Data Protection Policy

Copenhagen Youth Project (CYP)

Last Updated:	April 2026
Approved by Trustees:	April 2026
Review Date:	March 2027

Introduction and Scope

Copenhagen Youth Project (CYP), the Data Controller needs to use certain types of personal information on, for example, Youth members and Parents and others with whom it communicates. In addition, it may occasionally be required by statute to collect and use certain types of information to comply with the requirements of external bodies.

This policy outlines CYP's commitment to data protection and compliance with the UK Data Protection Act 2018. The purpose of this policy is to ensure that all personal data held by the charity is processed lawfully, fairly, and transparently, and that the rights of data subjects are protected. This policy applies to all individuals working on behalf of CYP including trustees, staff, and volunteers.

CYP is registered with the Information Commissioner's Office as an organisation that processes personal data. The registration number is Z9653040

CYP will ensure that all data processing activities comply with the UK GDPR, the Data Protection Act 2018, and current ICO guidance.

Data Protection Lead (DPL)

CYP will appoint a Data Protection Lead who will be responsible for overseeing data protection and leading on any incident investigation and reporting. The DPL will also ensure that all staff and volunteers are provided with any induction, on the job or other training and made aware of their data protection responsibilities.

If you have any queries, please contact our Data Protection Lead:

Name:	Position:	Contact:
Theo Thomas	Chief Operating Officer	theo@cyproject.org

CYP fully endorses and adheres to the seven principles of the UK GDPR. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal data. Employees and any others who obtain, handle, process, transport and store personal data for CYP must adhere to these principles.

Data Protection Principles

Data is:

1. Processed lawfully, fairly and in a transparent manner.
    - There are several lawful bases for collecting and processing personal data, including consent. However, CYP may also rely on other legal bases under UK GDPR, such as legitimate interests, contractual necessity, and legal obligations, where applicable.
    - We are clear that our collection of data is legitimate and we have obtained consent to hold an individual's data, where appropriate.
    - We are open and honest about how and why we collect data and individuals have a right to access their data.
2. CYP identifies and records the lawful basis for all personal data processing activities within its internal Records of Processing Activities (ROPA). This ensures that every category of data held is processed transparently and in accordance with UK GDPR requirements.Collected for specified, explicit and legitimate purposes and not used for any other purpose.
    - We are clear on what data we will collect and the purpose for which it will be used.
    - Only collect data that we need.
    - When data is collected for a specific purpose, it may not be used for any other purpose, without the consent of the person whose data it is.

3. Adequate, relevant and limited to what is necessary.
    - We collect all the data we need to get the job done.
    - And none that we don't need.
4. Accurate and, where necessary, kept up to date.
    - We ensure that what we collect is accurate and have processes and/or checks to ensure that data which needs to be kept up-to-date is, such as beneficiary, staff or volunteer records.
    - We correct any mistakes promptly.
5. Kept for no longer than is necessary. We understand what data we need to retain, for how long and why.
    - We only hold data only for as long as we need to.
    - That includes both hard copy and electronic data.
    - Some data must be kept for specific periods of time (eg accounting, H&SW).
    - We have a process that ensures data no longer needed is destroyed.
6. CYP maintains an internal Record of Processing Activities (ROPA). This record outlines the types of data we collect, our lawful basis for processing, and our retention schedules, ensuring we meet our accountability obligations under UK GDPR. Processed to ensure appropriate security, not only to protect against unlawful use, but also loss or damage.
    - Data is held securely, so that it can only be accessed by those who need to do so. For example, paper documents are locked away, access to online folders in shared drives is restricted to those who need it, IT systems are password protected, and/or sensitive documents that may be shared (eg payroll) are password protected.
    - Data is kept safe. Our IT systems have adequate anti-virus and firewall protection that's up to date. Staff understand what they must and must not do to safeguard against cyber-attack, and that passwords must be strong and not written down or shared.
    - Data is recoverable. We have adequate data back-up and disaster recovery processes.
    - CYP applies "privacy by design and default" by embedding data protection considerations into systems, processes, and decision-making.
7. CYP shall be accountable for and be able to demonstrate compliance with the above points.

Training

Staff and Volunteers will be provided with appropriate training on data protection laws tailored to their specific roles. It is mandatory for Staff and Volunteers to complete any training sessions as required. If there are any changes to the roles or responsibilities of a Staff member or Volunteer, they are responsible for requesting updated data protection training that aligns with their new role or duties. If Staff or Volunteers require additional training on data protection matters, they should contact their line manager or the DPL. CYP will maintain training records to ensure compliance.

All staff and volunteers are responsible for reporting any concerns about data protection compliance to the DPL without delay.

Maintaining Confidentiality

CYP will treat all your personal information as private and confidential and not disclose any data about you to anyone other than the Trustees of CYP to facilitate the administration and day-to-day running of the project. All CYP staff and volunteers who have access to Personal Data will be required to agree to sign a Confidentiality Policy and a Data Protection Policy.

There are four exceptional circumstances to the above permitted by law:

1. Where we are legally compelled to do so.
2. Where there is a duty to the public to disclose.
3. Where disclosure is required to protect your interest.
4. Where disclosure is made at your request or with your consent.

