KARAMOJA TUMAINI NETWORK · KTN

Data Protection and Privacy Policy

Holding the information of Karamoja's children, families and communities with care

Policy Category Governance Policy · Classification: Public

Adopted by the Board of Directors June 2026

Status Version 1.0 · Effective June 2026 · Next review June 2028

A KARAMOJONG-LED CHILD PROTECTION ORGANISATION · KAMPALA & NAPAK, UGANDA

OUR COMMITMENT

Karamoja Tumaini Network commits to holding the information of children, families and communities with the same care it holds the children themselves. We collect only what a purpose requires, keep it only as long as that purpose lasts, and guard it for as long as we hold it.

Consent is asked for in a language people understand, and refusing it never costs anyone the help they came for. Where a child's information is concerned, the child's best interests settle the question. Every breach is reported, recorded and learned from.

WHY IT MATTERS

A case file is not a row in a spreadsheet. It carries a name, a village, a family that may be part of the reason a child left, and sometimes the whereabouts of the person the child is being protected from. Information that leaks does not merely embarrass an organisation. It can put a child back within reach of the people who harmed them. Uganda's Data Protection and Privacy Act makes this a legal duty; the children make it a moral one.

WHERE IT APPLIES

Every person who handles information for or on behalf of KTN, in either office, in the field, and on any device. Every record, on paper or in a system, from a consent form to a dashboard. Every partner, processor and supplier that touches KTN's data, for as long as they hold it.

HOPE · HEAL · EMPOWER

Behind every record is a child who did not choose to be in it.

DATA PROTECTION AND PRIVACY POLICY · KARAMOJA TUMAINI NETWORK

Contents

Version 1.0 · Effective June 2026 · Next review June 2029

List of Tables

List of Figures

The KTN mark on the cover and the colour system throughout follow the KTN Brand Style Guide, Version 1.0, and are not numbered as figures.

Policy Approval

This Data Protection and Privacy Policy was considered and approved by the Board of Directors of Karamoja Tumaini Network in June 2026 and takes effect from that date as a governance instrument of the organisation. It establishes the organisation's standards for the responsible, lawful, ethical and secure management of information. Compliance with it is mandatory for everyone within the scope set out in Section 2.2. The resolution reference and the signatures below complete the formal record of adoption.

Item	Detail
Policy status	Approved
Approval authority	Board of Directors
Approval date	June 2026
Effective date	June 2026
Version	1.0
Board resolution reference	KTN/BRD/RES/2026/____

The Board Secretary enters the resolution number from the minutes of the approving meeting before the signed copy is filed.

APPROVAL SIGNATURE

Chairperson, Board of Directors
Karamoja Tumaini Network · June 2026

A Statement of Commitment from the Board

KTN exists to keep Karamojong children safe, and almost everything we do to keep them safe produces information about them. A case file names a child who ran from home. A reintegration record describes a household a child was returned to. A health screening notes a condition a family would not want spoken aloud in the trading centre. A research dataset, gathered to understand why children leave, holds the answers of hundreds of people who trusted us with them. This information is not paperwork. In the wrong hands it can find a child who must not be found, expose a survivor, or break the trust that makes our work possible at all.

The Strategic Plan makes Data one of the six pillars of the SHIELD model, because evidence is how KTN learns and how it earns the right to be believed. But the same plan is clear that data is a duty before it is an asset. This policy is how the Board makes that duty real. It is deliberately honest about what KTN is: a young, Karamojong-led organisation, not a technology company, working in places where a phone is more common than a filing cabinet and a connection is never guaranteed. The commitments here are ones an organisation of this size can actually keep.

We commit to obeying Uganda's data protection law in full, to collecting only what we need, to guarding what we hold, to telling people plainly what we do with their information, to treating a child's data as carefully as we treat the child, and to owning our mistakes when we make them. The Board has approved and adopted this policy, will fund its implementation, will appoint the officer it requires, and will receive the annual report it demands. It binds every one of us, from the boardroom to the furthest kraal.

Chairperson, Board of Directors

Karamoja Tumaini Network

Adopted by resolution of the Board of Directors, June 2026.

Document Control

Field	Detail
Policy title	Data Protection and Privacy Policy
Registered name	Karamoja Tumaini Network Limited, a company limited by guarantee without share capital, Reg. No. 80034272074698, incorporated on 1 July 2025 under the Companies Act, 2012 (Cap. 106)
Version	1.0
Status	Approved and adopted by the Board of Directors
Approval date	June 2026
Effective date	June 2026
Policy owner	Karamoja Tumaini Network, acting through its Board of Directors and the Executive Director
Policy custodian	The Data Protection and Privacy Officer (a designated focal person), supported by the Executive Director
Applies to	All board members, staff, volunteers, peer educators, interns, consultants, contractors, partners and visitors who handle KTN information, at every KTN office, activity and site, and on every device and system used for KTN work
Reads alongside	The Strategic Plan 2026 to 2030; the Child Safeguarding Policy; the PSEA Policy; the IT and AI Use Policy; the Human Resources and People Management Policy; the Procurement Policy; the Finance and Anti-Fraud Policy; the Complaints and Community Feedback Policy; the Health, Safety and Security Policy; the Environmental Policy; the Gender Equality and Social Inclusion Policy; and the Whistleblowing Policy
Definitions	Key terms are defined in Section 3.3; acronyms and abbreviations are listed at the front of this document
Review frequency	Every three years, or earlier where required by a change in law or regulation, a donor requirement, organisational restructuring, a revision of the Strategic Plan, a safeguarding development, a technology development, an emerging organisational risk, a serious data breach, or the direction of the Board (Section 9.2)
Next scheduled review	June 2029

Version Control Register

Version	Date	Description of change	Approved by
1.0	June 2026	First edition. Full policy developed, reviewed and adopted as a governance instrument of Karamoja Tumaini Network.	Board of Directors

Amendment History Register

No.	Date	Section(s) affected	Summary of amendment	Approved by
1	16 August 2026	Front matter; Contents; Chapter 1; new Section 8.3; cross-references throughout	Presentation and completeness update. Executive Summary moved from Section 1.1 into the front matter and Organisational Context renumbered 1.1; Contents rebuilt as one live field listing sub-headings and annexes; new Section 8.3, Records, Audit Trail and Retention; eight cross-references to a superseded section scheme corrected; front-matter pages given the running band and roman page numbers; inside-cover commitment page and closing page added; Chairperson's signature applied to the Policy Approval page. Approved by the Executive Director as an administrative update under Section 9.2.	Executive Director

Completed by the policy custodian as amendments are approved under Section 9.2. Until an amendment is made, this register intentionally remains blank.

Distribution List

Recipient	Format	Date issued
Board of Directors	Electronic copy and one signed print copy for the corporate record	June 2026
Executive Director and all staff	Electronic copy; included in the staff induction pack	June 2026
Volunteers and peer educators	Induction summary, in English and Nga'Karamojong as needed	At induction
Partners, contractors and suppliers	Relevant extracts issued with their agreements and data sharing agreements	With each agreement
Donors	Full copy in due diligence and assessment packs	On request
Public	Published on the KTN website, www.karamojatumaini.org	From adoption

The policy custodian keeps this list current. The authoritative version of this policy is the signed copy held by the custodian; numbered electronic copies carry the same text.

Contact Information

Item	Detail
Policy owner	Karamoja Tumaini Network
Policy custodian	The Data Protection and Privacy Officer, supported by the Executive Director
Data protection contact	dataprotection@karamojatumaini.org
Kampala office	Da Joy House, Room JS05A, Waliggo Road, Komamboga, P.O. Box 10066, Kampala
Napak office	C/o Matany Trading Centre, Matany Town Council, Napak District
General email	info@karamojatumaini.org

Item	Detail
Website	www.karamojatumaini.org

Acronyms and Abbreviations

Acronym	Meaning
AI	Artificial Intelligence
CPC	Child Protection Committee
CRC	United Nations Convention on the Rights of the Child
DPIA	Data Protection Impact Assessment
DPO	Data Protection and Privacy Officer
DPPA	Data Protection and Privacy Act, No. 9 of 2019
GDPR	General Data Protection Regulation (European Union)
ICRC	International Committee of the Red Cross
ISO	International Organization for Standardization
IT	Information Technology
KCCA	Kampala Capital City Authority
KTN	Karamoja Tumaini Network
MEAL	Monitoring, Evaluation, Accountability and Learning
NITA-U	National Information Technology Authority, Uganda
OECD	Organisation for Economic Co-operation and Development
PDPO	Personal Data Protection Office (Uganda)
PSEA	Protection from Sexual Exploitation and Abuse
RD4C	Responsible Data for Children (UNICEF and The GovLab)
S.I.	Statutory Instrument
SHIELD	Safeguard, Heal, Integrate, Empower, Lead, Data: the framework of the KTN Strategic Plan
UBOS	Uganda Bureau of Statistics
UNICEF	United Nations Children's Fund
VSLA	Village Savings and Loan Association

Key terms used in this policy are defined in Section 3.3.

