Child.org Data Protection Policy

Policy owner: Operations Manager
Last updated: October 2024
Review date: October 2026

Any concerns regarding this policy should be reported to the CEO.

1. Introduction

Child.org needs to collect and use certain types of information about the Individuals or Service Users who come into contact with Child.org in order to carry out our work. This personal information must be collected and dealt with appropriately whether it is collected on paper, stored in a computer database, or recorded on other material, and there are safeguards to ensure this under the General Data Protection Regulations 2016 (GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), and all other relevant Data Protection legislation.

The purpose of the GDPR is to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. Further, it protects the rights and privacy of individuals and ensures that personal data are not processed without their knowledge, and, wherever possible, consent.

Child.org is committed to compliance with this regulation, and to protecting the rights and privacy of individuals, volunteers, staff and others in accordance with it.

This policy applies to all individuals who have access to information by virtue of their involvement with Child.org and it is the responsibility of all such individuals to comply with the GDPR, PECR and this policy. Any breach of the GDPR, PECR or the Child.org Data Protection Policy is considered to be an offence and in that event, disciplinary procedures may apply.

All employees and volunteers are responsible for providing accurate and up to date information to Child.org and are also responsible for informing Child.org of any changes to information they have provided.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the GDPR, PECR or other relevant legislation.

2. Data Controller

Child.org is the Data Controller under the GDPR, which means that it determines what purposes personal information held, will be used for, and the means by which it will be processed. As the data controller, Child.org will ensure that all contracts with processors (those accessing, using or editing their data) comply with the GDPR.

Child.org is responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for. We are required to register with the Information Commissioner the fact that we hold personal data and to acknowledge the right of 'subject access' – voluntary and community group members and staff must have the right to copies of their own data. Subjects also have a range of other rights in relation to their data, which are laid out in this policy.

3. Purpose of data held by Child.org

Data may be held by us for the following purposes:

1. Staff Administration
2. Fundraising
3. Realising the Objectives of a Charitable Organisation or Voluntary Body
4. Accounts & Records
5. Advertising, Marketing & Public Relations
6. Information and Databank Administration
7. Journalism and Media
8. Processing For Not For Profit Organisations
9. Research
10. Volunteers

In so far as is possible, subjects will be notified at the time of collection the purpose of the data processing. The purpose will also be listed in a privacy notice which they will have access to on all relevant websites.

4. Individual rights

Child.org are committed to respecting individuals' rights in relation to their personal data. The rights set out in the GDPR are:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

These rights are central to everything in this policy, and are upheld at every stage of data processing, but are not intended to be limited to the activities and policies set out in this policy.

All Individuals/Service Users have the right to access the information Child.org holds about them. Child.org will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes.

Child.org will ensure that anybody wanting to make enquiries about handling personal information knows what to do, by having this information plainly stated in a privacy notice on all relevant websites. Staff will also be briefed on this information, in order to inform anybody in person or over the phone. All action will be taken promptly and courteously.

The procedure for responding to requests for information relating to personal data:

1. When a request comes in, it should immediately be reported to the Data Controller (specified in s.7 below). The request should be logged on civiCRM under that person's record.
2. Confirm that the person requesting is the person the data held refers to.
3. Once confirmed, check their request falls within the rights laid out above.
4. If it does, you can then check their data on civiCRM (via 'contact reports') and carry out the request. Ensure at all times that this is done safely and securely, and that there is no way that the data could be lost or stolen in the process.

5. Ensure the request is satisfied within 30 days.

5. Managing Data Protection

Child.org regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal. We therefore intend to ensure that personal information is treated lawfully and correctly.

To this end Child.org will adhere to the Principles of Data Protection, as detailed in the GDPR 2016.

Specifically, the Principles require that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals. In order to be processed lawfully, it must have one of the following legal bases:

- Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
- Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- Vital interests: the processing is necessary to protect someone's life.
- Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In addition, it is stated that:

> [T]he controller shall be responsible for, and be able to demonstrate, compliance with the principles.