Use of Personal Information

CYP will use your data for three main purposes:

1. The day-to-day administration of CYP. We work in liaison with relevant professionals and agencies outside the project to meet children's specific needs. We will only share information if required by law.
2. Contacting you to keep you informed of CYP activities and events and external activities that we think may be of interest to you.
3. Statistical analysis; gaining a better understanding of CYP demographics.

Third Party Access to Data

Under no circumstance will the Charity share with, sell or otherwise make available to Third Parties any personal data except where it is necessary and unavoidable to do so in pursuit of its charitable objects as authorised by the Data Controller, such as local authorities, funders, or safeguarding bodies when required by law or in the legitimate interests of CYP's charitable activities. Where applicable, data sharing agreements will be in place to ensure compliance with UK GDPR.

Whenever possible, data subjects will be informed in advance of the necessity to share their personal data with a Third Party in pursuit of CYP's Objectives.

N.B. although collated CYP data may be passed to a third party (funders), such as, number of small groups or small group's attendance, no personal data will be disclosed.

CYP will ensure that all third-party processors enter into GDPR-compliant data processing agreements that set out their obligations and safeguards.

Reporting Breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. CYP has a legal obligation to report any data breaches to the Information Commissioner's Office (ICO) within 72 hours. All staff members are required to report actual or potential data protection compliance failures to the Data Protection Lead. This enables us to:

- Investigate the failure and take necessary remedial actions
- Maintain a register of compliance failures
- Notify the ICO of any material compliance failures, whether they occur individually or as part of a pattern of failures

The Data Protection Lead will inform the ICO and then the trustees and if necessary, individuals affected by the breach (by Telephone and or Email).

Failure to report a breach, or knowingly or suspecting a breach has occurred and not following the correct reporting procedures, will result in disciplinary action.

CYP will document all data breaches, whether reportable or not, in accordance with ICO expectations.

Upshot Database

Information contained on the database will not be used for any other purposes than set out in this section. The database is accessed through the cloud and therefore, can be accessed through any

computer or smart device with internet access. The server for the database is maintained and held by the Football Foundation.

1. Access to the database is strictly controlled through the use of name specific passwords, which are selected by the individual.
2. Those authorised to use the database only have access to their specific area of use within the database. This is controlled by the Data Controller and other specified administrators. These are the only people who can access and set these security parameters.
3. People who will have secure and authorised access to the database include CYP Staff & data in-putters (Mentors & Volunteers).
4. The database will NOT be accessed by any unauthorised users outside of the UK, in accordance with the Data Protection Act. In cases where international data transfers are necessary, CYP will ensure that appropriate safeguards are in place, such as Standard Contractual Clauses (SCCs) or an adequacy decision, in compliance with UK GDPR.
5. All access and activity on the database is logged and can be viewed by the Database Controller.
6. Subject Access - all individuals who are the subject of personal data held by CYP are entitled to:
    - Subject Consent - The need to process data for normal purposes has been communicated to all data subjects. Ask what information CYP holds about them and why.
    - Ask how to gain access to it.
    - Be informed how to keep it up to date.
    - Be informed what CYP is doing to comply with its obligations under the Data Protection Act 2018.
7. Personal information will not be passed onto any third parties outside of CYP.

Where Upshot involves processing that is likely to result in high risk to individuals, CYP will conduct a Data Protection Impact Assessment (DPIA) before processing begins.

Destruction of Records

All records of young people and children who have left CYP in the previous year will be removed to the archives and then deleted / destroyed by shredding after a further period of 5 years. The five-year retention period is based on CYP's operational needs and relevant legal requirements. Some records, such as financial data, may be retained longer where required by law (e.g., six years for HMRC compliance).

Privacy Notices

CYP provides clear and transparent privacy notices outlining the purpose of the data collection, the legal basis for processing, and their rights under the UK GDPR. Privacy notices will be provided at the point of data collection, including registration forms, the CYP website, and other appropriate communication channels to ensure transparency.

Rights to Access Information

Employees and other subjects of personal data held by CYP have the right to access any personal data that is being held in certain manual filing systems. This right is subject to certain exemptions. Personal Information may be withheld if the information relates to another individual.

Any person who wishes to exercise this right should make the request in writing to the CYP Data Officer, using the standard letter which is available online from www.ico.gov.uk.

In addition to access rights, individuals also have the rights to rectification, erasure, restriction of processing, data portability, objection, and rights related to automated decision-making, as set out in UK GDPR. If personal details are inaccurate, they can be amended upon request.

CYP aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within 30 days of receipt of a completed form unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

Policy Review and Updates

CYP will regularly review this Data Protection Policy to ensure its compliance with current data protection legislation and best practices. The policy will be updated as needed to reflect any changes in the law, ICO guidance, or CYP's data processing activities. All updates will be communicated to staff, volunteers, and any relevant stakeholders.

Data protection Policy understanding and acceptance:

Name:
Position/ role:
Dept:

I function in the roles below (please circle those that are applicable)
Staff member / Data input team member (Mentor or Volunteer)

I have read and understood this policy and agree to adhere to its contents.
Signed:
Date: