



GDPR AND DATA SECURITY POLICY

YOUTH CANCER TRUST

VERSION 2.0

Contents

Version Control	3
Introduction	4
Scope	4
Definitions	5
Data Protection Principles – Service Users and Staff	7
The Basis for Processing Personal Information – Service Users and Staff	7
Sensitive Personal Information – Service Users and Staff	9
Criminal Records Information - Staff	11
Data Protection Impact Assessments (DPIAs) – Service Users and Staff	11
Documentation and Records - Staff and Trustees	12
General Controls in Place	13
Privacy Notice - Service Users and Staff	13
Individual Rights – Service Users and Staff	14
Individual Obligations - Staff and Trustees	14
Information Security	16
Storage and Retention of Personal Information – Service Users and Staff	17
Data Breaches	18
International Transfer of Data	19
Consequences of Failing to Comply	19
Service User/Persons Data Storage and Retention	20
Systems Used and Data Stored – Service Users	20
Systems Used and Data Stored – Staff	20
Sharing of Data – Service Users/Staff	20
Data Disposal	20
Service Users Data Stored	21
Staff Data Stored	22
Data Sharing Process Flow – Service Users	24

Subject Access Requests and Data Rights – Service Users and Staff	25
Introduction	25
SAR and Data Rights Procedure	25
SAR Timescales	25
SAR Fee’s	25
SAR Business Processes	25
Undertaking Privacy Impact Assessments	26
Confidentiality	27
Service Users	27
Discussions and Meetings	28
Outside of Work	28
Requests for Information	28
Access to Records	29
Security of Personal Data	29
Disclosure Policy	30
Procedure on Disclosures	30
Staff Records	31
Outside of Work	31
Personal and Sensitive Information	31
Requests for Information	31
Disclosure Policy and Procedures	32
Procedure on Disclosures	32
Governance	32

Version Control

Amendments

Version	Author	Date	Comments
1.0			
2.0	Policy Pros	August 2021	Review of Version 1.0

Reviewed By

Name	Date	Next Review	Comments
Policy Pros	August 2021	August 2022	Review and update with reference to new online ways of working and new data collected and stored
GH, WP, LH	03/02/2022	12/12/22	

Introduction

Youth Cancer Trust obtains, keeps, and uses personal information - also referred to as data – about the young people using our services online (members) or on holidays (guests) jointly referred to in this policy as ‘Service Users’, job applicants and current and former employees, temporary and agency workers and volunteers for several specific lawful purposes.

This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to our workforce and Service Users. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

We are committed to complying with our data protection obligations, and to being concise, clear, and transparent about how we obtain and use personal information relating to our workforce and Service Users, and how (and when) we delete that information once it is no longer required.

Georgina Hillman is responsible for informing and advising Youth Cancer Trust and its staff on its data protection obligations, and for monitoring compliance with those obligations and with Youth Cancer Trust’s policies.

If you have any questions or comments about the content of this policy or if you need further information, you should contact the data protection officer by emailing georgina@yct.org.uk or by letter to: Youth Cancer Trust, Tracy Ann House, 5 Studland Road, Alum Chine, Bournemouth, BH4 8HZ. By Telephone: +44 (0) 1202 763 591.

Scope

This policy applies to the trustees, employees (full time, part-time or casual), volunteers and subcontractors of Youth Cancer Trust, who will be referred to as ‘staff’ or ‘staff members’.

This document is also applicable to our Service User's other stakeholders in Youth Cancer Trust.

Youth Cancer Trust policy and procedure documents may be distributed to suppliers, accreditation, and compliance bodies and any other relevant third parties.

In some cases, third parties such as suppliers or those performing on-site work or through our online presence for Youth Cancer Trust will be expected to adhere to our policies, which will be made available where applicable.

We will review and update this policy following our data protection obligations. It does not form part of any employee’s contract of employment, and we may amend, update, or supplement it from time to time.

We will circulate any new or modified policy to staff and any other stakeholders when it is adopted.

Definitions

Criminal Records Information	Means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
Data Breach	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
Data Subject	Means the individual to whom the personal information relates;
Personal Information	(Sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;
Processing Information	Means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
Pseudonymised	Means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to

technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;

Sensitive Personal Information Sometimes known as 'special categories of personal data' or 'sensitive personal data' means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

Controller

Art.2(d) GDPR

"Controller" means the natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller may be designated by those laws.

