on our organisational database, CARE, using the information provided by the individual with regards to how they would like to be contacted in the future.
* Speak to the Database team if you are unsure how the suppressions should be used – they will be happy to help and offer any additional training that might be needed.
 |
| **L**   | * Never collect data that is irrelevant 'just in case it might be useful’; this is illegal.
 |
| * Never use personal data in any other way than agreed with the individual when their data was collected (see: [Data Protection statements](https://teenagecancertrust759.sharepoint.com/%3Aw%3A/s/FundraisingStandardsandOperationsTeams/EQ9QxxeLi2BJiSm-1JQicbABHCKdEJM2bJy1uRl-k31iFQ?e=PHEhyy), our [Privacy Policy](https://www.teenagecancertrust.org/privacy-policy-and-cookies) and [Lawful Basis for Processing Personal Data Process Map](https://teenagecancertrust759.sharepoint.com/%3Ab%3A/s/FundraisingStandardsandOperationsTeams/EUIm507UYohEj5JTYDslMM8B-bK-dNc7eltEnXW_mgKHuw?e=WeK8fv).)
 |

|  |
| --- |
| **Principle 3**:  **Data Minimisation**  |
|  **Definition**: *We are only allowed to hold adequate and relevant data on an individual’s record and limited this to what is necessary in relation to the purposes for which they are processed.*   |
| **J**  | * Only collect and store the amount of personal data you need to fulfil the specified purpose.
 |
| * Ask yourself the question 'Do I really need all this data?' when working on forms and surveys to avoid collecting excessive data.
 |
| **L** | * Never ask for personal data which is not relevant to the purpose of collecting the data and therefore not needed, for example is someone’s date of birth essential to your data processing purpose?
* Never use data collected for one purpose for another purpose without asking for further consent.
 |

|  |
| --- |
| **Principle 4**:  **Accuracy**  |
|  **Definition**: *We are responsible for making sure that all personal data we store on our database(s) is kept up to date and accurate.*   |
| **J**  | * Update records when changes occur without delay.
 |
| * If data is manually added or amended on the database, make sure that all details are recorded correctly and accurately.
 |
| * Keep personal records as up to date as possible.
* If personal data is recorded in more than one place, for example on the organisational database CARE and in a document on your team’s site on Sharepoint with a personal data tag, ensure that all sources of data are kept up to date. NB. Data should be stored outside CARE only in exceptional circumstances.
 |
| **L**  | * Never knowingly use out of date and/ or inaccurate data.
* Refrain from recording subjective or personal comments about individuals on the database or anywhere else, for example: 'She is a really lovely lady' or 'She is very rude and unpleasant'.  Those are your personal opinions not facts, therefore this data is inaccurate.
 |
|   |

|  |
| --- |
| **Principle 5**:  **Storage Limitation**  |
| **Definition**: *Personal data should never be kept for longer than necessary.*  |
| **J**  | * Personal data will only be kept for as long as specified in the [Personal Data Retention Policy](https://teenagecancertrust759.sharepoint.com/%3Ab%3A/s/BackstagePolicyCentral/EWCeQZrE_81HqcY5xz8zVrwBLZ9pzXO6JPeNAlQ5tNqffA?e=UrZ84i). This policy must be followed in order to ensure we are compliant with personal data regulations under the GDPR.
 |
| * Shred/ securely dispose of any data that is no longer needed.
 |
| **L** | * Never keep data 'just in case it might be needed later', we only retain personal data when we have a need to keep it.
 |