Executive Summary

This is Karamoja Tumaini Network's authoritative framework for protecting the information it holds. It was reviewed and adopted by the Board of Directors in June 2026 and applies to every person who works for or with KTN, on every device and system used for KTN work, in every place where KTN operates, regardless of the source of funding.

KTN handles some of the most sensitive information any organisation can hold: the names, histories and whereabouts of children who have run from home or been found on the street; the circumstances of families a child may be returned to; health and protection details that could expose a survivor; and research data gathered from hundreds of people on the understanding that it would be handled with care. A leak here is not an administrative embarrassment. It can put a child in danger. That is why this policy exists, and why it is written plainly enough for everyone bound by it to follow.

The policy does four things. First, it sets out KTN's commitments and the principles behind them, anchored in the Constitution of Uganda, the Data Protection and Privacy Act, 2019 (Cap. 97) and its 2021 Regulations, and the international standards Uganda's law gives effect to, including the UNICEF Responsible Data for Children principles. Second, it sets practical standards for the whole life of information at KTN: how it is collected, the lawful basis for holding it, how consent is sought, how it is secured, how long it is kept, and how it is destroyed. Third, it gives children's data the heightened protection it requires, in line with the Child Safeguarding Policy and the best-interests principle that governs everything KTN does. Fourth, it builds the governance, monitoring and breach-response arrangements that make the commitments real, including a designated Data Protection and Privacy Officer, a small set of honest indicators, and an annual report to the Board.

The policy is deliberately proportionate. KTN is a young, growing Ugandan organisation, not a technology company, and the commitments here are ones it can actually keep. Where specialist expertise is needed, KTN partners rather than pretends. Where a control is aspirational rather than already in place, the policy says so and sets a date. That honesty is itself a KTN value, and it runs through every section that follows.

1

CHAPTER ONE

INTRODUCTION

Why this policy exists and the context it serves.

1 Introduction

Why this policy exists and the context it serves.

1.1 Organisational Context

Karamoja Tumaini Network Limited is a Karamojong-led, child-focused organisation incorporated in Uganda as a company limited by guarantee. It works to break the cycle that pushes children from the Karamoja sub-region onto the streets of Kampala and other urban centres, and to give those already on the streets a credible, culturally grounded route back to school, family and stable life. Its work runs the length of the migration corridor, from the source districts of Napak, Moroto, Kotido and Kaabong, through the road towns, to Kampala and across the border into Kenya, organised under the six pillars of the SHIELD framework: Safeguard, Heal, Integrate, Empower, Lead and Data.

Information runs through every one of those pillars. Safeguard generates case files, household assessments and reintegration records. Heal generates health and psychosocial notes. Integrate follows a child through school re-entry and family tracing. Empower records the households in livelihood and savings work. Lead documents the partners and authorities KTN coordinates with. And Data, the sixth pillar, is built on the longitudinal study of why children leave and what brings them home, which means asking hundreds of children and families to share things they would not tell a stranger. KTN cannot do this work without collecting personal data, and it cannot keep the trust the work depends on unless it protects that data well.

9 districts
of Karamoja where KTN collects personal information from children, families and communities

~500 km
of migration corridor along which case information moves between field, office and partners

Children
whose data carries the highest risk of harm if it is lost, leaked, sold or misused

Zero
tolerance for handling a child's information in a way that could put that child in danger

Figure 1. What KTN holds, and why it matters.

> *A child's information can find a child. We hold it as carefully as we hold the child.*
>
> Statement of Commitment, this policy

This policy reads alongside KTN's other governance documents, in particular the Child Safeguarding Policy and the PSEA Policy, which govern how KTN protects children and which take precedence wherever they are stricter; the IT and AI Use Policy, which governs the devices, systems and artificial intelligence tools through which most data now flows; the Human Resources and People Management Policy, which governs staff data and discipline; the Procurement and Finance and Anti-Fraud Policies, which govern supplier and donor data; and the Complaints and Community Feedback Policy, through which people raise concerns. Where those documents set the detailed procedure, this policy points to them rather than repeating them.

2

CHAPTER TWO

PURPOSE, OBJECTIVES AND SCOPE

What the policy is for, who it binds and where it applies.

2 Purpose, Objectives and Scope

What the policy is for, who it binds and where it applies.

2.1 Purpose of the Policy

This policy exists to:

1. establish a single, Board-approved framework for how KTN collects, uses, stores, protects, shares and disposes of information across all of its governance, operations, programmes, research and partnerships;
2. ensure full compliance with the Data Protection and Privacy Act, 2019 (Cap. 97), its Regulations, and the wider laws of Uganda, and with the international standards to which they give effect;
3. protect children, families, communities, staff, volunteers and partners from the harm that the loss, leak, sale or misuse of their information could cause;
4. set clear, practical standards that staff can apply every day, so that good data practice is the ordinary way KTN works rather than an exception for inspection week;
5. define responsibilities, measurable indicators, and reporting, breach-response and audit arrangements, so that KTN's data protection performance can be assessed by its Board, its donors, the regulator and the communities it is accountable to.

2.2 Scope and Applicability

This policy applies to every member of the Board of Directors and every member of staff, and to all volunteers, peer educators, community workers, interns, consultants and contractors engaged by KTN. It applies to partners, processors and suppliers to the extent set out in their agreements and data sharing agreements with KTN, and Sections 4.7 and 7.1 describe how those expectations are built in.

It applies to all personal data and confidential information KTN handles, in any form: paper files and registers; digital records, databases and spreadsheets; data collected through KoboToolbox and similar tools; photographs, audio and video; messages on phones and messaging apps used for work; email; and information held in the cloud or on any device. It applies regardless of whether the information sits in the Kampala office at Da Joy House, the Napak office at Matany, a field worker's notebook, a case manager's phone, a partner's system, or a donor's portal.

It applies in every place where KTN works: both offices; field operations across the nine districts of Karamoja, namely Abim, Amudat, Kaabong, Karenga, Kotido, Moroto, Nabilatuk, Nakapiripirit and Napak, and along the migration corridor; urban outreach locations; any drop-in centre or other facility KTN establishes; community events; travel on KTN business; and KTN's digital operations governed by the IT and AI Use Policy.

It applies to all of KTN's activities regardless of the source of funding, and whether or not a donor imposes data conditions of its own. Where a donor's requirements are stricter than this policy, the stricter requirement is followed. Where Ugandan law is stricter than either, the law prevails.

Nothing in this policy reduces any obligation under the Child Safeguarding Policy or the PSEA Policy. Where information concerns a child, or a survivor of abuse or exploitation, those policies apply in full and alongside this one.

Compliance is mandatory for everyone within scope. A breach by a member of staff or a volunteer is handled under the Human Resources and People Management Policy and may result in disciplinary action, up to and including dismissal. A breach by a partner, processor, contractor or supplier is handled under its agreement with KTN, up to and including termination. Conduct that is also an offence under the Data Protection and Privacy Act or any other Ugandan law is reported to the relevant authority.

2.3 Data Protection and Privacy Policy Statement

> *Karamoja Tumaini Network commits to protecting the information of every person it serves and every person it works with. We will obey Uganda's data protection law in full. We will collect only the information we genuinely need, and tell people plainly what we will do with it. We will keep what we hold accurate, secure and confidential, for only as long as we need it, and then destroy it safely. We will give children's data the heightened protection it demands, and weigh every decision against the best interests of the child. We will let people see, correct and, where the law allows, withdraw their information. We will report breaches honestly and fix what caused them. And we will measure our performance, report it to our Board, and improve year on year.*

This statement is displayed at every KTN office and included in staff induction materials.

3

CHAPTER THREE

GOVERNANCE FRAMEWORK

The law, the principles, the definitions and the structures through which KTN governs personal data.

3 Governance Framework

The law, the principles, the definitions and the structures through which KTN governs personal data.

3.1 Legal and Regulatory Framework

KTN's primary obligation is to the law of Uganda. The Constitution of the Republic of Uganda, 1995 protects, in Article 27, the privacy of a person, their home, correspondence, communication and property. The Data Protection and Privacy Act, No. 9 of 2019 (now Cap. 97 in the 2023 revised laws) and the Data Protection and Privacy Regulations, 2021 (S.I. No. 21 of 2021) give that right detailed effect: they set the principles of lawful processing, the rights of data subjects, the duties of data collectors, controllers and processors, the special protection of children's and sensitive data, the rules on processing data outside Uganda, and the requirement to deal honestly with security breaches. The Act establishes the Personal Data Protection Office (PDPO), which sits under the National Information Technology Authority, Uganda (NITA-U) and maintains the national data protection register.

Several other Ugandan laws bear on KTN's information handling and are read with this policy: the Children Act, Cap. 59, as amended, which makes the best interests of the child the first consideration in any matter concerning a child; the Computer Misuse Act, 2011 as amended; the Electronic Transactions Act, 2011 and the Electronic Signatures Act, 2011; the Regulation of Interception of Communications Act, 2010; the Access to Information Act, 2005 (Cap. 95); and the Registration of Persons Act, 2015. KTN registers as a data controller and processor with the PDPO and keeps that registration current, as Section 8.2 requires.