Data Protection Principles – Service Users and Staff

Youth Cancer Trust will comply with the following data protection principles when processing personal information:

- We will process personal information lawfully, fairly and in a transparent manner;
- We will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;
- We will only process the personal information that is adequate, relevant, and necessary for the relevant purposes;
- We will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;
- We will keep personal information for no longer than is necessary for the purposes for which the information is processed; and
- We will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and accidental loss, destruction, or damage.

The Basis for Processing Personal Information – Service Users and Staff

Concerning any processing activity, we will, before the processing starts for the first time, and then regularly while it continues:

- Review the purposes of the processing activity, and select the most appropriate lawful basis (or bases) for that processing, for example:
 - That the data subject has consented to the processing;
 - That the processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject before entering into a contract;
 - That the processing is necessary for compliance with a legal obligation to which Youth Cancer Trust is subject;
 - That the processing is necessary for the protection of the vital interests of the data subject or another natural person; or

- That the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or
 - That the processing is necessary for legitimate interests of Youth Cancer Trust or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.
- Except where the processing is based on consent, satisfy ourselves that the processing is necessary for the relevant lawful basis (for example, that there is no other reasonable way to achieve that purpose);
- Document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles.
- Include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s).
- Where sensitive personal information is processed, also identify a lawful special condition for processing that information, and document it; and
- Where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.
- Determine whether Youth Cancer Trust’s legitimate interests are the most appropriate basis for lawful processing, we will:
 - Conduct a legitimate interest’s assessment (LIA) and keep a record of it, to ensure that we can justify our decision;
 - If the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);
 - Keep the LIA under review, and repeat it if circumstances change; and
 - Include information about our legitimate interests in our relevant privacy notice(s).

Sensitive Personal Information – Service Users and Staff

Sensitive personal information is sometimes referred to as ‘special categories of personal data’ or ‘sensitive personal data’.

- Youth Cancer Trust may need to process sensitive personal information. We will only process sensitive personal information if:
 - We have a lawful basis for doing to set out above, for example, it is necessary for the performance of the employment contract, to comply with Youth Cancer Trust’s legal obligations for people or for Youth Cancer Trust’s legitimate interests; and
 - One of the special conditions for processing sensitive personal information applies, for example:
 - The data subject has given explicit consent so Youth Cancer Trust can provide its services.
 - The processing is necessary for exercising the employment law rights or obligations of Youth Cancer Trust or the data subject.
 - The processing is necessary to protect the data subject’s vital interests, and the data subject is physically incapable of giving consent.
 - Processing relates to personal data which are manifestly made public by the data subject.
 - The processing is necessary for the establishment, exercise, or defence of legal claims; or
 - The processing is necessary for reasons of substantial public interest.
- Before processing any sensitive personal information, staff must inform the DPO of the proposed processing, so that the DPO may assess whether the processing complies with the criteria noted above.
- Sensitive personal information will not be processed until:
 - The assessment/training has been agreed to; and

- The individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.
- Youth Cancer Trust will not carry out automated decision-making (including profiling) based on an individual's sensitive personal information.
- Youth Cancer Trust's Privacy Notice sets out the types of sensitive personal information that Youth Cancer Trust processes, what it is used for and the lawful basis for the processing.
- Concerning sensitive personal information, Youth Cancer Trust will comply with the procedures set out to make sure that it complies with the data protection principles set out above.
- During the recruitment process: the organisation will ensure that (except where the law permits otherwise):
 - During the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, for example, race or ethnic origin, trade union membership or health;
 - If sensitive personal information is received, for example, the applicant provides it without being asked for it within their CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted;
 - Any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing, or making the recruitment decision;
 - 'Right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview, or decision-making stages;
 - We will not ask health questions in connection with recruitment.
- During employment: the organisation will process:
 - Health information to administer sick pay, keeping sickness absence records, monitoring staff attendance, and facilitating employment-

related health and sickness benefits;

- Sensitive personal information for equal opportunities monitoring and pay equality reporting. Where possible, this information will be anonymised; and
- Trade union membership information for staff administration and administering 'check off'.

Criminal Records Information - Staff

Criminal records information will be processed following the Youth Cancer Trust DBS Policy.

