World Child Cancer UK

Data Protection policy

Updated March 2019

1. **POLICY STATEMENT**

1.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about those we help, our donors, our employees, our volunteers and other third parties.

1.2 Data users are obliged to read this policy because it contains important information about:

1.2.1 the data protection principles which we must comply with;

1.2.2 what is meant by personal data and sensitive personal data;

1.2.3 how we gather, use and (ultimately) delete personal data and sensitive personal data in accordance with the data protection principles;

1.2.4 your rights and obligations in relation to data protection; and

1.2.5 the consequences of failure to comply with this policy.

1.3 You must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

2. **ABOUT THIS POLICY**

World Child Cancer UK and World Child Cancer US ('**we'**, '**us'**, '**our'**) may process personal data about current, past and prospective beneficiaries, current, past and prospective donors, current, past and prospective employees, volunteers, trustees, supporters, suppliers, and others that we communicate with. Personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the General Data Protection Regulation and the UK Data Protection Act 2018 (together, the 'Act') and other regulations. This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.1 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.2 The Finance Director is responsible for ensuring compliance with the Act and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Finance Director.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 **Data subject** means the individual to whom the personal data relates.

3.2 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.3 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act.

3.4 **Data users** are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this policy and any applicable data security procedures at all times.

3.5 **Data processors** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

3.6 **Processing** is any activity that involves use of personal data or sensitive personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.7 **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions (see paragraph 6 for further details).

4. DATA PROTECTION PRINCIPLES

4.1 We will comply with the following enforceable principles when processing personal data:

4.1.1 we will process personal data lawfully, fairly and in a transparent manner;

4.1.2 we will collect personal data for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

4.1.3 we will only process the personal data that is adequate, relevant and necessary for the relevant purposes;

4.1.4 we will keep accurate and up to date personal data, and take reasonable steps to ensure that inaccurate personal data are deleted or corrected without delay;

4.1.5 we will keep personal data for no longer than is necessary for the purposes for which the data is processed; and

4.1.6 we will take appropriate technical and organisational measures to ensure that personal data are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

5. FAIR AND LAWFUL PROCESSING

5.1 The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

5.2 For personal data to be processed lawfully, they must be processed on the basis of one of the lawful bases set out in the Act. These include (but are not limited to) the data subject's consent to the processing, that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met (as set out in paragraph 6 below). When processing personal data as data controllers in the course of our activities, we will ensure that those requirements are met.

6. SENSITIVE PERSONAL DATA

6.1 Sensitive personal data is sometimes referred to as ‘special categories of personal data’.

6.2 We may from time to time need to process sensitive personal data. We will only process sensitive personal data if:

6.2.1 we have a lawful basis for doing so; and

6.2.2 one of the special conditions for processing sensitive personal data applies, e.g.

6.2.2.1 the data subject has given explicit consent;

6.2.2.2 the processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or the data subject;

6.2.2.3 the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

6.2.2.4 processing relates to personal data which are manifestly made public by the data subject;

6.2.2.5 the processing is necessary for the establishment, exercise or defence of legal claims; or

6.2.2.6 the processing is necessary for reasons of substantial public interest.

6.3 Before processing any sensitive personal data, staff must notify the Finance Director in order that he/she may assess whether the processing complies with the criteria noted above.

6.4 Sensitive personal information will not be processed until:

6.4.1 the assessment referred to in paragraph 6.3 has taken place; and

6.4.2 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.

7. PROCESSING FOR LIMITED PURPOSES

7.1 In the course of our activities, we may collect and process the personal data set out in the Schedule below. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, other charities, sub-contractors in technical, payment and delivery services, and others).

7.2 We will only process personal data for the specific purposes set out in the Schedule below or for any other purposes specifically permitted by the Act. We will notify those purposes to the data subject (as set out in paragraph 8 below).

8. NOTIFYING DATA SUBJECTS

8.1 If we collect personal data directly from data subjects, we will inform them about:

8.1.1 the purpose or purposes for which we intend to process that personal data;

8.1.2 the types of third parties, if any, with which we will share or to which we will disclose that personal data; and

8.1.3 the means, if any, with which data subjects can limit our use and disclosure of their personal data.