3.1.1 International standards KTN aligns with

KTN is not bound by foreign law simply by working with international partners, but it aligns its practice with the standards donors, regulators and peers expect, and which good child-focused data work follows in any case:

- the *United Nations Convention on the Rights of the Child*, especially Article 3 on the best interests of the child and Article 16 on the child's right to privacy;
- the UNICEF Responsible Data for Children (RD4C) principles, which shape Sections 4.4 and 6.3: purpose-driven, people-centric, participatory, protective of children's rights, proportional, professionally accountable, and preventive of harm;
- the *UN Personal Data Protection and Privacy Principles* (2018), the common baseline across the UN system KTN partners with;
- the *EU General Data Protection Regulation (GDPR)*, whose Article 5 principles KTN treats as the international reference point, and which some KTN donors require by contract;
- the *OECD Privacy Guidelines*, the *African Union Convention on Cyber Security and Personal Data Protection* (Malabo, 2014), and the *ICRC Handbook on Data Protection in Humanitarian Action*;
- the logic of *ISO/IEC 27001* on information security and *ISO/IEC 27701* on privacy management, whose cycle of plan, do, check and act KTN applies without claiming certification it does not hold.

Where these standards point in the same direction as Ugandan law, which is almost always, KTN follows both. Where any of them is stricter than the law, KTN treats the stricter standard as its own.

3.2 Guiding Principles

Eight principles guide how this policy is applied. When a situation arises that the policy does not expressly cover, decisions follow these principles. They restate, in KTN's words, the principles of the Data Protection and Privacy Act and the international standards above.

Lawfulness, fairness and transparency

KTN processes personal data only on a lawful basis, never by deception or pressure, and tells people in plain language what it collects, why, and what it will do with it.

Purpose limitation

Data is collected for a specific, stated purpose and not quietly reused for another. A consent given for case management is not a licence to put a child's photograph in a fundraising appeal.

Data minimisation

KTN collects the least information that will do the job, and no more. The temptation to gather everything because it might be useful one day is the opposite of protection. If a field is not needed, it is not asked.

Accuracy

Information is kept accurate and up to date, because a wrong address or a mistaken note in a child's file can do real harm. Errors are corrected promptly when found or reported.

Storage limitation

Data is kept only for as long as there is a lawful and operational reason to keep it, then destroyed safely under the schedule in Section 4.8 and Annex J. KTN does not hoard.

Integrity and confidentiality

Information is protected against loss, theft, unauthorised access and damage, by controls proportionate to its sensitivity. The more a record could harm someone, the harder it is guarded.

Children at the centre

A child's data is treated as carrying special risk. Every decision about it is weighed against the best interests of the child, today's and tomorrow's, consistent with the Child Safeguarding Policy and the CRC.

Accountability and honesty

KTN can show, not just assert, that it follows these principles: through registers, records and audit. When it gets something wrong, it says so, to the person affected, to the regulator where the law requires, and in its own reporting. An organisation that hides its data failures cannot be trusted with data.

3.3 Definitions and Key Concepts

In this policy, unless the context requires otherwise:

Term	Meaning
Personal data	Information about an identified or identifiable person, such as a name, photograph, location, phone number, case history, health detail or any combination that could identify someone.

Term	Meaning
Sensitive (special) personal data	Data the Act gives extra protection: a person's religious or philosophical beliefs, political opinions, sexual life, financial information, health status or medical records, and data about children. KTN also treats protection and safeguarding details, and the location of a child or survivor, as sensitive.
Data subject	The person the data is about: most often a child, a parent or guardian, a community member, a member of staff, a volunteer or a research participant.
Data controller	The party that decides why and how personal data is processed. For the data it gathers, KTN is a data controller.
Data processor	A party that processes data on a controller's behalf, such as a software provider that hosts KTN's records, or a partner collecting data under KTN's instructions.
Processing	Anything done with data: collecting, recording, organising, storing, using, sharing, transferring, altering or destroying it.
Consent	A freely given, specific, informed and unambiguous agreement to a stated use of one's data; for a child, the consent of a parent or guardian together, wherever possible, with the child's own assent.
Personal data breach	A security failure leading to the loss, theft, unauthorised access, alteration, disclosure or destruction of personal data, whether by accident or by act. Section 6.5 sets the response.
Anonymisation / pseudonymisation	Anonymisation removes identifiers so a person can no longer be identified. Pseudonymisation replaces identifiers with a code held separately, reducing but not removing risk.
Data Protection Impact Assessment (DPIA)	A structured assessment of the privacy risks of a new activity, system or research before it begins, and of how those risks will be reduced. The tool is at Annex C.
Data sharing agreement	A written agreement governing the disclosure of data between KTN and another party: what is shared, why, on what basis, for how long, and under what safeguards. The template is at Annex G.
Data Protection and Privacy Officer (DPO)	The named member of staff who holds day-to-day responsibility for this policy, as described in Sections 3.4 and 10.

3.4 Data Protection Governance Framework

Data protection governance at KTN follows the same chain of accountability as every other governance matter, with one addition: a named officer who keeps the day-to-day work moving.

The Board of Directors

The Board holds ultimate accountability for this policy. It approves the policy and any substantive amendment, appoints and resources the Data Protection and Privacy Officer through the Executive Director, receives the annual data protection report described in Section 8.2, reviews serious breaches, and satisfies itself once a year that the organisation is meeting its legal obligations and its own commitments.

Board sub-committees

The Finance and Audit Sub-Committee reviews data protection risks as part of its quarterly review of the organisational risk register, and reviews the findings of data protection audits. The Programmes Sub-Committee satisfies itself that privacy is built into programme and research design, as Sections 4.2 and 6.3 require.

The Executive Director

The Executive Director is accountable to the Board for implementation. The Executive Director designates the Data Protection and Privacy Officer in writing, ensures data protection responsibilities appear in the relevant job descriptions, approves the annual data protection work plan and budget line, decides on the response to breaches, and escalates serious breaches to the Board and, where the law requires, to the PDPO.

The Data Protection and Privacy Officer

The DPO is a named member of staff who, at KTN's current size, holds the role alongside other duties, with enough independence to raise concerns directly with the Executive Director and the Board. The DPO maintains the data processing register and the data protection risk register, coordinates DPIAs, oversees consent and data sharing arrangements, leads the response to breaches, organises training, keeps KTN's PDPO registration current, liaises with the regulator, and prepares the quarterly and annual reports. The role carries influence, not sole responsibility: protecting data belongs to everyone who touches it.

All staff, volunteers and associates

Every person covered by this policy is responsible for following it in their own work, for protecting the information they handle, for reporting breaches and concerns promptly, and for treating the data of children and communities with the same respect KTN asks for the children themselves.

4

CHAPTER FOUR

POLICY REQUIREMENTS

The binding standards for collecting, securing, sharing and retaining personal data, and the additional protection children's data requires.

4 Policy Requirements

The binding standards for collecting, securing, sharing and retaining personal data, and the additional protection children's data requires.

4.1 Types of Data Managed by KTN

KTN knows what it holds, because an organisation that cannot list its data cannot protect it. The processing register at Annex B records every category in detail, with its purpose, lawful basis, location, access and retention. The table below is the summary.

Category	What it includes	Sensitivity
Child and case data	Identity, history, location, family details, case notes, reintegration and follow-up records, household assessments	**Highest**
Health and protection data	Health screening notes, psychosocial records, disability information, abuse and exploitation disclosures	**Highest**
Beneficiary and community data	Participant lists, VSLA membership, livelihood records, attendance and distribution records	High
Research and learning data	Longitudinal study responses, interview and survey data, consent records, transcripts	High
Images and recordings	Photographs, audio and video of children, families and events, and their consent and usage records	High
Staff and volunteer data	Recruitment, contracts, payroll, performance, health and safeguarding-check records	High
Partner, donor and supplier data	Contacts, agreements, grant and due diligence records, financial details	Moderate
Operational and digital data	Email, messages, device and system logs, location data on KTN phones and vehicles	Varies

The point of the table is not bureaucracy. It is that the strongest controls, in Sections 4.4, 4.5 and 4.6, fall on the highest categories: child, case, health and protection data. Lower-risk categories are protected proportionately. KTN does not guard a supplier's phone number the way it guards a child's address, and it does not guard a child's address loosely because that would be convenient.

4.2 Personal Data Collection Standards

Collection is where most data risk is created or avoided, because what is never collected can never be leaked. Five standards govern how KTN gathers information.

Collect the minimum

Before a form is designed or a question is asked, the test is whether the information is genuinely needed for the stated purpose. Forms, including KoboToolbox forms, are reviewed to strip fields that are merely interesting. A field that would be nice to have is not collected.

Be open about it

People are told, in language they understand and in Nga'Karamojong where needed, who is collecting their data, why, what will be done with it, who it may be shared with, how long it will be kept, and how to reach KTN about it. For children and low-literacy participants, this is explained in conversation, not buried in a form.

Collect on a lawful basis

Every collection rests on one of the lawful bases in Section 4.3. For most KTN work that is consent, the vital interests of a child at risk, a legal obligation, or KTN's legitimate interest in delivering and learning from its programmes; the basis is recorded in the processing register.

