



Promoting Support for Quality Education for All

## **Data Protection Policy (DPP)**

**April, 2026**

## Table of Contents

Table of Contents.....	1
Vision.....	2
Mission.....	2
Principles.....	2
1. Introduction .....	3
2. Purpose of the Policy.....	3
3. Scope of the Policy .....	3
4. Key Definitions Used .....	4
5. Data Protection Principles.....	4
6. Data Collection and Processing Activities of the Organisation .....	4
7. Types of Personal Data Collected.....	5
8. Rights of Data Subjects.....	5
9. Procedures for Exercising Data Subject Rights and Handling Data Privacy Complaints .....	6
10. Security Measures to Protect Personal Data .....	6
11. Procedures for Data Breach Management: .....	6
12. Data Retention Periods and Procedures .....	7
13. Procedures for Disposal of Personal Data.....	7
14. Responsibilities of Management, Departments, Employees, Data Protection Officer and Third Parties .....	7
15. Procedures for Data Sharing .....	8
16. Contact Details of the Data Protection Officer .....	8
17. Review Dates of the Policy .....	8
18. Approval of the Policy by the Board of Directors.....	9
References .....	9

## **Vision**

A society in which all children are learning and realising their full potential

## **Mission**

To promote support for quality education for all through assessment, research, engagement and influencing, in collaboration with other stakeholders

## **Principles**

Treat all children as equal

Understand the context

Prioritise lasting practical changes

Work evidence-based

Develop appropriate content

Be prepared to adapt

Collaborate based on trust and mutual respect

## 1. Introduction

Uwezo Uganda is a non-profit civil society organisation dedicated to promoting support for quality education for all children in Uganda through citizen-led assessments, research, engagement and influencing. In line with our 2025-2028 Strategy ('Promoting Support for Quality Education for All'), we collect and process personal data to generate evidence on learning outcomes (e.g. through household-based assessments of children aged 4-16 years and young people aged 13-20 years) and support systemic change in education.

This Data Protection Policy sets out Uwezo Uganda's commitment to protecting the privacy and rights of all data subjects, including children, parents/guardians, teachers, volunteers, staff, partners and stakeholders, in accordance with Uganda's Data Protection and Privacy Act, 2019 (Cap. 97) (the 'Act') and the Data Protection and Privacy Regulations, 2021. We recognise that data protection is integral to our child safeguarding policy, ethical research practices, and building public trust.

## 2. Purpose of the Policy

The purpose of this policy is to:

- a) Ensure full compliance with the Act and best international practices.
- b) Protect the privacy, rights and freedoms of data subjects
- c) Establish clear standards, procedures, and responsibilities for the lawful, fair, and secure handling of personal data.
- d) Mitigate risks associated with our core activities (assessments, research and stakeholder engagement) while enabling us to fulfil our mission.

## 3. Scope of the Policy

This policy applies to:

- a) All personal data collected, processed, stored, shared or disposed of by Uwezo Uganda, in electronic or manual form.
- b) All persons acting on behalf of Uwezo Uganda, including employees, Board members, volunteers/enumerators, consultants, interns, and third-party data processors.
- c) All activities aligned with our organisational strategy, including learning assessments, research, national and subnational engagements, monitoring/evaluation/learning (MEL), human resources, partner collaborations, stakeholder engagement, website and social media operations, and donor reporting.
- d) Data processed within Uganda or relating to Ugandan data subjects, including any cross-border transfers.

All in all, the policy applies organisation-wide and is binding on all relevant parties.

#### 4. **Key Definitions Used** (As defined in Section 2 of the Act)

- Data Subject: An individual whose personal data is collected, processed, held or used (e.g. assessed children, parents, teachers, staff, volunteers, etc.)
- Personal Data: Any information relating to an identified or identifiable living individual, including name, age, gender, location, education level, assessment results, contact details, and opinions.
- Special Personal Data: Personal data revealing religious or philosophical beliefs, political opinions, sexual life, financial status, health/medical records, or data relating to children.
- Data Controller: Uwezo Uganda – the entity that determines the purpose and means of processing personal data.
- Data Processor: Any person or entity other than Uwezo Uganda employees who processes personal data on our instructions e.g. volunteers/enumerators, research and assessment consultants, district partners, etc.
- Consent: Any freely given, specific, informed and unambiguous indication of the data subject's wishes (by statement or clear affirmative action). For children under 18, parental/guardian consent is required.
- Personal Data Breach: Any incident leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.
- Processing: Any operation performed on personal data (collection, recording, organisation, storage, use, disclosure, deletion, etc.
- Third party: Any person or entity other than the data subject, controller or processor.