8.2 If we receive personal data about a data subject from other sources, we will use reasonable efforts to provide the data subject with this information.

8.3 Data subjects have the right to request that their data is not kept on our systems. There should be an information opt-out option on all materials sent to data subjects.

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

9. DATA PROTECTION IMPACT ASSESSMENTS (DPIAS)

9.1 Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where we are planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

9.2 whether the processing is necessary and proportionate in relation to its purpose;

9.3 the risks to individuals; and

9.4 what measures can be put in place to address those risks and protect personal data.

10. RECORDS

10.1 In order to comply with our obligations under the Act, we keep written records of our processing activities, including records of processing which are high risk, i.e. which may result in a risk to individuals' rights and freedoms or involve sensitive personal data or criminal records information.

11. PROCESSING IN LINE WITH DATA SUBJECTS' RIGHTS

11.1 Data subjects (including you) have the following rights in relation to their personal data:

11.1.1 to be informed about how, why and on what basis that information is processed—see our Privacy Policy for further information in respect of this;

11.1.2 to obtain confirmation that their personal data is being processed and to obtain access to it and certain other information, by making a subject access request (see paragraph 18 below in respect of this);

11.1.3 to have their personal data corrected if it is inaccurate or incomplete;

11.1.4 to have personal 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');

11.1.5 to restrict the processing of personal data where the accuracy of the information is contested, or the processing is unlawful (but they do not want the data to be erased), or where the we no longer need the personal data but the data subject requires the personal data to establish, exercise or defend a legal claim; and

11.1.6 to restrict the processing of personal data temporarily where they do not think it is accurate (and we are verifying whether it is accurate), or where they have objected to the processing (and we are considering whether our legitimate interests override the data subject's interests).

12. INDIVIDUALS' OBLIGATIONS

12.1 Individuals are responsible for ensuring that we keep their personal data up to date. You should let the Finance Director know if the information you have provided to us changes, for example if you move house or change details of the bank or building society account to which you are paid.

12.2 You may have access to the personal data of other members of staff, our suppliers, our donors or our beneficiaries in the course of your employment or engagement. If so, we expect you to help us meet our data protection obligations to those individuals.

12.3 If you have access to personal data, you must:

12.3.1 comply with our IT policy;

12.3.2 only access the personal data that you have authority to access, and only for authorised purposes;

12.3.3 only allow other staff to access personal data if they have appropriate authorisation;

12.3.4 keep personal data secure (e.g. by complying with our rules on access to premises, computer access, password protection and secure file storage and destruction);

12.3.5 not remove personal data, or devices containing personal data (or which can be used to access it), from our premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and

12.3.6 not store personal data on local drives or on personal devices that are used for work purposes**.**

12.4 You should contact the Finance Director if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

12.4.1 processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions in paragraph 6;

12.4.2 any data breach as set out in paragraph 17 below;

12.4.3 access to personal data without the proper authorisation;

12.4.4 personal data has not been kept or deleted securely;

12.4.5 removal of personal data, or devices containing personal data (or which can be used to access it), from our premises without appropriate security measures being in place;

12.4.6 any other breach of this policy.

13. DATA SECURITY

13.1 We will ensure that appropriate technical and organisational security measures to protect against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data are in place.

13.2 We will put in place appropriate procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if such data processor agrees to enter into a data protection agreement that is compliant with the Act.

12.3 All documents or files with sensitive personal data should be password protected.

13.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

13.3.1 **Confidentiality** means that only people who are authorised to use the data can access it;

13.3.2 **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed;

13.3.3 **Availability** means that authorised users should be able to access the data if they need it for authorised purposes.

13.4 Security procedures include:

13.4.1 **Entry controls**. Any stranger seen in entry-controlled areas should be reported;

13.4.2 **Methods of disposal**. Paper documents containing personal data that are no longer required should be shredded;

13.4.3 **Equipment**. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log out of or lock their laptop when it is left unattended.

14. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

14.1 We may transfer personal data outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein and Norway) to a country outside of the EEA on the basis of:

14.1.1 an adequacy decision;

14.1.2 binding corporate rules;

14.1.3 standard data protection clauses (known as model); or

14.1.4 where some other mechanism that (i) allows for such transfers outside of the EEA; and (ii) complies with the Act is in place.