Collect accurately and securely

Data is recorded accurately at the point of collection, and protected from that moment: devices are locked, paper is not left in the open, and a child's details are never gathered where others can overhear or read them.

Build privacy in from the start

Privacy by design and by default is the rule for any new form, system, programme or research activity. A DPIA under Annex C is completed before collection begins for anything that handles children's data, sensitive data, a new technology, or large volumes of personal data. Privacy is designed in at the planning stage, not bolted on after a donor asks.

4.3 Consent and Lawful Processing

KTN processes personal data only where it has a lawful basis under the Data Protection and Privacy Act. The basis for each processing activity is recorded in the register at Annex B. The table sets out the bases KTN relies on and how each is applied.

Lawful basis	How KTN applies it	Typical use
Consent	Freely given, specific, informed and recorded; may be withdrawn; for children, parental or guardian consent with the child's assent where possible	Research; photography and media; non-essential programme activities
Vital interests	Where processing is needed to protect the life, safety or welfare of a child or another person and consent cannot be obtained in time	An emergency rescue, a child in immediate danger, an urgent medical referral
Legal obligation	Where the law requires processing or disclosure	Mandatory reporting of abuse; statutory financial and tax records; lawful requests from authorities
Legitimate interests	Where processing is necessary for KTN's proper functions and is not overridden by the rights of the person, weighed and recorded	Routine case management; programme administration; security of premises and systems
Public task / contract	Where processing is part of an agreed service to a person or a coordinated child-protection function	Service delivery agreed with a family; coordinated case work with statutory bodies

How consent works at KTN

Consent is sought in plain language, in Nga'Karamojong where needed, and never bundled so that a person must agree to everything to receive any service. A person can decline a non-essential use, such as photography,

and still receive support; child protection services are provided on need alone and are never conditioned on consent to research or media. Consent is recorded, showing who consented, to what, when and how, using the templates at Annex D. Where consent is the basis, it can be withdrawn, and withdrawal is acted on promptly for everything that is not already required by law.

KTN is honest about the limits of consent in its context. A family in crisis is not in a strong position to refuse an organisation offering help, and a child cannot give legally effective consent alone. That is exactly why minimisation, purpose limitation and the best-interests test matter more here than a signature on a form. A consent form is a record of a conversation, not a substitute for one.

4.4 Children's Data Protection

This is the section that matters most, because protecting children's data is not a subset of KTN's mission; it is the same work by another means. Section 3.3 of the Data Protection and Privacy Act prohibits processing a child's personal data unless it is done with the consent of a parent or guardian and in a manner that protects and advances the rights and best interests of the child. KTN treats that as a floor, not a ceiling, and adds the standards below.

1. The best interests of the child come first in every decision about a child's data: whether to collect it, how to store it, whether to share it, and when to destroy it. This is consistent with the Child Safeguarding Policy and Article 3 of the CRC.
2. A child's location, identity and history are treated as among the most sensitive data KTN holds. They are never disclosed in a way that could let a trafficker, an abuser, or anyone the child fled, find the child.
3. Consent for processing a child's data is sought from a parent or guardian, and the child's own views are sought and respected according to age and understanding. Where a child is unaccompanied or the guardian is the source of risk, the best-interests test governs, and the Child Safeguarding Policy decides who may act for the child.
4. Children's data is collected by minimisation as a strict rule: only what the case or the service genuinely requires, never to build a fuller picture for its own sake.
5. Access to children's case files is limited to the staff who need it for their work, logged, and never opened out of curiosity. Discussing a child's case where it can be overheard, or showing a file to someone with no role in it, is a breach.
6. KTN applies the UNICEF Responsible Data for Children principles to children's data: it is purpose-driven, people-centric, participatory, protective of children's rights, proportional, professionally accountable, and designed to prevent harm. These principles also govern the research in Section 6.3.
7. Children's views on how their information is handled are heard through KTN's child participation mechanisms, in Nga'Karamojong, and inform how this policy is applied. The children of Karamoja will live longest with the records made about them now, and they are owed a say in how those records are kept.

Annex E gives field-level guidance for staff and volunteers who collect, carry and store children's data in the conditions KTN actually works in: on outreach, in a vehicle, on a phone with a weak signal, far from the office.

4.5 Sensitive and High-Risk Data

The Act gives special protection to sensitive personal data: religious or philosophical beliefs, political opinions, sexual life, financial information, health status and medical records, and data about children. KTN adds to that

list the categories that carry the most risk in its own context: safeguarding and abuse disclosures, the location of a child or a survivor, and any data that could expose someone to violence, stigma or trafficking.

Sensitive and high-risk data is handled under tighter rules than ordinary data:

- it is collected only where there is a clear, recorded purpose and a lawful basis, and never gathered speculatively;
- it is stored separately or with stronger controls than routine data, and access is limited to the smallest group who need it, on a need-to-know basis that is logged;
- it is encrypted in transit and at rest wherever the system allows, and pseudonymised in datasets used for analysis and research;
- it is never sent over open messaging channels or carried on an unsecured device, and never discussed in public or with anyone outside the case;
- its disclosure, even to a partner or authority, follows Section 4.7 and requires a recorded decision against the best interests of the person, especially where the person is a child or a survivor.

A DPIA under Annex C is required before any new activity that involves sensitive or high-risk data at scale, a new technology, or a new sharing arrangement. The more an error could harm a person, the more carefully the activity is designed before it starts.

4.6 Data Security Requirements

Section 7.1 of the Data Protection and Privacy Act requires KTN to secure the integrity of the personal data in its possession, to identify the risks to that data, and to keep appropriate safeguards against those risks under review. The controls below put that duty into practice at a scale KTN can actually maintain. They read alongside the IT and AI Use Policy, which holds the technical detail, and the Health, Safety and Security Policy, which governs the physical security of premises.

Access on a need-to-know basis

Information is available only to the people whose work requires it. Each member of staff has their own login; passwords are not shared, written on desks or sent over messaging apps. Access to children's case files, health and protection records, and research datasets is restricted to named roles, granted by the DPO or system owner, and reviewed when someone changes role or leaves. Curiosity is not a reason to open a file.

Devices, encryption and screens

KTN laptops and phones used for work are protected by a password or PIN, lock automatically when idle, and are encrypted where the device allows. Anti-malware and security updates are kept current. A device carrying KTN data is never left unattended in a vehicle, a meeting or a public place, and a lost or stolen device is reported immediately as a possible breach under Section 6.5. Personal devices are used for KTN data only where the IT and AI Use Policy permits and the same protections apply.

Field collection and sync

Data collected on KoboToolbox and similar tools is held on the device only as long as needed before it is synced to the secure server, and removed from the device once synced. Forms are designed so that the most sensitive fields are protected, and a phone used for field collection is treated as carrying confidential information from the moment the first answer is entered.

Paper, premises and a clean desk

Paper files with personal data are kept in locked cabinets, not on open shelves or desks, and are signed out when removed. The clean-desk rule applies at both offices: sensitive paper is put away when a desk is unattended, and nothing identifying a child is left on a printer, a whiteboard or a noticeboard.

Cloud, backups and channels

KTN's records are held in approved, access-controlled cloud services and backed up regularly, with backups tested so they actually restore. Sensitive and high-risk data is encrypted in transit and at rest wherever the system allows. Children's personal data is never sent over open WhatsApp, SMS, personal email or social media; where a messaging tool must be used in the field, it is one the IT and AI Use Policy approves, and identifying detail is kept out of it.

Security is proportionate and honest. Some of these controls are already in place; others, such as full device encryption across the fleet and a formal backup-restore test, are scheduled in the roadmap at Section 9.1. The checklist at Annex H is the working tool for keeping all of this real rather than aspirational, and is completed on the schedule it sets.

4.7 Data Sharing and Disclosure

KTN shares personal data only where there is a lawful basis, a genuine need, and a recorded decision that the sharing serves the purpose and, where a child or survivor is involved, their best interests. The default is to share the least that will do the job, and to prefer anonymised or aggregated information over identifiable records, especially for donors and audiences who do not need names.

Who KTN shares with, and why

Routine sharing happens with Probation and Social Welfare Officers and district authorities in coordinated child-protection work; with partner shelters, schools and health facilities involved in a child's care; with the police where a child's safety requires it; with the Office of the Prime Minister and mandated agencies in a declared emergency; and with donors, who receive narrative and aggregated reporting rather than identifiable case data unless a specific, lawful and agreed reason exists. Each routine flow is recorded in the processing register at Annex B.

Systematic sharing needs an agreement

Any regular or bulk sharing of personal data with another organisation is governed by a written data sharing agreement using the template at Annex G, which states what is shared, why, on what basis, for how long, and under what safeguards. A one-off disclosure in a child's interest does not wait for paperwork, but it is still recorded.

The location rule, and lawful demands

The location, identity and history of a child or a survivor are never disclosed in a way that could let a trafficker, an abuser, or anyone the person fled reach them. Where the law compels disclosure, through a court order or a mandatory reporting duty, KTN complies, checks that the demand is lawful and properly authorised, discloses only what is required, and records what was shared and why. Mandatory reporting of abuse under the Child Safeguarding Policy and PSEA Policy always takes precedence over confidentiality.