|  |
| --- |
| **Principle 6**:  **Integrity & Security**  |
| **Definition**:*We must ensure that we have the appropriate security measures in place to prevent the personal data we hold from being accidentally or deliberately compromised; including unlawful processing, accidental loss, destruction of, or damage to.*  |
| **J**  | * Always adhere to the [IT Policy](https://teenagecancertrust759.sharepoint.com/%3Ab%3A/s/BackstagePolicyCentral/EVMHNm4QHiVDqhSLCb6it1MBj6ojamOkWi32p1hDhnJHaw?e=eoQY8O) for Acceptable Use when handling personal data.
 |
| * Ensure any third party suppliers who handle and/or process data on our behalf, sign and adhere to the [Data Security Agreement (DSA)](https://teenagecancertrust759-my.sharepoint.com/%3Aw%3A/g/personal/rebecca_dobbie_teenagecancertrust_org/EQBB9mgm4JRPk5lrvl-8pF8B4v01mj18q715m_2q0nlD1Q?e=BdPVVX) and/or [Non-Disclosure Agreement (NDA](https://teenagecancertrust759-my.sharepoint.com/%3Aw%3A/g/personal/rebecca_dobbie_teenagecancertrust_org/EfS5D_sJZiVMtkTuH5WkucUBcUHYE8etBjt1bX4wc7omJw?e=bnrve6)).
 |
| * Refer to the [Framework and guidance for working with young people](https://teenagecancertrust759.sharepoint.com/%3Ab%3A/r/sites/BackstageHR/Shared%20Documents/Framework%20and%20guidance%20for%20working%20with%20young%20people.pdf?csf=1&web=1&e=ZaQbn0)when making a decision about sharing young people's data with third parties.
* When sending data electronically, make sure that you do this in a secure manner, for example as a zipped and password protected file or using a SFTP (Secure File Transfer Protocol) site.
* Aim for all personal data to be stored on the organisational database CARE. If, for any reason, you need to store personal data outside CARE, e.g. CARE extracts, this needs to be stored on Sharepoint.
* If personal data has to be stored on a shared spreadsheet, ensure this is password protected and the password is only shared with those who need to access it.
* Shred/delete/securely dispose of documents containing personal data when no longer needed.
* Keep securely locked any paper documents containing personal and/or sensitive data.
* Carry out identification checks before giving out information about individuals.
* When sending e-mails or post ensure you are sending them to the correct person.
* Always use Special Next Day Delivery when sending documents containing personal or sensitive data via post.
* When making outgoing phone calls, make sure you are speaking to the right person before giving out any information.
* Make sure that passwords you use to access websites storing personal data are secure and kept safe.
* If you become aware of any data breaches or potential data breaches**,**please refer to the [Personal Data Breach Procedures](https://teenagecancertrust759-my.sharepoint.com/%3Aw%3A/g/personal/helen_harris_teenagecancertrust_org/EduAa0t7m6RAi9zwucCBdRABoMg59ygwZRZ_5WoyWukgpQ?e=pOayOt)**immediately**for the appropriate next steps to take. The incident will need to be reported on the Incident Reporting Log on the Intranet, flagged as ‘Data Protection’ so that the Data Protection Leads are notified., The designated DP Lead will investigate the incident and will decide on the appropriate course of action within 72 hours and notify the authorities and affected individuals, if deemed required under the circumstances.
 |
| **L** | * Never leave any documents containing personal data laying around in the London office or your home office, this includes your desk and printers.
* Never send personal data via e-mail in files that are not encrypted (e.g. password protected).
* Aim to not carry with you any documents containing personal data outside of the London office or your home office; if this is absolutely necessary, take extra precautions, such as not leaving the documents unattended, making sure that you carry them in a securely closed folder/bag etc.
* Never disclose personal information to third parties without permission from the individual concerned.
* Never share passwords you use to access websites storing personal data.
* Never transfer data to another country without prior approval from the Data Protection Leads (dataprotection@teenagecancertrust.org)
 |

|  |
| --- |
| **Principle 7**:  **Accountability and Governance**  |
|  **Definition**: *Teenage Cancer Trust shall be responsible for, and be able to demonstrate, compliance with the principles.*   |
| **J**  | * Remember that we are **all** responsible for keeping personal data secure and processing it in a lawful manner.
* Ensure that you are clear on the [organisational roles and responsibilities](https://teenagecancertrust759.sharepoint.com/%3Aw%3A/s/teamsites/teams/fundraising/fundraising_operations/ESFCyiAEktBAsjhvw4YkqYoBlOEURuDIsmV16QbUgrS1qA?e=8AfKIj) around Data Protection, including Data Protection Leads and Data Protection Officer.
* If you are unsure of anything, always flag with our Data Protection Leads, so they can offer advice or additional training for you or your team.
 |
|   |