#### 5. **Data Protection Principles**

Uwezo Uganda shall comply with Section 3 of the Act. All processing of personal data shall adhere to the following principles:

- a) Accountability to the data subject for any data collected, processed, held, or used;
- b) Fair and lawful collection and processing;
- c) Data minimisation – collect only what is adequate, relevant, and not excessive;
- d) Purpose limitation – collect only for a specified, explicit, and legitimate purpose;
- e) Data quality – ensure data is accurate, complete, and up to date;
- f) Storage limitation – retain data only as long as necessary;
- g) Security safeguards – implement appropriate technical and organisational measures; and
- h) Transparency and participation of the data subject, including respect for their rights.

#### 6. **Data Collection and Processing Activities of the Organisation**

Uwezo Uganda processes personal data in support of our organisational strategy pillars (Assessment, Research, Engagement & Influencing, MEL and Organisational Development):

- Citizen-led assessments: Household-based surveys conducted by trained community volunteers/enumerators assessing foundational literacy, numeracy, life skills and related

competencies for children, adolescents and young people aged 4-20 years. This also includes collection of contextual community, household, parental and school data.

- Research studies: Mixed-method research (surveys, interviews, case studies) on factors affecting learning (e.g. family/community influences, exposure to early childhood education, school funding, special education needs, etc.).
- Engagement, influencing and MEL: Stakeholder consultations, contact management. Media/communications, outcome harvesting, and evidence dissemination.
- Organisational development: Human resources (staff/interns/volunteers/consultants), donor reporting, partner coordination, and administrative functions.

Data processing is based on lawful and ethical grounds: consent (especially for child assessments and research), legitimate interests (evidence generation and advocacy), and public interest (education improvement). All data is pseudonymised/anonymised for reports as much as possible.

## 7. Types of Personal Data Collected

Uwezo Uganda collects the following types of data:

- Assessment/research participant data: Child demographics (name where necessary, age, gender, village/district, school status, age), literacy/numeracy/life skills results, and household characteristics (parent education, home environment).
- Special category / sensitive data: Data on children with special educational needs/disabilities, health indicators, or vulnerable status such as those in refugee contexts or displaced communities (processed with explicit safeguards and consent).
- Staff, intern, volunteer/enumerator / consultant data: Names, national ID, contact details, qualifications, bank details, training records, employment/performance data.
- Partner/stakeholder/consultant data: Contact information (names, emails, phones) for district partners, government officials, schools, donors, media and community leaders.
- Other: Feedback/opinions from engagements, event registrations, and financial transaction data

We do not collect unnecessary sensitive data and prioritise aggregation and anonymisation for public outputs.

## 8. Rights of Data Subjects

Consistent with the Act, we ensure our data subjects have the right to:

- a) Be informed about processing (purpose, lawful basis, recipients)
- b) Access their personal data
- c) Request rectification/correction of inaccurate or incomplete data)
- d) Request erasure/deletion (where data is no longer necessary or processing is unlawful)
- e) Withdraw consent at any time (where consent is the basis)
- f) Object to or restrict processing (including for direct marketing or where it causes distress)
- g) Lodge complaints with Uwezo Uganda or the Personal Data Protection Office (PDPO).

## **9. Procedures for Exercising Data Subject Rights and Handling Data Privacy Complaints**

- a) Submit requests in writing or by email to the Data Protection Officer (DPO), using our official email address that is publicly available on our website
- b) We will verify (free of charge unless manifestly unfounded/excessive) and respond without undue delay (normally within 30 days; extensions notified)
- c) Complaints are acknowledged within 7 days, investigated thoroughly, and resolved or escalated
- d) All requests/complaints are logged, outcomes documented, and reported to senior management where appropriate
- e) Unresolved issues may be referred to the PDPO.

## **10. Security Measures to Protect Personal Data**

Uwezo Uganda implements appropriate technical and organisational measures (per Section 20 of the Act), including:

- Role-based access controls
- Secure servers, firewalls, antivirus, regular backups, and vulnerability assessments
- Physical security (locked offices, safe for storing sensitive information, secure filing for paper records)
- Mandatory data protection training for all staff and data collectors upon onboarding and annually
- Data protection impact assessments for new/high-risk projects
- Contracts with third parties containing data processing agreements (DPAs)
- Integration with our Child Protection and Safeguarding Policy

## **11. Procedures for Data Breach Management:**

In the event of a suspected breach, we will:

- a) Contain the incident and notify the DPO/Senior Management immediately (within 24 hours).
- b) Assess scope, risks to data subjects and impact.
- c) Notify the PDPO without undue delay.
- d) Notify affected data subjects without undue delay if the breach poses a high risk to their rights and freedoms.
- e) Document the breach, conduct root-cause analysis, implement remedial actions, and update the breach register.
- f) Review and strengthen controls post-incident.