Sharing across the border

Because the migration corridor runs into Kenya, KTN sometimes shares case information across the border for tracing and reintegration. Such sharing follows the cross-border rules of the Regulations, goes only to a trusted, identified counterpart under agreed safeguards, and is weighed carefully against the child's safety before anything is sent.

4.8 Data Retention and Disposal

KTN keeps personal data only for as long as there is a lawful and operational reason to keep it, then destroys it safely. Holding data longer than needed adds risk without adding value. The full schedule is at Annex J; the table below sets the periods for the main record types. Periods that depend on the best interests of a child, or on legal advice, are set with the relevant authority rather than guessed.

Record type	How long KTN keeps it	Then
Child case and reintegration files	While the case is open and through agreed follow-up; core records retained long-term under the Child Safeguarding Policy and the child's best interests	Secure archive; a care-experienced adult may seek their own record
Safeguarding and abuse records	Long-term, as the Child Safeguarding Policy and PSEA Policy require	Secure archive; destroyed only on documented review
Research data	For the period agreed in the study's data management plan and ethics approval, pseudonymised throughout	Anonymised or securely destroyed
Consent and media records	While the image or use is in circulation, plus an agreed period after last use or withdrawal	Securely destroyed
Beneficiary and programme records	Duration of the programme plus the donor and audit retention period	Reviewed, then securely destroyed
HR and volunteer records	Per the Human Resources Policy and Ugandan employment and tax law	Securely destroyed
Finance, donor and supplier records	Per the Finance and Anti-Fraud Policy and tax law	Securely destroyed
Routine email and operational data	As long as operationally needed; reviewed periodically	Deleted

CHILDREN WITH NO GUARDIAN, OR A GUARDIAN WHO IS THE RISK

The Act requires the consent of a parent or guardian before a child's data is processed. A significant share of the children KTN works with are unaccompanied, cannot have a guardian traced, or have a guardian who is the source of the harm. A best-interests test is how KTN decides; it is not by itself a lawful basis.

In those cases KTN processes on the basis of the child's vital interests and of KTN's legal obligation to protect a child at risk. Before any processing that is not immediately protective, the Designated Safeguarding Lead signs a short written best-interests determination, countersigned by the data protection focal point, and the District Probation and Social Welfare Officer is engaged as the statutory authority for the child. The determination is filed on the case file and the basis relied on is recorded in the processing register.

Record type	How long KTN keeps it	Then
KTN has asked its legal adviser to confirm whether a Probation Officer's authorisation substitutes for guardian consent under the Act. Until that advice is received, KTN applies the stricter reading: it processes only what protection requires, and records why.		

Table 4. Retention periods for the main KTN record types. The full schedule, with disposal methods and owners, is at Annex J.

The periods KTN applies

The full schedule is set out in Annex A of the Records Management and Retention Policy, and the periods below are the same ones stated there. A child case or reintegration file is kept until the child reaches 25, then reviewed rather than destroyed automatically. A safeguarding or abuse record is kept for at least 25 years from the last entry, because survivors often disclose late, and is destroyed only after a documented review. The longitudinal dataset is held pseudonymised for the life of the study plus five years, and the key linking identity to identifier is destroyed at the end of the study. Beneficiary, programme, finance and donor records are kept for seven years from the end of the grant unless a donor requires longer. Consent and media records are kept for the period of use plus three years.

The seven-year figure is being confirmed with KTN's accountant against tax and Companies Act requirements, and any amendment will be made in the Records Management and Retention Policy first. The child file periods are KTN's own policy choice and are stated as such.

Destroying data safely

Paper records are destroyed by cross-cut shredding or through a contracted secure-destruction service, never by open burning or dumping, consistent with the Environmental Policy. Digital records are securely deleted, and devices are wiped before reuse or disposal under Section 6.1. Every destruction of a record set is logged: what was destroyed, when, by whom and how. A legal hold, an open case or an ongoing investigation suspends destruction until it is lifted.

4.9 Records Management

Good data protection is impossible without good records management. KTN cannot protect, find, correct or destroy information it cannot locate, so records are organised on the principle of one reliable place for each thing.

Records are filed in a consistent structure, physical and digital, that the processing register at Annex B maps. Each record set has an owner, a sensitivity level, an access list and a retention period. Working copies are kept to a minimum, because every extra copy is an extra thing to lose; where a copy must be made, it follows the same controls as the original. Case files are the single authoritative record for a child, kept current and complete, so that a decision is never made on a stray note or an out-of-date version.

Records are backed up under Section 4.6 and archived under the retention schedule rather than left to accumulate. Being able to retrieve a record quickly is not only good order; it is what lets KTN honour an access or correction request under Section 6.6 within the time the law allows. When records management slips, data protection slips with it, which is why it is audited under Section 8.2.

5

CHAPTER FIVE

ROLES, RESPONSIBILITIES AND ACCOUNTABILITIES

Who is responsible and accountable for protecting personal data.

5 Roles, Responsibilities and Accountabilities

Who is responsible and accountable for protecting personal data.

5.1 Roles and Responsibilities

Data protection is everyone's job, but specific duties sit with specific people. The matrix states who does what, so that nothing in this policy depends on goodwill alone.

Who	Responsibility under this policy
Board of Directors	Adopts the policy and its revisions; resources the DPO role and budget line; receives the annual data protection report and audit findings; reviews serious breaches; holds the Executive Director accountable.
Finance and Audit Sub-Committee	Reviews the data protection risk register quarterly; receives audit findings and tracks corrective actions; ensures data protection costs are budgeted.
Programmes Sub-Committee	Satisfies itself that DPIAs and privacy-by-design are applied to programme and research design; reviews data protection outcomes within programme reporting.
Executive Director	Owns the policy day to day; appoints and supports the DPO; receives quarterly reports and breach escalations; signs off the annual report; approves minor administrative updates under Section 9.2.
Data Protection and Privacy Officer	Coordinates implementation across all sites; maintains the processing register, risk register and breach log; leads DPIAs, consent oversight, training and the annual internal audit; keeps the PDPO registration current; drafts the annual report. Held alongside existing duties.
Programme Manager	Ensures every new project, system and research activity completes a DPIA before it begins; builds data protection costs into project budgets; ensures field activities follow Sections 4.2 to 4.9.
MEAL Officer	Designs KoboToolbox forms and the MEAL framework to collect the minimum data needed; applies pseudonymisation and access controls to datasets; supports data quality and secure analysis.
Finance and Administration Officer	Safeguards HR, payroll, donor and supplier data; manages physical file security, access logs and the secure destruction of records; manages processor and supplier data clauses with the DPO.
Case managers and field teams	Collect only what a case needs; record consent; keep devices and files secure in the field; never discuss or display a child's information where it can be overheard or seen; report breaches within 24 hours.
All staff and volunteers	Complete data protection induction and refreshers; sign the confidentiality declaration at Annex I; follow the security rules of Section 4.6; report breaches and raise concerns without fear of detriment.
Partners, processors and suppliers	Meet the expectations in Sections 4.7 and 7.1 and in their agreements and data sharing agreements; report breaches arising from work done for KTN; cooperate with corrective action.

6

CHAPTER SIX

PROCEDURES AND OPERATIONAL REQUIREMENTS

How the standards are delivered in systems, research, communications, breach response and the exercise of data subject rights.

6 Procedures and Operational Requirements

How the standards are delivered in systems, research, communications, breach response and the exercise of data subject rights.

How to reach these routes

KTN does not yet operate a dedicated telephone line. Until it does, concerns are raised by email to the role addresses below, in person at either office, or through a case worker, community volunteer or Clan Committee member. Addresses are held by role and not by named person, so a change of staff never closes a reporting route. A dedicated toll-free line is a funded priority and this section will be amended to carry the number once it is live.

Safeguarding: safeguarding@karamojatumaini.org. Whistleblowing and concerns about a senior person: report@karamojatumaini.org. Data protection: dataprotection@karamojatumaini.org. Human resources and grievances: hr@karamojatumaini.org. General: info@karamojatumaini.org. The national child helpline, 116, is free from any Ugandan network and independent of KTN.

TELLING THE REGULATOR AND THE PEOPLE AFFECTED

The data protection focal point notifies the Personal Data Protection Office immediately on KTN becoming aware of a breach where there is reasonable belief that personal data has been accessed or acquired by an unauthorised person. The time KTN became aware, the time of notification and the reason for any gap between the two are recorded.

People affected are told without undue delay and in any case within seven days, in Nga'Karamojong, by a route they can actually receive: in person, through their case worker, or through the Clan Committee. The exception is where telling them would itself put a child at risk, in which case the Designated Safeguarding Lead decides and the reason is recorded.

The Ugandan duty is immediate notification. It is not the seventy-two hour period that applies in some other jurisdictions, and KTN does not work to that period, because doing so would give it a deadline the Act does not allow. KTN has asked its legal adviser to confirm the exact wording of section 23 of the Act and of the Data Protection and Privacy Regulations, 2021, and this clause will be amended if the advice requires it.

