Chipukeezy Youth Empowerment Foundation
TALA, MACHAKOS COUNTY, KENYA

GOVERNANCE · POLICY 07

Data Protection Policy

How CYEF collects, uses, stores and disposes of personal information and what staff must do to meet the Data Protection Act, 2019.

Document	Data Protection Policy (internal)
Version	1.0
Owner	CYEF Board of Directors
Date adopted	pending board adoption
Review cycle	Reviewed every two years
Public counterpart	The CYEF Privacy Policy published at chipukeezyfoundation.org
Regulator	Office of the Data Protection Commissioner, odpc.go.ke

1. Purpose and scope

CYEF holds personal information about children, parents and guardians, staff, volunteers, donors and partners. Some of it is sensitive: health details, safeguarding records and information about children in difficult circumstances.

This policy sets out how that information is handled. It applies to every director, employee, coach, volunteer, intern, contractor and partner who processes personal data for CYEF, in any format, whether on paper, on a phone, in a spreadsheet or in a messaging app.

The public-facing Privacy Policy tells people what CYEF does with their data. This document tells staff what they must do.

2. The principles

Under the Data Protection Act, 2019, personal data must be:

- Processed lawfully, fairly and transparently
- Collected for a specified, explicit and legitimate purpose and not used for something else without a new basis
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- Kept no longer than necessary
- Protected by appropriate security
- Not transferred outside Kenya except under the conditions in section 48 of the Act

> The practical version: collect only what you need, use it only for the reason you collected it, keep it secure and get rid of it when it has served its purpose. If you cannot explain why CYEF holds a piece of information, CYEF should not be holding it.

3. What CYEF holds, and why

Category	Examples	Lawful basis
Programme participants	Name, age, sex, school, guardian contact, attendance	Consent, and legitimate interest in running the programme safely
Health and emergency data	Conditions, allergies, medication, emergency contacts	Consent, and protection of vital interests in an emergency

Category	Examples	Lawful basis
Safeguarding records	Concerns, disclosures, referrals, outcomes	Legal obligation under the Children Act, 2022 and protection of vital interests
Images and stories	Photographs, video, case studies	Consent, recorded on the CYEF media consent form
Staff and volunteers	Applications, contracts, references, Police Clearance Certificates, payroll	Contract, and legal obligation under the Employment Act, 2007
Donors and supporters	Name, contact details, donation records	Contract, legal obligation for financial records and consent for marketing
Website visitors	Cookie preference, anonymous engagement data	Consent

3.1 Sensitive personal data

Health information, information about children and safeguarding records carry a higher duty. They are collected only where genuinely necessary, held separately from general files and accessible only to named individuals.

4. Rules for staff

4.1 Collecting

- Tell people what you are collecting, why and who will see it
- Collect the minimum. Do not ask for an identity number, a home address or a photograph unless there is a clear reason
- Use CYEF forms. Do not gather participant details in a personal notebook or a private chat
- For children, collect through the parent or guardian using the consent forms

4.2 Storing

- Paper records go in a locked cabinet, not a desk drawer or a bag
- Digital records go on CYEF-controlled storage, protected by a password and, where available, two-factor authentication
- Devices holding personal data are locked with a passcode and are not shared
- Do not store participant lists, consent forms or safeguarding notes on a personal phone, personal email or a personal cloud account
- Safeguarding files are stored separately, with access limited to the Safeguarding Focal Person and the Board Chair

4.3 Sharing

- Share on a need-to-know basis only
- Never share a participant list, contact details or images with a partner, sponsor or media outlet without checking the consent that covers it
- Use blind copy when emailing a group, so addresses are not exposed to each other
- Check the recipient before sending. Misdirected email is the most common breach in small organisations
- Safeguarding information is shared with authorities entitled to receive it, and with nobody else

4.4 Disposing

- Follow the retention schedule below
- Paper is shredded, not binned
- Digital files are deleted from the store and from backups where practicable
- Devices are wiped before disposal, resale or reassignment