14.2 Personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

15. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

15.1 We may share personal data we hold with HMRC, our pension provider, Companies House, The Charity Commission and other third parties, as necessary.

15.2 If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our beneficiaries, donors, employees, suppliers, or others.

15.3 We may also share personal data we hold with selected third parties for the purposes set out in the Schedule.

16. STORAGE AND RETENTION OF PERSONAL DATA

16.1 Personal data (including sensitive personal data will be kept securely and stored in accordance with our Data Retention Policy).

17. DATA BREACHES

17.1 A data breach may take many different forms, for example:

17.1.1 loss or theft of data or equipment on which personal data is stored;

17.1.2 unauthorised access to or use of personal data either by a member of staff or third party;

17.1.3 loss of personal data resulting from an equipment or systems (including hardware and software) failure;

17.1.4 human error, such as accidental deletion or alteration of personal data;

17.1.5 unforeseen circumstances, such as a fire or flood; and

17.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams.

17.2 We will:

17.2.1 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; and

17.2.2 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.

18. SUBJECT ACCESS REQUESTS

18.1 Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to the Finance Director as soon as possible.

18.2 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

18.2.1 we will check the caller's identity to make sure that information is only given to a person who is entitled to it; and

18.2.2 we will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

18.3 Our employees will refer a request to their manager for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

19. TRAINING

19.1 We will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

20. CONSEQUENCES OF FAILING TO COMPLY

20.1 We take compliance with this policy very seriously. Failure to comply with the policy:

20.1.1 puts at risk the data subjects whose personal data is being processed;

20.1.2 carries the risk of significant regulatory fines; and

20.1.3 may, in some circumstances, amount to a criminal offence by the individual.

20.2 Because of the importance of this policy, 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.

20.3 If you have any questions or concerns about anything in this policy, do not hesitate to contact Finance Director.

21. CHANGES TO THIS POLICY

21.1 We reserve the right to change this policy at any time.

World Child Cancer
No child should suffer

THE SCHEDULE

DATA PROCESSING ACTIVITIES

Type of data subject	**Beneficiaries.**	**Donors.**	**Employees, job applicants, contractors, temporary workers, volunteers, trustees temporary agents, and interns of the Charity, and other individuals whose data is collected in connection with human resources activities, such as dependents and emergency contacts.**
Type of data	**Personal details**: Name, address, work-related and home email addresses and contact information, national identity/registry/ insurance/social security numbers, medical certificate, proof of work eligibility/national ID number/passport, immigration or citizenship status, images, date and place of birth, citizenship and nationality, domicile or residency, gender and details of language skills. **Family & social details**: Family composition (including family history, marital status, names of spouse and/or dependants and/or	**Personal details**: Name, address, email addresses and contact information. **IT details**: IP address, device used, and electronic message communication details. **Financial details**: Donation details; bank account details, credit or debit card details, direct deposit/credit arrangements, and credit card details.	**Personal details**: Name, address, work-related and home email addresses and contact information, national identity/registry/insurance/social security numbers, medical certificate, proof of work eligibility/national ID number/passport, immigration or citizenship status, images, date and place of birth, citizenship and nationality, domicile or residency, gender and details of language skills, and drivers licence details. **Family & social details**: Family composition (including family history, marital status, names of spouse and/or dependants and/or next of kin and relationship), nominated beneficiaries, emergency contact details, holiday/annual leave arrangements and details of leave taken. **Education & Training details**: Educational and vocational training (including qualifications, grades, attendance at educational establishments and training received) student status and spoken/written/reading language proficiency. **Employment details**: Performance ratings, work time/utilization records and forecasts, training records, evaluations, information relating to labour contract and disciplinary actions, health and safety data and employee benefit plan participation details, work authorisation/eligibility/permit/visa requirements/status, business title/unit/department, cost centre, job function, position held, working arrangements (full/part-time), job location, seniority