Data Protection Impact Assessments (DPIAs) – Service Users and Staff

Where the processing is likely to result in a high risk to an individual's data protection rights we will, before commencing the processing, carry out a DPIA to assess:

- Whether the processing is necessary and proportionate concerning its purpose.
- The risks to individuals; and
- What measures can be put in place to address those risks and protect personal information.
- Before any new form of technology is introduced, the manager responsible should therefore contact the data protection officer so that a DPIA can be carried out.
- During any DPIA, the employer will seek the advice of the data protection officer and any other relevant stakeholders.

Documentation and Records - Staff and Trustees

We will keep records of processing activities, including:

- The name and details of the employer's organisation (and where applicable, of other controllers, the employer's representative and DPO);
- The purposes of the processing;
- A description of the categories of individuals and categories of personal data;
- Categories of recipients of personal data;
- Where relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;
- Where possible, retention schedules; and
- Where possible, a description of technical and organisational security measures.

As part of our record of processing activities we document, or link to documentation, on:

- Information required for privacy notices.
- Records of consent.
- Controller-processor contracts.
- The location of personal information.
- DPIAs; and
- Records of data breaches.
- If we process sensitive personal information or criminal records information, we will keep written records of:
 - The relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;

- o The lawful basis for our processing; and
- o Whether we retain and erase the personal information following our policy document and, if not, the reasons for not following our policy.
- We will conduct regular reviews of the personal information we process and update our documentation accordingly. This may include:
 - o Carrying out information audits to find out what personal information Youth Cancer Trust holds.
 - o Distributing questionnaires and talking to staff across Youth Cancer Trust to get a more complete picture of our processing activities; and
 - o Reviewing our policies, procedures, contracts, and agreements to address areas such as retention, security, and data sharing.
- We document our processing activities in electronic form so we can add, remove, and amend information easily.

General Controls in Place

- There is a process of continual review to determine whether any changes in the organisation's registration are required as a result of changes in the nature of the business.
- The details of Youth Cancer Trust are registered are kept up to date.
- The notification to the Information Commissioner's Office is renewed annually.
- Youth Cancer Trust maintains and updates the public data protection register which will be reviewed regularly and at least on an annual basis.

Privacy Notice - Service Users and Staff

Youth Cancer Trust will issue privacy notices from time to time, informing you about the personal information that we collect and hold relating to you, how you can expect your personal information to be used and for what purposes.

We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

Individual Rights – Service Users and Staff

People have the following rights concerning their personal information:

- To be informed about how, why and on what basis that information is processed.
- To obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request— see the SAR Policy information.
- To have data corrected if it is inaccurate or incomplete;
- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as ‘the right to be forgotten);
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information, but you require the data to establish, exercise or defend a legal claim; and
- To restrict the processing of personal information temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation’s legitimate grounds override your interests).
- If you wish to exercise any of the rights in the paragraphs above, please contact the data protection officer.

Individual Obligations - Staff and Trustees

Individuals are responsible for helping Youth Cancer Trust keep their personal information up to date. You should let Youth Cancer Trust know if the information you have provided to Youth Cancer Trust changes, for example, if you move to a new house or change details of the bank or building society account to which you are paid.

You may have access to the personal information of other members of staff, suppliers, and Service Users of Youth Cancer Trust in the course of your employment or engagement. If so, Youth Cancer Trust expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out above.

If you have access to personal information, you must:

- Only access the personal information that you have authority to access, and only for authorised purposes;
- Only allow other Organisation staff to access personal information if they have appropriate authorisation;
- Only allow individuals who are not Organisation staff to access personal information if you have specific authority to do so from the data protection officer.
- Keep personal information secure (for example. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in Youth Cancer Trust's Privacy Policy.
- Not remove personal information, or devices containing personal information (or which can be used to access it), from Youth Cancer Trust's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and
- Not store personal information on local drives or on personal devices that are used for work purposes.
- You should contact the data protection officer if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):
 - Processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions being met;

- Any data breach as set out below;
- Access to personal information without the proper authorisation;
- Personal information not kept or deleted securely;
- Removal of personal information, or devices containing personal information (or which can be used to access it), from Youth Cancer Trust's premises without appropriate security measures being in place;
- Any other breach of this Policy, or any of the data protection principles set out above.