1. **Individuals’ Rights**

Personal data remains the property of the individual about whom the data is about and they hold a number of enhanced rights which organisations need to recognise and act upon, including the right to object to processing their data and the right to access what personal information is held by the data controller.

|  |
| --- |
| **Right to be informed**  |
| * Individuals have the **right to be informed** about the collection and use of their personal data. We must provide them with information on our purposes for collecting and processing their personal data, our retention period for personal data and who it will be shared with. This is called privacy information and we make it available to individuals in our [Privacy Policy](https://www.teenagecancertrust.org/about-us/privacy-policy), available on our website, which must be provided to individuals at the time we collect their personal data.
 |
| **Right of access**  |
| * Individuals have a **right of access** to their personal data and any additional supplementary information (emails, spreadsheets etc.) If an individual requests to see all the information we hold about them, contact the DP leads on dataprotection@teenagecancertrust.org immediately so they can start dealing with the request without any delays. Refer to the [Subject Access Request](https://teenagecancertrust759.sharepoint.com/%3Aw%3A/s/FundraisingStandardsandOperationsTeams/EeUHOIApvvpKix7hifz17MMBednuSkTmi1o9wVNjW72u7g?e=RaM5Z9) procedures for details on how to recognise and manage the request.
* Remember that any comments or notes you record on the individuals' record on the organisational database CARE, HR system, e-mails or similar, will need to be disclosed to the individual when a Subject Access Request is made.
 |
| **Right to rectification**  |
| * Under GDPR, the **right to rectification** gives individuals the right to have inaccurate personal data which we hold rectified or completed if it is incomplete. If an individual informs us that information we hold on one of our databases is incorrect or incomplete, this must be amended
 |
| **Right to erasure**  |
| * Individuals have the **right to be forgotten**, meaning we must be able to delete all of their personal data from our organisational databases and documents on Sharepoint and shared drives.
* If an individual requests to ‘be forgotten’ or erased (deleted) from our systems, contact the Data Protection Leads on dataprotection@teenagecancertrust.org immediately so they can start dealing with the request without any delays.
* Please refer to [The Right to Erasure Policy](https://teenagecancertrust759.sharepoint.com/%3Aw%3A/s/BackstagePolicyCentral/EYmCAG-iWYtEuJv45fXBYyEBctcXpj1EKZS38dzVua45dw?e=AZ63Id) on the intranet to familiarise yourself with the process and for more information.
* Never ignore the request to be forgotten; if you are unsure if this is what the individual is asking for – speak to the Data Protection Leads.
 |
| **Right to restrict processing**  |
| * Don’t forget that individuals can limit the way that an organisation uses their data as well as put restrictions on how it is processed, under GDPR this is the **right to restrict processing**.
* Do not process an individual’s data if they have exercised their **right to restrict processing**, there are however a few exceptions to this, which include a legal basis for processing.
 |
| **Right to object**  |
| * Never ignore a request from an individual who requests for their data not to be used for direct marketing purposes. The **right to object** gives individuals the absolute right to object to this processing and we must make people aware of their right to object by including an unsubscribe link or opt out wording on all communications.
* Don’t forget to update the individual’s contact preferences - suppressions onto their record on CARE, as/when requested by them
 |
| **Rights related to automated decision making including profiling**  |
| * Individuals have the right to not be subjected to any **automated decision making** on their data, an example of this is large scale data **profiling**. As we may do data profiling from time to time, we inform about it in our [Privacy Policy](https://www.teenagecancertrust.org/about-us/privacy-policy) and we advise individuals they can opt out, if they wish to.
 |

1. **Sensitive/Special Category Data**

Special category (also referred to as sensitive) personal data is personal data which relates to an

individual (highlighted in bold the data that Teenage Cancer Trust would most commonly collect):

* Racial or ethnic origin
* Political opinion or trade union memberships
* Religious beliefs
* Genetics or biometrics
* **Physical or mental health condition**
* Sexual life/sexual orientation

An individual’s criminal background is treated the same way as GDPR special category data under the DPA.