	next of kin and relationship), and emergency contact details. **Education & Training details**: Educational and vocational training (including qualifications, grades, attendance at educational establishments and training received), student status and spoken/written/reading language proficiency. **Sensitive data**: Racial or ethnic origin, physical or mental health data, disabilities, religious beliefs, trade union membership, [criminal background data]		data, retirement age, contract length, hire/re-hire date, supervisor hierarchy, line management details, previous work history, security clearance, job history and references, work experience, and details of mobility/willingness to relocate. **IT details**: Company property issued (e.g. hardware, software, mobile telephone); IT access codes, IT usage data, IT login data and incident data, electronic message communication details, and service requests. **Financial details**: Salary information, expense reimbursement, benefit information, bank account details, credit card details, direct deposit/credit arrangements, pension payment and stock option information (stock grants or option exercise details), bonus, additional pay, variable compensation awards, tax data (national and local), flexible spending enrolments, grant valuation information, paid time off and credit card details (personal and business) for transactions and payments. **Sensitive data**: Racial or ethnic origin only where required for the purposes of compliance with anti-discrimination laws; trade union membership or affiliation only where required by law for the purposes of payroll processing; religious beliefs where required by law; physical or mental health data of any employee where required by law and/or relating to employee benefits, accommodation of an employee's disabilities, leave entitlement, statutory sick pay, occupational health and/or health and safety at work; criminal background data where permitted by law;
Type of processing	The transmission, making available to and storage on the Charity's systems/network servers; the transmission to sub-processors; management and	The transmission, making available to and storage on the Charity's systems/ network servers; the transmission	The transmission, making available to and storage on the Charity's systems/network servers; the transmission to sub-processors; operation and maintenance of systems; management and management reporting; financial reporting; and risk management, compliance, legal and audit functions.

	management reporting; financial reporting; and risk management, compliance, legal and audit functions.	to sub-processors; management and management reporting; financial reporting; and risk management, compliance, legal and audit functions.	
Purpose of processing	- Identifying, supporting, and providing care to children with cancer. - Compliance with contractual and legal obligations; policies and procedures and codes of conduct; and for legitimate purposes relating to the operations of the Charity.	- Processing of donations to the Charity, contacting donors. - Compliance with contractual and legal obligations; policies and procedures and codes of conduct; and for legitimate purposes relating to the operations of the Charity. - Management, financial reporting, accounting and audit functions, including reporting and implementation of programs and to support	Prior to employment, throughout employment (or engagement), and for as long as is necessary after the termination of employment (or engagement), the Charity will need to process personal data for: - Employment, human resources administration, reporting and management, legal and/or regulatory compliance and/or administrative purposes connected with their employment, including: recruitment and hiring activities; appraisals; performance; promotion; training; relocation and secondments; visa and work permit applications; leave entitlement (maternity/paternity/sickness/compassionate/bereavement); pay and remuneration and incentive compensation; pension and insurance and other benefits; tax and other deductions from pay; health and safety; discipline; grievances and termination of employment (or engagement); calculating prospective headcount changes (fluctuation, termination or headcount addition numbers); resource planning; organising of trips; talent management and career development; succession and personnel planning; and ensuring compliance with company policies and compliance requirements imposed by regulatory authorities. - Compliance with contractual and legal obligations; policies and procedures and codes of conduct; and

		administrative activities (including publications and communications, internal audits, risk management and data analytics). - For the purposes of obtaining legal advice and/or the company defending itself or otherwise engaging in litigation and protecting the Charity against injury, theft, legal liability, fraud, abuse and other misconduct.	for legitimate purposes relating to the operations of the Charity. - Operating and defending its information systems, including monitoring and recording the use of computer systems, telephone systems and all other electronic communication devices; carrying out internal and external investigations into security or compliance concerns, or in cases of suspected employee misconduct; data backup; data archive and document retention; operation, development and maintenance of IT systems. - Management, financial reporting, accounting and audit functions, including reporting and implementation of programs and to support administrative activities (including publications and communications, internal audits, risk management and data analytics). - Quality Assurance relating to legal obligations of reporting incidents to regulatory and other competent authorities. - For the purposes of obtaining legal advice and/or the company defending itself or otherwise engaging in litigation and protecting the Charity against injury, theft, legal liability, fraud, abuse and other misconduct. - To facilitate communication between employees from different workplace locations.

All of the above categories include current, past or prospective data subjects.