Information Security

Youth Cancer Trust will use appropriate technical and organisational measures to keep personal information secure and to protect against unauthorised or unlawful processing and accidental loss, destruction, or damage. These may include:

- Making sure that, where possible, personal information is pseudonymised or encrypted;
- Ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- Ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored promptly; and
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- In rare cases where Youth Cancer Trust uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

- The organisation may act only on the written instructions of Youth Cancer Trust;
 - Those processing the data are subject to a duty of confidence;
 - Appropriate measures are taken to ensure the security of processing;
 - Sub-contractors are only engaged with the prior consent of Youth Cancer Trust and under a written contract.
 - The organisation will assist Youth Cancer Trust in providing subject access and allowing individuals to exercise their rights under the GDPR;
 - The organisation will assist Youth Cancer Trust in meeting its GDPR obligations concerning the security of processing, the notification of data breaches and data protection impact assessments;
 - The organisation will delete or return all personal information to Youth Cancer Trust as requested at the end of the contract; and
 - Youth Cancer Trust will submit to audits and inspections, provide Youth Cancer Trust with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell Youth Cancer Trust immediately if it is asked to do something infringing data protection law.
- Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the Data Protection Officer.

Storage and Retention of Personal Information – Service Users and Staff

- Personal information (and sensitive personal information) will be kept securely following Youth Cancer Trust’s Data Security Policy.
- Personal information (and sensitive personal information) should not be retained any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should follow Youth Cancer Trust’s Retention Policy which set out the relevant retention period or the criteria that should be used to determine the retention period. Where there is any

uncertainty, staff should consult the data protection officer georgina@yct.org.uk

- Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

Data Breaches

- A data breach may take many different forms, for example:
 - Loss or theft of data or equipment on which personal information is stored;
 - Unauthorised access to or use of personal information either by a member of staff or third-party;
 - Loss of data resulting from an equipment or systems (including hardware and software) failure;
 - Human error, such as accidental deletion or alteration of data;
 - Unforeseen circumstances, such as a fire or flood;
 - Deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
 - 'Blagging' offences, where information is obtained by deceiving the organisation which holds it.

- In the event of a Data Breach, Youth Cancer Trust will:
 - Make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals;
 - Notify the affected individuals, if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.
 - Risk assesses the situation and determine what steps need to be taken.
 - Immediately take such steps as are necessary to minimise the risk to Service Users, staff, and the organisation.
 - Take such steps as are necessary to ensure that similar breaches cannot happen again.

International Transfer of Data

Youth Cancer Trust does not intend to transfer personal information outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein, and Norway) to other countries.

If this were to be required, it would be on the basis that that country, territory or organisation is designated as having an adequate level of protection OR that the organisation receiving the information has provided adequate safeguards by way of standard data protection clauses.

Consequences of Failing to Comply

Youth Cancer Trust takes compliance with this policy very seriously. Failure to comply with the policy:

- Puts at risk the individuals whose personal information is being processed; and
- Carries the risk of significant civil and criminal sanctions for the individual and Youth Cancer Trust; and
- May, in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this policy, a staff member's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the Data Protection Officer.

Service User/Persons Data Storage and Retention

The Directors of managers of Youth Cancer Trust store personal and sensitive personal information on Service Users to manage their test results and fulfil the person's unique cases.

Systems Used and Data Stored – Service Users

The following core systems are used to service user's data defined in Service Users data stored.

Access is only provisioned to the YCT employees' members who work with the service users and software access controls are managed internally.

Any paper copies of any service user data are stored in a locked cabinet.

- Desktop/Laptops Windows 10
- Zoho CRM System
- Google Workspace

Systems Used and Data Stored – Staff

Any paper copies of any staff data are stored in a locked cabinet.

- Desktop/Laptops Windows 10
- Google Workspace

Sharing of Data – Service Users/Staff

Staff Service User data is only shared when required with the following individuals and organisations:

- Welfare organisations (if required)
- Police and Government related organisations (if required)
- Accounting and Payroll is outsourced to Taylorcocks.
- Bookkeeping is outsourced to Maggie Spears.

Data Disposal

The Youth Cancer Trust has hardware disposal policies in place, so all hard drives are destroyed by a professional organisation when upgraded.

Confidential waste is also removed and destroyed by a professional organisation

Service Users Data Stored

Information Type
Service User Data
Data Stored
Service User CRM data, Service User Enquiry Forms, Service User Complaints. This data can include medical diagnosis and, in some cases, medical information as well as all logged communications, including safeguarding reports and recordings of online sessions. Images.
Processing Reason
<ul style="list-style-type: none">● Administration of YCT services.
Legal Interest/Legitimate Reason
<ul style="list-style-type: none">● Legitimate reason for performing contract duties.● Consent is given by a parent at the initial stage or opt in.
Retention Policy
4 years/as long as required. Removed if individual passes away.