## 12. Data Retention Periods and Procedures

Personal data is retained only as long as necessary for the stated purpose or as required by law. We maintain a Retention Schedule reviewed annually by the DPO. Examples of our data retention practices include the following:

- Raw assessment/research data (identifiable): Up to 5-7 years after report publication (for verification/audit, then anonymised or deleted).
- Aggregated/anonymised data: Indefinitely for reference and MEL.
- HR/employment records: Duration of relationship + 6 years (or statutory minimum for taxes/labour law).
- Volunteer/partner contact data: Duration of active relationship + 2 years (or until they opt-out).
- Consent records: Duration of processing + 2 years.

Archived data receives restricted access.

## 13. Procedures for Disposal of Personal Data

When retention data expires, we do the following:

- Electronic data: Secure permanent deletion/overwriting using certified tools
- Paper records: Cross-cut shredding or certified destruction services
- Disposal is approved by the DPO, logged with date/method/responsible person, and witnessed for sensitive data
- Third parties must follow equivalent secure disposal procedures.

## 14. Responsibilities of Management, Departments, Employees, Data Protection Officer and Third Parties

The following responsibilities apply to the different stakeholders:

- a) Board of Directors: Overall accountability, policy approval, resource allocation, and oversight of compliance
- b) Senior Management/Heads of Units: Ensure team compliance, report issues, and support Data Protection Impact Assessments (DPIAs).
- c) Employees, Volunteers/Enumerators and Interns: Comply with this policy, complete mandatory training, handle data securely, obtain valid consent where required, and report breaches/incidents immediately.
- d) Data Protection Officer (DPO): Day-to-day monitoring of compliance, advice on DPIAs/rights requests/breaches, training delivery, liaison with PDPO and data subjects, maintenance of records, and policy reviews.
- e) Third Parties/Processors/Partners: Subject to due diligence, written DPAs or data-sharing agreements, and ongoing monitoring. They must meet equivalent standards and allow audits.

## 15. Procedures for Data Sharing

We share data based on the following procedures:

- Sharing occurs only where necessary, with a lawful basis, and on a need-to-know/minimized basis
- Internal sharing: Strictly on a need-to-know basis
- External sharing with processors/partners: This requires written Data Processing Agreements (specifying purpose, security, sub-processing restrictions, audit rights, return/deletion of data upon termination)
- With other recipients (e.g. government, funders, research collaborators, academics): Data Sharing Agreements or consent; preferably anonymised/aggregated data
- Cross-border transfers: This is done only with adequate safeguards (e.g. contractual basis) or to countries with equivalent protection (e.g. those within the East African Community); subject to PDPO guidelines where applicable.
- No sale of personal data. All sharing of data is recorded and reviewed periodically.

## 16. Contact Details of the Data Protection Officer

The Data Protection Officer can be contacted at:

Name: Judith Nyakaisiki, Human Resources Associate & Communications Officer

Email: [jnyakaisiki@uwezouganda.org](mailto:jnyakaisiki@uwezouganda.org) or [info@uwezouganda.org](mailto:info@uwezouganda.org)

Tel: +256 393 193441

Address: Uwezo Uganda, Corner House, Suite B1, Plot 436/437, Mawanda Road  
Kamwokya, Kampala. P.O Box 33275, Kampala, Uganda

## 17. Review Dates of the Policy

Given the sensitivity of this policy, it will be reviewed every two years or sooner following changes in law, operations, strategy or significant incidents.

## 18. Approval of the Policy by the Board of Directors

This policy was approved by the Board of Directors of Uwezo Uganda.

**Date:** 7<sup>th</sup> April 2026

**Signed:** .....  .....

**Name:** Prof Albert James Lutalo-Bosa  
Chairperson, Uwezo Uganda Board of Directors

## References

The Data Protection and Privacy Act, 2019 (Act No. 9 of 2019) (Chapter 97 of the Laws of Uganda)

The Data Protection and Privacy Regulations, 2021 (Statutory Instrument No. 21 of 2021)

Uwezo Uganda Child Protection and Safeguarding Policy (2020) Adapted from Twaweza East Africa 2018  
Child Protection and Safeguarding Policy