6.1 Digital Systems and Technology Management

Most of KTN's data now lives in or moves through digital systems: KoboToolbox for field collection, cloud storage and email for everyday work, a case management record for children in the caseload, and the phones that carry all of it into the field. This section governs how those systems are chosen, run and retired. The IT and AI Use Policy sets the technical standards; this policy sets the data protection ones.

Choosing systems and processors

Before KTN adopts a new system or appoints a provider that will hold personal data, the DPO checks that the provider offers adequate security, will process data only on KTN's instructions, will report breaches to KTN, and will return or delete KTN's data when the arrangement ends. These terms go into the contract, as Section 7.1 requires. A free tool with no data protection terms is not a saving; it is an unmanaged risk.

Where data is hosted

KTN records where its data is stored, including whether it is held outside Uganda. Personal data of Ugandan citizens is transferred to or stored in another country only where that country offers protection at least equivalent to the Act, or with the consent of the data subject, in line with the Regulations on cross-border processing. Where a cloud service stores data abroad, that fact is recorded in the processing register and weighed in the DPIA.

No unmanaged tools, and orderly change

Staff do not move KTN personal data onto unapproved apps, personal cloud accounts or unmanaged spreadsheets, however convenient. New systems, and significant changes to existing ones, go through a DPIA under Annex C before they handle real data. System access is reviewed at least annually, and removed promptly when a person leaves.

Retiring devices and systems

When a device or system reaches the end of its life, the data on it is securely wiped before the hardware is reused, donated or disposed of, and the disposal is logged. Equipment then follows the e-waste route in the Environmental Policy and the IT and AI Use Policy. A device is never sold, given away or thrown out with KTN data still readable on it.

6.2 Artificial Intelligence and Data Ethics

Artificial intelligence tools can help KTN translate, transcribe, summarise and analyse, and they bring a real risk: anything typed into a public AI tool may leave KTN's control and be used to train someone else's model. The rules below govern AI use and read with the IT and AI Use Policy. They start from a simple position: a child's information is not raw material for an experiment.

1. Personal data about children, families, survivors, research participants or staff is never entered into a public or consumer AI tool. Where AI is genuinely useful, KTN uses only a tool approved under the IT and AI Use Policy, under terms that keep KTN's data out of training and within KTN's control.
2. Where AI assists with translation, transcription or analysis, the data is de-identified first wherever possible, and a person checks the output. AI drafts; people decide.
3. No decision that materially affects a child or a person, such as a referral, a reintegration step or an eligibility judgement, is made by an automated system alone. A named member of staff is always accountable for the decision.
4. KTN is alert to bias. Tools trained far from Karamoja may misread its languages, names and circumstances, and KTN treats their output as a suggestion to be tested against what staff and communities know, not as fact.
5. Any new use of AI on personal data is assessed through a DPIA under Annex C before it begins, and recorded in the processing register.

> *A tool that is convenient for us is not worth a child's safety. When the two collide, the child wins.*
>
> Section 6.2, Artificial Intelligence and Data Ethics

6.3 Research and Learning Data Protection

The Data pillar of the SHIELD framework rests on research, above all the longitudinal study of why children leave Karamoja and what brings them home. That work asks hundreds of children and families to share difficult things on the understanding that the information will be handled with care. Honouring that understanding is a condition of doing the research at all, not an add-on to it.

Ethics, consent and the freedom to refuse

Research involving people goes through ethics review and any clearance required in Uganda before it begins, including registration with the relevant authority where the study calls for it. Participation is voluntary and informed: people are told what the study is for, what will happen to their answers, and that they may decline or stop at any time. For children, a parent or guardian consents and the child's own assent is sought according to age and understanding. Taking part, or declining, never affects a child's access to protection services, which are provided on need alone.

Minimise, pseudonymise, secure

Research collects the least data needed to answer the question. Identifiers are separated from responses and replaced with codes held securely apart, so that analysis works on pseudonymised data. Datasets are stored with the controls in Section 4.6, and access is limited to the named research team. Each study has a written data management plan covering collection, storage, sharing, retention and destruction.

Sharing and publishing

Where KTN works with academic partners such as Makerere University, Gulu University and the AfriChild Centre, data is shared only under a data sharing agreement and the relevant ethics approval, and only to the extent the work requires. Anything published, including the State of Pastoralist Child Protection Report, uses aggregated or anonymised data: no individual child, family or community is identifiable in a report, a dataset or a conference slide. The UNICEF Responsible Data for Children principles govern the whole of this work.

6.4 Photography, Media and Communications Data Protection

A photograph of a child is personal data, and often sensitive data, because it can identify the child and sometimes reveal where they are. KTN's communications work, including its Nga'Karamojong radio programming, depends on telling real stories, and it does so without trading a child's safety or dignity for a stronger image.

1. Photographs, audio and video of identifiable people are taken only with informed consent, recorded using the templates at Annex D. For a child, a parent or guardian consents and the child's own assent is sought; a child old enough to object is never overridden.
2. Consent is purpose-specific. Agreement to a programme record is not agreement to a public fundraising appeal, and consent for one use does not unlock every use. A person may refuse images entirely and still receive every service.
3. No image is used that reveals or implies the location of a child or survivor, that could let someone the child fled find them, or that shows a child in a way that strips their dignity. KTN does not pair a child's full name with their image in public material.
4. Image libraries are stored securely with their consent records, access is limited, and a person may withdraw consent for future use; KTN stops using the image going forward and records the withdrawal.

5. Survivors of abuse or exploitation are given particular care, consistent with the Child Safeguarding Policy and PSEA Policy: their images are not used in ways that could expose or re-traumatise them, even with consent, where the risk outweighs the benefit.

The brand voice carries here too: communications are plain, specific and respectful, and never depict the children of Karamoja as helpless or anonymous. A story told with consent and dignity is stronger than one taken without either.

6.5 Data Breach Management

A personal data breach is any security failure that leads to the loss, theft, unauthorised access, alteration, disclosure or destruction of personal data, whether by accident or design: a lost phone, a misdirected email, a stolen file, a hacked account, a document left where it should not be. KTN treats breaches as a question of when, not if, and judges itself on how fast and how honestly it responds. The reporting form is at Annex F.

1. Whoever discovers a breach, or suspects one, makes the situation safe if they can, by recovering a device, recalling an email or stopping further exposure, and reports it to the DPO within 24 hours. A phone call first and the form after is better than a delayed form. No one is blamed for reporting in good faith, including a breach they caused; the Whistleblowing Policy's protections apply.
2. The DPO logs the breach, assesses its severity with the relevant manager, and leads containment and recovery.
3. Where a child or survivor could be endangered, the safeguarding response under the Child Safeguarding Policy begins at once and in parallel: protecting the person comes before completing the form.
4. The DPO notifies the Executive Director the same day for any serious breach, and the Board at its next sitting or sooner. Where the Act requires, the breach is reported to the Personal Data Protection Office without undue delay, and the affected people are informed where the law or the PDPO directs and where doing so helps them protect themselves.
5. Every breach closes with a short learning note: what happened, why, and what changed so it does not happen again. Lessons feed the risk register, the training in Section 8.1, and the annual report.

Severity	What it looks like	Response
Critical	A child or survivor put at risk; large-scale or sensitive data exposed	Immediate containment and safeguarding response; ED and Board informed same day; PDPO notified; affected people informed
High	Sensitive data exposed, or data of several people, with real risk of harm	Same-day escalation to ED; PDPO notification assessed and usually made; corrective action tracked to closure
Medium	Limited personal data exposed with some risk	Contained and logged; reviewed by the DPO; PDPO notification assessed
Low	A near miss or minor exposure quickly contained, little or no risk	Logged and learned from; controls tightened where the near miss revealed a weakness

Table 5. Data breach severity and response. The DPO assigns severity; the affected person's safety, not KTN's convenience, decides it.

6.6 Complaints and Data Subject Rights

The Data Protection and Privacy Act gives people rights over their own data, and KTN honours them in practice, not only on paper. A person can exercise any of these rights free of charge by contacting the DPO, in

Nga'Karamojong where needed, and KTN helps people who cannot read or write to make their request. KTN confirms the person's identity before acting, so that one person cannot obtain another's data.

The right	How KTN honours it
To be informed	People are told what KTN holds, why, who it is shared with and how long it is kept, in plain language at the point of collection (Section 4.2).
To access their data	A person may ask for a copy of the personal data KTN holds about them; KTN provides it within the time the law allows, withholding only what would endanger another person, especially a child.
To correct or update	Inaccurate or out-of-date data is corrected promptly when a person points it out or KTN finds it.
To prevent processing	A person may object to processing or ask KTN to stop, and KTN does so unless the law requires it to continue, for example for a safeguarding or statutory duty.
To withdraw consent	Where consent is the basis, it can be withdrawn for anything not already required by law, including photography and research.
To complain	A person may complain to KTN through the Complaints and Community Feedback Policy, and to the PDPO, which investigates complaints within the period the law sets.

Children's rights are exercised through a parent or guardian and, where the guardian is the source of risk, through the best-interests route in the Child Safeguarding Policy. A child old enough to have a view is heard. Where KTN must refuse part of a request, for example to protect another child, it explains the refusal and tells the person how to take the matter further.