Staff Data Stored

Information Type
Staff Data
Data Stored
<p>Typical staff data stored is below. YCT may store parts or all of the data depending in the individual use case.</p> <p>Personal Information</p> <ul style="list-style-type: none">● Name, address, email, telephone number.● Next of Kin.● Application Form data/CV.● Interview notes.● Offer and acceptance letters <p>Contract</p> <ul style="list-style-type: none">● Dated/signed.● P60/P45. <p>Photographic Evidence of Identity</p> <ul style="list-style-type: none">● Valid Passport/Driving Licence copy. <p>Various</p> <ul style="list-style-type: none">● National Insurance and Bank details.● Copies of relevant qualifications.● Right to Work in the UK● Evidence of Current Address

- References.
- Training Record.
- Record of sickness, leave and disciplinaries.
- Statutory Maternity, Adoption, Paternity Pay
- Statutory Sick Pay
- Payroll and PAYE Records
- Health and Safety Consultations
- DBS Check Data.
- Redundancy Details
- Disciplinary, working time and training data
- Images and recordings

Processing Reason

- Provision of employment obligations.
- Fulfilment of contract.

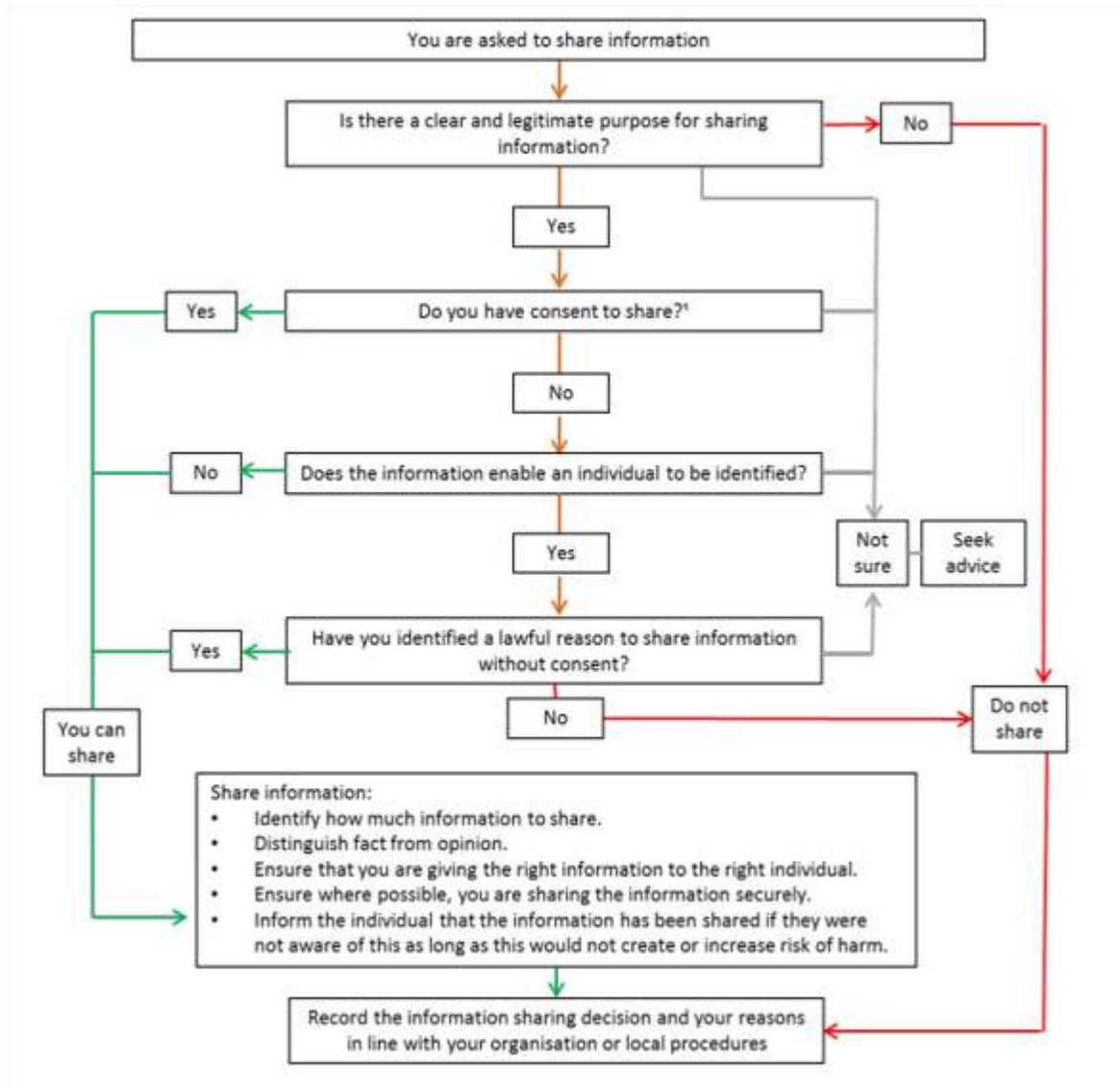
Legal Interest/Legitimate Reason

- Legitimate reason for performing contract duties.
- Consent is given by an individual at the initial stage (contract).

Retention Policy

6 Years.

Data Sharing Process Flow – Service Users



Subject Access Requests and Data Rights – Service Users and Staff

Introduction

Under GDPR legislation, Data Controllers shall provide the information outlined in Articles 13 & 14 to Data Subjects and Data Subjects may access, correct, delete, restrict processing of, and transfer their personal data, as well as object to automated decision-making based on their personal data.

SAR and Data Rights Procedure

Subject Access Requests should come to the email address georgina@yct.org.uk in the first instance and be followed up with an acknowledgement letter/email.

All requests and their progress must be logged by the data protection officer in a secure place with no external access.

SAR Timescales

All Subject Access Requests will be completed within 30 days unless defined as complex – if the time will exceed 30 days, the requestor will be notified.

SAR Fee's

Subject Access Requests coming directly from the data subject will be free, however, Youth Cancer Trust can charge a fee if requests become unfounded or excessive. If requests are coming from a Service User on behalf of a data subject, Youth Cancer Trust may charge a fee for data retrieval.

SAR Business Processes

The processes cover SAR and other data rights of individuals:

- Right of Access and Data Portability
- Right to Erasure
- Right to Object