All staff will have the principles in mind and adhere to them in full at all times. The following sections set out some of the policies followed by Child.org in ensuring compliance with the regulation.

5.1. Data collection

Child.org will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing an online or offline form.

Before any new data is collected, the responsible staff member will ensure the following steps are taken:

1. Confirm that a legal basis as specified in the regulation is applicable. If consent is being relied upon, ensure that the Individual/Service User:
    a. Clearly understands why the information is needed.
    b. Understands what it will be used for and what the consequences are should the Individual/Service User decide not to give consent to processing.
    c. As far as reasonably possible, grants explicit consent, either written or verbal, for data to be processed.
    d. Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress.
    e. Has received sufficient information on why their data is needed and how it will be used.
2. Individuals have access to a privacy notice relevant to the data collection, which includes the relevant legal basis and purpose, information on how to request access or removal of their data, notification of the length of time data will be held for, instructions for complaints to the ICO, and all other required information to ensure that the processing of their information is transparent and fair.
3. That all potential purposes for the data collected are set out in the privacy notice, and that the processing of the data will be restricted to these alone.
4. Confirm that the collection method and subsequent storage and processing of data all adhere to the security principles set out in this policy.

When confirming the legal basis, Child.org will take the following into consideration:

Informed consent is when:

- An Individual/Service User clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data.
- And then gives their consent.

5.2. Storing, accessing and processing personal data

Information and records relating to service users will be stored securely and will only be accessible to authorised staff and volunteers.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

When processing any personal data (including accessing) the following principles will be adhered to:

1. All data will have a recorded legal basis, as specified in the regulation.
2. A privacy notice accessible to everyone will notify all individuals of our activities in relation to personal data, and their rights in relation to it. In particular, they will be notified of their right to access the data, to request us to remove it, and directed to the ICO if they wish to make a complaint in relation to the processing of their data.
3. The purpose will be set out explicitly in the privacy notice, which all subjects have access to and will be directed to at the point of collection. The purpose of individual pieces of data will be recorded.
4. Data will only be processed in a way necessary to the specific purpose. The purpose will not later be changed without notification to the subject, and then only in such ways as are allowed by the regulation.
5. All data held will be kept as up to date as possible. Subjects will be invited to update their information whenever it is relevant to do so.
6. Data will only be kept for as long as it is required. The time deemed necessary varies by purpose, but in most cases we will keep data for 100 years. We will implement regular checks on data to ensure it is still required.
7. The storage and processing of data all adhere to the security principles set out in this policy.

Child.org will conduct data protection review every 5 years, to ensure the above principles are being adhered to. This will include

- Checking the legal basis of data held.
- Reviewing all privacy notices.
- Reviewing the way that data is used to ensure that it isn't being processed for an unspecified purpose.
- Data is up to date and accurate.
- Data is still necessary for the purpose it is being held.
- That security principles are being upheld.

5.3 Data transfers

To other organisations

As a matter of good practice, other organisations and individuals working with Child.org, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that any staff who deal with external organisations will take responsibility for ensuring that such organisations sign and agree with this policy, and sign contracts where necessary.

Child.org may share data with other agencies. Individuals will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows Child.org to disclose data (including sensitive data) without the data subject's consent.

These are:

A. Carrying out a legal duty or as authorised by the Secretary of State

B. Protecting vital interests of a Individual/Service User or other person
C. The Individual/Service User has already made the information public
D. Conducting any legal proceedings, obtaining legal advice or defending any legal rights
E. Monitoring for equal opportunities purposes – i.e. race, disability or religion

F. Providing a confidential service where the Individual/Service User's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Individuals/Service Users to provide consent signatures.

In all other circumstances, the subject will be notified of any transfer made to another organisation. This will usually be by way of a privacy notice at the point of data collection (visible afterwards on the relevant website), but when this is not possible or appropriate, other action will be taken to ensure they are notified.

When data is shared with other organisations, they will adhere to this policy and all relevant laws.