7

CHAPTER SEVEN

RISK MANAGEMENT AND INTERNAL CONTROLS

The controls over partners and third parties who handle KTN data.

7 Risk Management and Internal Controls

The controls over partners and third parties who handle KTN data.

7.1 Partner and Third-Party Data Requirements

When KTN lets another organisation hold or handle its data, KTN's responsibility does not transfer with the data. KTN remains accountable, so it chooses partners and processors with care and binds them in writing. This section reads with the Procurement Policy, which sets the procedure for selecting and contracting suppliers.

Before a partner, processor, contractor or supplier handles personal data for KTN, the DPO checks that they can protect it, and their agreement requires them to:

- process the data only for the agreed purpose and only on KTN's instructions, never for their own ends;
- apply security at least as strong as this policy requires, proportionate to the sensitivity of the data;
- keep the data confidential, and bind their own staff to do the same;
- not engage a sub-processor or pass the data on without KTN's written agreement;
- report any breach to KTN without delay, and cooperate with KTN's response;
- return or securely destroy the data when the work ends, and confirm in writing that they have done so;
- allow KTN to check compliance, and accept correction up to and including termination of the agreement.

A partner or supplier who breaches these terms is corrected once and removed from KTN's arrangements if the breach repeats or is serious. The standard applies to everyone who touches KTN data, from a national NGO partner to the local provider servicing a laptop.

8

CHAPTER EIGHT

COMPLIANCE, MONITORING AND REPORTING

How the policy is trained, monitored, audited and reported.

8 Compliance, Monitoring and Reporting

How the policy is trained, monitored, audited and reported.

8.1 Staff Training and Capacity Development

A policy nobody understands protects nothing. KTN builds data protection capability the same way it builds safeguarding capability: induction first, refreshers thereafter, and deeper training for the people who carry specific duties.

Every new staff member, volunteer, intern and peer educator completes a data protection induction within their first month and signs the confidentiality declaration at Annex I before handling personal data. The induction covers what this policy commits KTN to, the daily practices expected at every site, how to recognise sensitive and children's data, and how to report a breach. An annual refresher, no longer than ninety minutes, keeps the commitments current and shares what the year's breaches and audit have taught.

The DPO receives deeper training in DPIAs, the processing register, breach handling and the Act, drawing on PDPO guidance and reputable courses. Case workers and field teams are trained on collecting, carrying and storing children's data in field conditions, using Annex E. The MEAL Officer is trained on secure dataset design and pseudonymisation. Finance and administration staff are trained on HR, donor and supplier data. Data protection responsibility appears in role descriptions and is a fair subject in performance conversations, in the same plain way as safeguarding: did you collect only what was needed, did you keep it secure, did you report what you saw.

8.2 Monitoring, Compliance and Audit

KTN measures its data protection performance against a small set of honest indicators, chosen to be collectable rather than impressive. The full set sits with the DPO; the core indicators are:

- the processing register complete and reviewed, with a lawful basis recorded for every activity;
- PDPO registration current, and the annual compliance report filed on time;
- the share of new projects, systems and research activities with a completed DPIA before they began (target: all of them);
- staff, volunteers and peer educators inducted and holding a signed confidentiality declaration (target: all of them);
- breaches reported within 24 hours, and the share closed with a learning note within 30 days;
- data sharing agreements in place for every systematic sharing arrangement;
- access reviews and the information security checklist at Annex H completed on schedule.

Reporting, audit and the regulator

The DPO reports quarterly to the Executive Director against these indicators, and prepares an annual data protection report that the Executive Director presents to the Board and KTN publishes, in line with its transparency value. Once a year the DPO leads an internal audit using the checklist at Annex K, joined by a colleague independent of day-to-day data duties so the audit is a check, not a self-assessment. An independent

external review is commissioned at least once within the life of the Strategic Plan, and earlier if a serious breach warrants it.

KTN keeps its registration with the Personal Data Protection Office current and files the annual data protection and privacy compliance report the PDPO requires within ninety days of the end of each financial year, summarising complaints received and their status and disclosing the year's breaches. Donor due diligence and data protection assessments are supported openly, with the registers, logs and records this policy requires made available without rehearsal.

8.3 Records, Audit Trail and Retention

A data protection policy that cannot itself be audited is only a statement of intention. Every duty this policy creates leaves a record, made at the time it happens, protected from quiet alteration, and destroyed on a schedule rather than at anyone's discretion. This section sets the audit trail that runs beneath the whole policy, and reads with the retention rule at Section 4.8 and the schedule at Annex J.

8.3.1 The audit trail

Recorded when it happens. A consent, a data sharing agreement, a DPIA decision, a subject access request and a breach are entered in their register at the moment they occur, not reconstructed later. The processing register at Annex B is the index to all of them.

Every decision, with its reason. Each decision this policy calls for is recorded with its date, the person who took it and the reason for it. That includes the decisions an auditor asks about first: a decision that a DPIA was not needed, a decision to share data with a third party, and a decision that a breach did not require notification.

Systems keep their own log. Every system holding personal data records who opened, added to, changed or exported each record, and when. Access logs for systems holding child, case, health or protection data are retained for twelve months, with the last three months immediately retrievable, and are reviewed by the Data Protection and Privacy Officer each quarter for access that has no business reason behind it.

No silent edits. Records are not altered after the fact. A correction is made as a dated addition that leaves the original entry legible, so that what was known, and when it was known, can be reconstructed. This applies equally to a paper case file and to a database row.

One authoritative place. Each record set has a single authoritative location, an owner, a sensitivity level, an access list and a retention period, as Section 4.9 requires. A record that exists in three places has three chances to leak and no reliable version.

8.3.2 Retention periods

The retention schedule at Annex J governs how long each record type is kept, and Section 4.8 governs how it is disposed of. The periods there are minimums. Where a donor agreement, an open case, a police or court process, a data subject complaint or a direction of the Board requires a record to be kept longer, the longer period applies, and nothing is destroyed while a matter it relates to is live. A legal hold is recorded in the processing register and lifted in writing.

8.3.3 Protection, review and disposal

Protected while held. Paper records are held under lock with access by named role; electronic records are held in systems that meet Section 4.6, with access reviewed at least twice a year. Child and case records are never filed with personnel or supplier records, and are never sent by open email.

Reviewed once a year. The Data Protection and Privacy Officer reviews the registers annually against Annex J, lists what has fallen due for disposal, and obtains the Executive Director's written approval before anything is destroyed.

Disposed of so it cannot be recovered. Paper is shredded; electronic records are deleted from live systems and from backups on their next cycle; devices are wiped before reuse or disposal. Each disposal is logged with the date, what was destroyed, the authority for it and who carried it out, and that disposal log is itself kept permanently.

9

CHAPTER NINE

ENFORCEMENT, IMPROVEMENT AND REVIEW

How the policy is implemented, reviewed and improved.

9 Enforcement, Improvement and Review

How the policy is implemented, reviewed and improved.

9.1 Implementation Roadmap

Implementation begins in the first quarter of the 2026/27 year and builds in the same disciplined sequence KTN uses elsewhere: foundations first, habits second, improvements as capacity allows. The detailed one-year plan, with responsibilities per action, sits with the DPO; the table is the summary.

Period	Focus
Year One, Q1 (Apr–Jun 2026)	Designate the Data Protection and Privacy Officer; confirm or complete PDPO registration; build the processing register from Annex B; have all staff and volunteers sign the confidentiality declaration; deliver first inductions; secure the highest-risk files and devices first.
Year One, Q2 (Jul–Sep 2026)	DPIA process (Annex C) live for new activities; consent templates (Annex D) in use; data sharing agreements (Annex G) concluded with the main partners; first information security checklist (Annex H) completed; first quarterly report to the Executive Director.
Year One, Q3 (Oct–Dec 2026)	Research data management plans in place for the longitudinal study; a breach-response walkthrough run with staff; access reviews completed; retention schedule (Annex J) applied to existing files.
Year One, Q4 (Jan–Mar 2027)	First annual data protection report to the Board, then published; first internal audit (Annex K); first annual compliance report filed with the PDPO within 90 days of year end; lessons consolidated and the Year Two plan agreed.
Years Two to Three	Strengthen the case management system and its access controls; full device encryption across the fleet; tested backups; refine the register and DPIAs as KTN grows.
Years Four to Five	Independent external review of data protection; data protection built into the State of Pastoralist Child Protection Report's data governance; policy revised for the next strategic period.

Table 7. Implementation roadmap. Year One actions are deliberately modest and achievable; capital improvements follow as funding allows.

9.2 Policy Review and Continuous Improvement

This policy is reviewed every three years, with the next scheduled review by June 2029. A review takes place earlier where required by any of the following: a change in Uganda's data protection law or regulation, or PDPO guidance; a donor requirement; organisational restructuring; a revision of the Strategic Plan; a safeguarding development that touches information handling; a technology development that changes how KTN operates, including new AI tools; an emerging organisational risk; a serious data breach; a finding from audit or evaluation that the policy is not working as written; or the direction of the Board.