- Right to Restriction
- Right to Rectification

Undertaking Privacy Impact Assessments

When Youth Cancer Trust undertakes the use of new technologies or will be involved in the processing of data that contains a high risk to the rights and freedoms of data subjects, it will undertake a Privacy Impact Assessment.

The scale and nature of each PIA will be shaped on a case-by-case basis, to capture the following information to inform the decision-making process:

- Risk Assessment
- Data types, collection, storage use and deletion methodologies
- Legal basis
- Information flows processes and procedures
- Consultation
- Evaluation of privacy procedures
- Final summary

For further information on PIA Please refer to:

<https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>

Confidentiality

We do not disclose information given to us to third parties without consent, unless required under our safeguarding policies and procedure or our obligations in regard to the Data Protection Act 1998 and GDPR 2019/UK GDPR 2021.

All breaches will be taken seriously and are potentially a disciplinary matter.

There are, however, exemptions for breaches of confidentiality under special circumstances.

Any actual or suspected breaches of Confidentiality shall be reported at once to a Youth Cancer Trust director who will immediately:

- Risk assesses the situation and determine what steps need to be taken.
- Immediately take such steps as are necessary to minimise the risk to Service Users, staff, and the business.
- Take such steps as are necessary to ensure that similar breaches cannot happen again.

Service Users

It is necessary to collect and keep a certain amount of information about our Service Users, however:

- We only collect and keep information that is necessary to enable us to perform our services.
- Access to the information held on people is restricted to Youth Cancer Trust staff.
- Information is not made available to third parties without the informed specific consent of the person (or by exceptions under the Data Protection Act 1998/UK GDPR).
- When collecting information, we should always inform them why information is required and what it will be used for.
- Subcontractors working for Youth Cancer Trust are also required to comply with our confidentiality policy.

Discussions and Meetings

- If discussing a person's situation in a meeting, staff should only disclose information relevant to the matter at hand.
- Staff should be aware that others with no involvement may be able to overhear e.g., at reception, in an open-plan office or corridors. Staff will ensure discussions happen in an appropriate place.
- Staff will not discuss personal facts about one person with or in the presence of, any other person.