In order to lawfully process special category data, you must identify both a lawful basis under

Principle 1 **and** also identify a separate condition for processing special category data under Article 9.

In order to process special category data, we will usually need to rely on one of the following grounds:

1. Explicit consent of the individual;

2. Necessary to comply with our obligations and rights in the field of employment and social

security;

3. The relevant information has already manifestly been made public.

Less commonly, we may seek to rely on:

1. Processing is necessary in connection with a legal claim;

2. Processing is necessary to protect the vital interests of the individual.

There are other conditions in Article 9 but these relate to information being necessary for the

substantial public interest, reasons of occupational health or public interest in the sphere of public

health or scientific/historical research purposes and it is therefore highly unlikely that Teenage Cancer Trust would be able to establish one of these conditions.

1. **Personal Data Breaches**

In a large organisation there will be occasions whether personal data is unlawfully or

accidentally deleted, lost, altered without permission or disclosed or accessed by those who were not authorised to see or access the information. This is defined as a personal data breach. It will cover a huge variety of incidents such as:

★ accidentally emailing a supporter’s details to the wrong email address;

★ paper consent forms being misplaced;

★ a laptop being stolen which contained personal data;

★ a supplier notifying us that their systems have been unlawfully accessed;

★ the Teenage Cancer Trust system or network being hacked;

★ incorrect access being given to staff members of a document or database containing sensitive

personal data. Teenage Cancer Trust has in place a Data Breach Incident Response Plan to respond with Personal Data Breaches.

The key message for all staff members is that you **must** notify using Incident Reporting **immediately** once you become aware of a breach. This is because if we are required to notify the Information Commissioner’s Office we need to do so without undue delay and if possible within 72 hours of becoming aware of the breach. We therefore have a very short timeframe

If you become aware of any data breaches or potential data breaches**,**please refer to the [Personal Data Breach Procedures](https://teenagecancertrust759-my.sharepoint.com/%3Aw%3A/g/personal/helen_harris_teenagecancertrust_org/EduAa0t7m6RAi9zwucCBdRABoMg59ygwZRZ_5WoyWukgpQ?e=pOayOt)**immediately**for the appropriate next steps to take. The incident will need to be reported on the Incident Reporting Log on the Intranet, flagged as ‘Data’ so that the Data Protection Leads are notified., The designated DP Lead will investigate the incident and will decide on the appropriate course of action within 72 hours and notify the authorities and affected individuals, if deemed required under the circumstances

1. **Children and Data Protection**

Where we are relying upon consent as the ground for processing the personal data of children, only those children aged over 13 may consent (in the UK - this may be 16 in other EU jurisdictions). At Teenage Cancer Trust we assume anyone under 18 is a child for Data Protection purposes and therefore we will need the consent of the individual with parental responsibility for the child and reasonable steps must be taken to verify this.

1. **Sharing Personal Data**

Personal data (including basic information such as names) must not be shared with any third party

outside of Teenage Cancer Trust (including contractors, suppliers, donors etc) without a contract being put in place and assurance that the third party has appropriate technical and organisational measures in place to safeguard the personal data. Template contracts have standard GDPR compliant data protection clauses for inclusion in your contracts. Please email dataprotection@teenagecancertrust.org if any queries.