5. Retention schedule

Record	Retention period	Reason
Programme participation and consent forms	7 years after participation ends	Reporting, audit and the possibility of a later claim
Child protection and safeguarding records	7 years after the child's 18th birthday	Matters may be raised long after the event
Health and emergency information	End of the programme year, unless part of an incident record	No longer needed once the activity ends
Images and stories	5 years from consent, reviewed annually	As stated on the consent form
Employment records	7 years after employment ends	Employment Act, 2007 and tax requirements
Police Clearance Certificates	Retained while engaged, renewed every 12 months	Vetting is only meaningful if current
Financial and donation records	7 years	Accounting and tax obligations
Enquiries through the website	24 months	Follow-up and reporting

Record	Retention period	Reason
Job applications from unsuccessful candidates	6 months	Recruitment queries

6. Rights of individuals

Under section 26 of the Act, a person whose data CYEF holds has the right to:

- Be informed of the use of their personal data
- Access their personal data
- Object to processing of their personal data
- Correct false or misleading data
- Have false or misleading data deleted

In practice CYEF also acts on requests to withdraw consent, to stop receiving communications and to remove an image.

6.1 Handling a request

1. Pass it to the Board Chair on the day it arrives, however it came in
2. Verify the identity of the person making the request, and the authority of anyone acting for a child
3. Respond within **30 days**. Where the request is complex, tell the person and explain the delay
4. Do not charge a fee for a reasonable request
5. Redact information about other people before releasing a record
6. Log the request, the response and the date

Requests involving children are handled with particular care. Where a guardian asks for records about a child, consider whether releasing them could place the child at risk and take advice before responding.

7. Data breaches

A breach is any loss, unauthorised access, unauthorised disclosure or destruction of personal data. A lost phone, a misdirected email, a stolen file and a shared password are all breaches.

> **72 hours**
>
> Where a breach is likely to result in a real risk to the rights and freedoms of the people affected, section 43 of the Data Protection Act, 2019 requires notification to the Data Commissioner within **72 hours** of becoming aware of it. That clock starts at discovery, not at the end of the investigation.

7.1 What to do

1. **Report it immediately** to the Board Chair. Do not attempt to fix it quietly first
2. **Contain it.** Recall the email, disable the account, recover the device, change the password
3. **Assess.** What data, how many people, what harm could follow. Record the reasoning
4. **Notify the Data Commissioner** within 72 hours where the risk threshold is met
5. **Tell the people affected** where there is a real risk to them, in plain language, with what they can do
6. **Record and learn.** Log every breach, including those not reported externally and change practice

Breaches involving children's data or safeguarding records are treated as high risk by default.

8. Transfers outside Kenya

Some CYEF tools, including email and cloud storage, may hold data outside Kenya. Section 48 of the Act permits this where there are appropriate safeguards, where the transfer is necessary for the performance of a contract or where the person has consented having been told of the risks.

Before adopting a new tool that stores personal data, check where the data will be held and what protections apply. Record the decision.

9. Working with partners and suppliers

- Where a partner processes personal data for CYEF, there must be a written agreement covering purpose, security, retention and deletion
- Partners may not use CYEF data for their own purposes without a separate basis
- Check a supplier's security arrangements before sharing anything sensitive
- Photographers and media crews are given data as narrowly as the job requires, and confirm deletion afterwards

10. Training and accountability

- Everyone handling personal data receives data protection training at induction and refreshers annually
- The Board Chair holds overall accountability, and CYEF will appoint a Data Protection Officer if the Act or the Data Commissioner requires one
- An annual review checks what data CYEF holds, why, where it sits and whether anything can be deleted
- Breaching this policy is a disciplinary matter. Deliberate misuse of personal data may also be a criminal offence

---

Read alongside the public Privacy Policy, the Child Safeguarding and Child Protection Policy, the Incident Reporting and Escalation Procedure and the Media, Photography and Image Use Guidance. Complaints may be made to the Office of the Data Protection Commissioner at odpc.go.ke.