Outside of Work

- Staff should regard all information they have access to or are given because of their work for Youth Cancer Trust as being always confidential unless advised otherwise.
- When working remotely, all personal and sensitive information should be kept in locked storage and should only be shared through secured systems, i.e., using password-protected documents, secure platforms, etc.

Requests for Information

- People have a right to request access to information kept about them. The request must be put in writing and dealt with by DPO.
- Third parties may request information about a person. This should only be given if we have received formal consent from the person.

Access to Records

Under GDPR legislation, Data Controllers shall provide the information outlined in Articles 13 & 14 to Data Subjects and Data Subjects may access, correct, delete, restrict processing of, and transfer their data, as well as to object to automated decision-making based on their data.

- GDPR gives persons the right to access the personal data held about them by Youth Cancer Trust through Subject Access Requests, specifically persons have the following rights:
 - Right of Access and Data Portability
 - Right to Erasure
 - Right to Object
 - Right to Restriction
 - Right to Rectification
- All Subject Access Requests will be completed within 30 days unless defined as complex – if the time will exceed 30 days, the requestor will be notified.
- Information requested by a person may cover both manual and computerised records. These requests should be processed in the same way as requests to view paper records.
- Subject Access Requests coming directly from the data subject will be free, however, Youth Cancer Trust can charge a fee if requests become unfounded or excessive.

Security of Personal Data

Youth Cancer Trust will ensure that personal data is held securely and for no longer than is necessary.

If you believe you have lost any personal data in the course of your work, you must report it immediately.

Failure to do so may result in disciplinary action up to and including dismissal.

Disclosure Policy

Youth Cancer Trust will not allow personal and sensitive personal data collected from service users to be disclosed to third parties except in circumstances that meet the requirements of our defined legal basis or other controls defined by GPDR.

Example situations are when:

- The person has consented to the disclosure.
- There is a serious risk of harm.
- Where Youth Cancer Trust receives information that may prevent a crime or assist in the detection of a crime.
- Where Youth Cancer Trust is legally obliged to disclose the data.

Procedure on Disclosures

Any disclosure to be made must be checked for suitability beforehand and the individual performing the check may refer to the Information Commissioner for advice and guidance.

Any request for data based on a legal requirement, e.g., from the Police or other body, must be put in writing and be checked by a member of the Senior Management Team against the advice of the Information Commissioner before any data is disclosed.

Staff Records

It is necessary to collect and keep a certain amount of information about current, former and potential staff.

Our confidentiality policy aims to safeguard privacy and ensure appropriate access to information:

- The processing of all information is governed by GDPR 2018.
- We only collect and keep the necessary information to perform roles and manage HR and payroll administration.
- Information is not made available to third parties without the informed consent of the staff member (or exceptions as in the Data Protection Policy or exceptions under the safeguarding policies and procedures).
- When collecting information from a staff member we should always inform them why information is required and what it will be used e.g., for supervision purposes.
- Personal facts about one staff member are not discussed with, or in the presence of, any other person
- Staff will not disclose personal details (home address, telephone number etc.) to persons or other parties but should use their project address when an address must be given.

Outside of Work

Staff must adhere to the Confidentiality and Data Protection policies and procedures at all times.

Personal and Sensitive Information

Youth Cancer Trust will process sensitive data such as medical information and DBS checks, primarily where it is necessary to enable Youth Cancer Trust to meet its legal obligations and in particular to ensure adherence to health and safety and vulnerable groups protection legislation or for equal opportunities monitoring purposes.

Youth Cancer Trust will not process sensitive personal data without consent.

Requests for Information

Staff have the same Subject Access Requests rights as Service Users.

Disclosure Policy and Procedures

Youth Cancer Trust will not allow personal and sensitive personal data collected from employees to be disclosed to third parties except in circumstances that meet the requirements of GDPR 2018/UK GDPR 2021.

This will be where either the employee has consented to the disclosure, or there is a serious risk of harm and where Youth Cancer Trust receives information which may prevent a crime or assist in the detection of a crime, or where Youth Cancer Trust is legally obliged to disclose the data.

Procedure on Disclosures

Any request for data based on a legal requirement, e.g., from the Police or other body, must be put in writing and be checked by HR, the relevant Manager, or a member of the Senior Management Team against the advice of the Information Commissioner before any data is disclosed.

Governance

All policies and procedures are reviewed annually by the department responsible; to ensure that we respond to staff needs, business strategy, legislation and any codes of practices determined by the market.