1. **Other relevant policies and procedures**

Data Breach procedures

Personal Data Retention Policy

Special Category Data Appropriate Policy

The Right to Erasure Policy

Appendix 1: Key Definitions

|  |  |
| --- | --- |
| **Anonymisation** | A method of modifying Personal Data so that there is no connection of that data with an individual. If anonymisation is used so the individual cannot be identified at all then GDPR does not apply *e.g. a fully anonymous survey with no identifiable factors.*However, if the Data Controller can use or restore the anonymisedinformation to identify individuals this is still classified as Personal Dataunder GDPR *e.g. a spreadsheet which contained personnel numbers only and no names would still be considered Personal Data if Teenage Cancer Trust is able to use the HR System together with the spreadsheet to identify individuals. This is not effective anonymisation.**Similarly, an anonymous survey which asked individuals to include details of their team, age, location would not be effective if a specific individual could be identified using this and other information held.* |
| **Categories of Data****Subject** | Within Teenage Cancer Trust we have identified the following categories of data subjectabout whom we may process personal data:1. Attendees of conference/meetings2. VIPs3. Young People4. Contractors/Consultants5. Employees6. Former Employees7. Journalists8. NHS staff9. Suppliers10. Supporters11. Trustees, and Board Committee Members who are not Trustees12. Visitors13. Volunteers |
| **Data Breach** | A breach of security that leads to the accidental, or unlawful, destruction,loss, alteration, unauthorised disclosure of, or access to, personal datatransmitted, stored or otherwise processed. |
| **Data Controller** | The person (including organisations or government bodies) who determines the purposes and means or processing the personal data. Teenage Cancer Trust will usually act as the Data Controller. |
| **Data Processor** | A person (including organisations or government bodies) who processpersonal data on behalf of Teenage Cancer Trust |
| **Data Protection Clause** | A standard clause **must** be used in all arrangements with third partieswhere Personal Data is shared. |
| **Data Protection Officer**  | The Data Protection Officer (DPO) ensures, in an independent manner, that an organization applies the laws protecting individuals' personal data. The designation, position and tasks of a DPO within an organization are described in Articles 37, 38 and 39 of the European Union (EU) General Data Protection Regulation (GDPR). Teenage Cancer Trust employs an external company to provide DPO services. |
| **Data Protection Leads**  | Small group who provide data protection advice and training internally. They can be contacted on: dataprotection@teenagecancertrust.org |
| **Data Subject** | Any living individual who is the subject of personal data held by teenage Cancer Trust. This will include employees, donors, next of kin, partners, referees, supporters, volunteers and young people.  |
| **Data Subject Rights** | The rights of an individual:1. To be informed2. Of access3. To rectification4. To erase5. To restrict processing6. To data portability7. To object8. In relation to automated decision making and profiling. |
| **DPA** | The UK Data Protection Act 2018, which implements UK-specific aspects ofthe GDPR |
| **DPIA** | A data protection impact assessment which must be used if an intendedprocessing activity (in particular using new technologies) is likely to result in a high risk to the rights and freedoms of Data Subjects. A template DPIA can be found [here.](https://teenagecancertrust759.sharepoint.com/%3Aw%3A/r/sites/BackstageFundraising/Shared%20Documents/Fundraising%20Standards%20and%20operations/Data%20protection%20impact%20assessment%20Template%202020.docx?d=wb5183a0486d84168b95c2a6ced4c683a&csf=1&web=1&e=CPlc1L) |
| **Electronic Processing** | Processing of Personal Data involving electronic means (i.e. emails, Backstage, Microsoft functionality, databases) |
| **GDPR** | General Data Protection Regulation which came into force on 25 May 2018, replacing the Data Protection Act 1998. |
| **ICO** | The Information Commissioner’s Office which is the regulatory for dataprotection legislation in England and Wales |
| **Manual Processing** | Processing of Personal Data entirely by people (i.e. paper records) |
| **Personal Data** | Data which relates to an identified or identifiable *living* individual. If aperson can be identified directly or indirectly from the data (i.e. if there is a named individual, or an identification number such as personnel number of national insurance number, location data or other online identifiers). |
| **Processing** | Any operation which is performed on personal data. Basically any treatmentof data will be treated as processing including, but not limited to: collecting,recording, organising, structuring, storing, adapting, altering, disclosing,erasing or otherwise making available. |
| **Profiling** | Any automated processing of personal data which is intended to evaluatecertain aspects relating to the data subject. This would include automatedanalysis of an individual's work performances, personal preferences,behaviour, health etc |
| **Sensitive or Special Category Data** | Personal information which reveals something about an individuals:● Racial or ethnic original● Political opinion or trade union memberships● Religious beliefs● Physical or mental health condition● Sexual life/sexual orientation● Criminal backgroundSpecial category data is of a confidential nature and needs to be treated with even greater care than other personal data.  |
| **Territorial Scope** | The GDPR relates to all personal data processed by Teenage Cancer Trust both in relation to individuals based in the UK and individuals overseas. |