To outside the EEA

Organisations and Child.org staff working outside of the EEA will be required to sign this policy, as well as an additional contract, agreeing to adhere to the principles set out in the GDPR. It is expected that any staff who deal with external organisations will take responsibility for ensuring that such organisations sign these contracts.

Child.org has partner projects in sub-Saharan Africa, which is outside the European Economic Area. For individuals taking part in the Charity Apprentice placement abroad, any other volunteering or fundraising activity, it will be necessary for Child.org to transfer personal data to project partners and minders on location for reasons of health and safety and logistical management. In addition, subjects will have personal data with them that has been brought from the UK.

Personal data will only be processed abroad for the duration of an individual's visit to the country. Those receiving personal data are told of the importance of keeping this data secure and of the requirement not to pass any data on to any third party. At the end of the visit any personal data provided by Child.org to project partners or other stakeholders must be destroyed or returned to Child.org staff.

Participants taking part in any activity for Child.org abroad are required to specifically state whether they give their consent to the above referenced data transfer by completing the relevant section of the registration process prior to travel.

5.4 Privacy and Electronic Communications

Child.org will adhere to the principles set out in PECR in all of its activities. The regulation relates to unsolicited (not specifically requested) electronic communications (i.e. via telephone and email).

When contacting via telephone, unsolicited calls must be screened against the Telephone Preference Service (TPS), Corporate TPS (CTPS) or Fundraising preference service (FPS), and our contact number must be displayed.

No marketing emails or texts to individuals will be sent without specific consent. Child.org will ensure that all communications of these sorts are done only if specific, positive, informed, freely given consent has been obtained.

The information relevant to the consent will be clear, in plain English, and not hidden in any privacy policy or other terms and conditions.

6. Security policy

Child.org is committed to keeping data safe and secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. We will ensure that:

- There is someone in the organisation whose responsibility it is to keep data secure.
- Everyone processing personal information understands that they are contractually responsible for following good data protection practice.
- Everyone processing personal information is appropriately trained to do so.
- Everyone processing personal information is appropriately supervised.
- Appropriate technical and organisational security measures are taken to safeguard personal information. These include:
    - Install all IT system updates as they are available
    - Access to the system will be managed only by senior managers, and limited only to those it is necessary to give access to. When staff or volunteers leave the organisation, their accounts will become inaccessible by them.
    - Ensuring physical security by requiring passwords to access all laptops and accounts. All staff will be mindful when accessing data in public places not to leave the data unattended or visible.
    - Ensuring all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.
    - We will ensure that partners who process data on our behalf, and in particular the companies who hold substantial amounts of data for us, such as having access to our database, CiviCRM, have appropriate safety standards and levels encryption. Data on any staging database that is not the live version will have masked data that is anonymised.

7. Queries and questions

In case of any queries or questions in relation to this policy please contact the Child.org Data Controller:

Clare Sulley

8. Training

Please watch this recorded training video which will talk you through exactly how Child.org practises GDPR. Child.org's Best GDPR Practice guide is a handy one-stop reference point if ever you need it. Once you've watched the training video, please fill in this form to record your training.

Glossary of Terms

Data Controller – The organisation and persons who (either alone or with others) decide what personal information Child.org will hold and how it will be held or used, and the person(s) responsible for ensuring that (Child.org) follows its data protection policy and complies with the relevant legislation.

Individual/Service User – The person whose personal information is being held or processed by Child.org for example: a client, an employee, a volunteer, or supporter.

Explicit consent – is a freely given, specific and informed agreement by an Individual/Service User in the processing of personal information about her/him. Explicit consent is needed for processing sensitive data.

Notification – Notifying the Information Commissioner about the data processing activities of Child.org, as certain activities may be exempt from notification.

The link below will take to the ICO website where a self assessment guide will help you to decide if you are exempt from notification: http://www.ico.gov.uk/for_organisations/data_protection/the_guide/exemptions.aspx

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees within Child.org.

Sensitive data – refers to data about:

- Racial or ethnic origin
- Political affiliations
- Religion or similar beliefs
- Trade union membership

- Physical or mental health
- Sexuality
- Criminal record or proceedings