Appendix 2: Roles and Responsibilities

1. **ROLES AND RESPONSIBILITIES**

|  |  |  |
| --- | --- | --- |
| **Role** | **Responsibilities** | **Role holder**  |
| Senior Leadership Team (SLT) and the Board of Trustees | * Playing a key role in fostering a Data Protection (DP) culture within Teenage Cancer Trust.
* Receiving updates from the Data Protection Leads in relation to organisational DP compliance, through quarterly Risk and Safeguarding report for the board
* Enabling the Data Protection Leads and Data Protection Officer (DPO) to perform their statutory requirements and ensuring they are provided with the necessary time, resources and support to perform their duties.
 | Members of SLT and the Board |
| Risk, Safeguarding Governance Group (RSGGG) | * Receiving updates from the Data Protection Leads in relation to organisational DP compliance through the extended version of the board report (including reporting on data breaches, SAR, Requests for Erasure and rolling actions from DPO meetings) as well as update on the actions from the most recent DP audit.
* Reports are submitted in advance of the Risk and Safeguarding meeting and any actions resulting from the discussion are documented on the internal audit report.
 | Members of RSGGG |
| Senior Risk Lead | * Senior executive with overall accountability for organisational risk management, including personal data and information as high risk assets.
 | Director of Finance and Strategic Performance |
| Data Protection Leads  | * The organisational leads on Data Protection, ultimately responsible for ensuring our processes, policies and systems are compliant with the DP rules, regulations and the best practice.
* Providing at least quarterly reports to RSGGG, SLT and the Board in relation to organisational DP compliance.
* Providing advice and recommendations to Senior Risk Lead, SLT and the Board in relation to data protection and related risks.
* Investigating and responding to data protection breaches and potential breaches (incidents).
* Ensuring the DPO is involved as required in all issues related to the protection of personal data.
* Keeping evidence of the steps taken to comply with the Data Protection regulations, including (but not limited to) General Data Protection Regulations (GDPR) and Privacy and Electronic Communications Regulations (PECR).
* Developing, reviewing and updating processes, policies and procedures related to DP as necessary and on regular basis.
 | Head of Data/Head of Fundraising Standards and Operations |
| Data Protection Support Lead | * Responsible for all day-to-day queries from internal and external stakeholders.
* Developing and delivering training to the organisation, including bespoke team training sessions as/when required
 | Fundraising Standards and Operations Manager  |
| Data Protection Group | * Cross organisational group responsible for ensuring Data Protection policies and procedures are adhered to within their area of the business
* Responsible for delivering training to their teams (with support from Data Protection Support Lead)
 |  |
| Data Protection Database Lead | * Database Team’s lead on DP.
* Ensuring that processes and procedures are in place to capture, record and select data to/from our database in a lawful manner
 |  |
| Data Protection IT Lead | * IT lead on DP.
* Ensuring that processes, procedures and systems are in place to ensure security of our IT systems and infrastructure.
 | Head of IT |
| Data Protection Officer (DPO) | * The point of contact with The Information Commissioner’s Office (ICO).
* The point of contact for Data Subjects’ queries or complaints about personal data.
* Providing advice on all aspects of Data Protection.
* Advising the Data Protection Leads in relation to potential personal data breaches.
* Updating on changes to DP legislation and on cases and the interpretation of DP legislation by the ICO.
* Reviewing policies, procedures and guidelines.
* Carrying out DP audits every 12 months to ensure Teenage Cancer Trust continues to operate in a compliant manner.
 | Moore ClearComm |
| All data users | * Responsible for keeping personal data secure and for processing it in a lawful manner, in line with organisational policies and guidelines, including DP Code of Conduct and IT Code of Conduct.
* Completing mandatory DP training and annual refresher trainings without any unnecessary delays.
* Attending bespoke team/role specific training sessions as/when required
* If in doubt, flagging questions and queries with Data Protection Leads, so they can offer advice or additional training as required.
 | All individuals who process personal data |