Minor administrative updates, such as corrected references, retitled roles or annex formatting, may be approved by the Executive Director. Any substantive change to commitments, standards or responsibilities is approved by the Board. Every change is recorded in the Version Control Register and the Amendment History Register at the front of this document, with the version number incremented accordingly. Each review checks

the policy against the current processing register, the breach log and the indicator data, so that revision is driven by evidence rather than by the calendar alone.

KTN holds some of the most sensitive information about some of the most vulnerable children in Uganda. Protecting it well is not a compliance chore set apart from the mission; it is the mission, carried out in the registers, the locked cabinets, the encrypted phones and the careful conversations where the real work of trust is done. This policy will be kept the way KTN keeps all its promises: in the open, against the evidence, for the long term.

Shielding pastoralist children · Building futures · Leading change

Karamoja Tumaini Network · www.karamojatumaini.org

10

CHAPTER TEN

ANNEXES

The working tools: registers, forms and reference material.

10 Annexes

The working tools: registers, forms and reference material.

The eleven annexes that follow are the working tools of this policy. They are templates, not records: blank copies are held by the Data Protection and Privacy Officer, completed copies are filed in the appropriate records folder, and the formats may be adjusted for practicality by the Executive Director provided the substance is kept. Where an annex refers to another KTN policy, that policy governs the detail.

Annex A: Data Protection Code of Conduct

The everyday rules every person who works for or with KTN follows. They fit on one page on purpose, so that there is no excuse for not knowing them.

1. Collect only what the work needs. If a field is not needed, do not ask for it.
2. Tell people, in language they understand, what you are collecting and why.
3. Treat a child's information as you would treat the child: protect it, and never expose it.
4. Open a file only when your work requires it. Curiosity is not a reason.
5. Keep devices locked and paper put away. Never leave personal data where it can be seen, overheard or taken.
6. Never put a child's personal data into a public AI tool, open WhatsApp, SMS or social media.
7. Share only with a lawful reason, only what is needed, and never the location of a child or survivor in a way that could endanger them.
8. Get consent before photographing or recording a person, and respect a refusal.
9. Report any breach, or suspected breach, to the DPO within 24 hours. You will not be blamed for reporting.
10. When in doubt, ask the DPO before you act, not after.

Annex B: Data Processing Register Template

The processing register is the backbone of this policy: an organisation that cannot list what it holds cannot protect it. The DPO keeps it current and the internal audit checks it. Each entry records the fields below. The rows that follow are worked examples; copy and replace them for each processing activity.

Activity	Data and subjects	Purpose and lawful basis	Access and sharing	Retention
Child case management	Identity, history, location, family, case notes; children and guardians	Protect and reintegrate the child; vital interests and legitimate interests	Case workers and DPO; shared with PSWO under DSA	Long-term per Section 4.8
KoboToolbox surveys	Survey responses; community members and households	Programme monitoring and learning; consent and legitimate interests	MEAL team; pseudonymised for analysis	Per data management plan
Photography and media	Photographs and video; children, families, staff	Documentation and communications; consent	Communications staff; published only with consent	Per Section 4.8

Activity	Data and subjects	Purpose and lawful basis	Access and sharing	Retention
Payroll and HR	Contracts, pay, performance; staff and volunteers	Employment administration; legal obligation and contract	Finance and Admin Officer; ED	Per HR Policy and tax law

Table 9. Data processing register format, with worked examples. A full entry also records the security measures applied and whether data is stored or transferred outside Uganda.

Annex C: Data Protection Impact Assessment (DPIA) Tool

Completed before any new activity, system, research study or sharing arrangement that involves children's data, sensitive data, a new technology, large volumes of personal data, or AI. It is completed by the officer designing the activity and reviewed by the DPO. Record the activity name, owner, date, and a short description, then answer the questions below.

No.	Screening question	Yes / No / N/A
1	Does the activity involve children's personal data?	
2	Does it involve sensitive data (health, protection, abuse, financial, beliefs)?	
3	Does it involve the location, identity or history of a child or survivor?	
4	Does it use a new system, tool, device or AI capability?	
5	Will it collect personal data from a large number of people?	
6	Will personal data be shared with another organisation or authority?	
7	Will any personal data be stored or processed outside Uganda?	
8	Could the activity expose a person to harm if the data leaked?	
9	Are people unable to refuse easily (for example, a family in crisis)?	
10	Is consent difficult to obtain or rely on for this activity?	

For every Yes, rate the likelihood of harm and the severity of its impact using the matrix below, and record the rating and the mitigation in an action plan.

Likelihood \ Impact	Minor	Moderate	Major
Unlikely	Low	Low	Medium
Possible	Low	Medium	High
Likely	Medium	High	High

Decision rule

If every answer is No or every rating is Low, the activity proceeds and the form is filed. If any rating is Medium, the activity proceeds only once mitigation is recorded with a named owner. If any rating is High, or if questions 1, 2 or 3 are answered Yes, the DPIA goes to the DPO and the Executive Director before any approval, and the DPO decides what further safeguards, or what changes to the activity, are required before it can begin.

Annex D: Consent Forms Template

Three short consent records for the situations KTN meets most often. Each is explained in conversation, in Nga'Karamojong where needed, and never relied on as a substitute for that conversation. Each records who consented, to what, when and how, and that the person was told they may decline or withdraw.

1. Programme and case consent

Records the person's agreement to KTN collecting and using their information to provide and coordinate support, having been told what is collected, why, who it may be shared with, and how long it is kept. Captures: name and role of the person consenting (the child's guardian, with the child's assent noted); the support concerned; date; and signature or thumbprint, with a witness where the person cannot read.

2. Research consent and child assent

Records voluntary, informed agreement to take part in a study, having been told the purpose, what participation involves, that answers are pseudonymised, that the person may stop at any time, and that taking part or declining does not affect any service. Captures guardian consent and, separately, the child's own assent in words the child understands.

3. Photography and media consent

Records purpose-specific agreement to be photographed, filmed or recorded, stating clearly whether the use is an internal record only or includes public communications, that the person may refuse and still receive services, and that consent may be withdrawn for future use. Captures the specific uses agreed, the date, and signature or thumbprint.

Annex E: Child Data Protection Guidance

Field-level guidance for everyone who collects, carries and stores children's data in the conditions KTN actually works in. It expands Section 4.4 into plain practice.

- Collect a child's details somewhere private. Do not gather identity, family or abuse information where others can overhear or read it.
- Carry the least you need into the field. A full case file rarely needs to travel; take only what the visit requires.
- Keep the phone locked, and sync as soon as you have signal, then remove the data from the device.
- Never put a child's name, photograph or location into WhatsApp, SMS, personal email or any public app.
- Do not discuss a child's case in a vehicle, a queue or a public place, even using a first name.
- Treat a child's location as the most dangerous fact you hold. Share it only with a lawful reason and only with someone entitled to it.
- If you lose a device, a file or your bearings about who has seen something, tell the DPO the same day. Reporting protects the child; silence does not.
- When a child asks what you are writing about them, answer honestly and at their level. It is their information too.

Annex F: Data Breach Reporting Form

Any lost or stolen device or file, misdirected message, unauthorised access, or exposure of personal data is a breach or a suspected breach. Report it to the DPO within twenty-four hours using the fields below. Where a child or survivor could be at risk, the safeguarding response begins at once and does not wait for this form.

Field	What to record
Date, time and location	When and where the breach happened or was discovered, as precisely as known
Reported by	Name and role; reports may also be made anonymously through the whistleblowing channel
What happened	A plain factual account, without speculation about blame
Data and people affected	What data was involved and whose; flag immediately if any child or survivor is affected
Immediate action taken	Containment: device recovered, email recalled, access closed, activity stopped
Risk of harm	What harm could follow, to whom, and how urgent; safeguarding risk is rated first
Notification required	Whether the PDPO, the affected people, the police or a safeguarding lead must be told, and when this was done
Root cause	Completed after review by the DPO: what allowed this to happen
Corrective action and owner	What will prevent recurrence, who owns it, and by when
Date closed and learning note	Closure requires a short learning note circulated to relevant staff

Annex G: Data Sharing Agreement Template

The heads of terms for any agreement under which KTN shares personal data with, or receives it from, another organisation on a regular or bulk basis. A complete agreement covers each of the clauses below; the DPO holds the full template.

1. Parties and contacts, including each side's data protection contact.
2. Purpose of the sharing, stated specifically and narrowly.
3. The data shared, the people it concerns, and the direction of sharing.
4. The lawful basis each party relies on, and confirmation that consent, where used, was properly obtained.
5. Security measures each party will apply, proportionate to the sensitivity of the data.
6. Confidentiality, and limits on further use or onward sharing without written agreement.
7. Breach notification: who tells whom, how fast, and how the parties cooperate.
8. Retention, return and secure destruction of the data when the arrangement ends.
9. The right to check compliance, and the consequences of breach, up to termination.
10. Term, termination, and the governing law of Uganda.

Annex H: Information Security Checklist

Completed by the DPO with the Finance and Administration Officer on a regular cycle, at least quarterly, and after any change to systems. A No answer is recorded with the action that will fix it and a date.

Check	Standard expected	Status and notes
Access on need-to-know	Unique logins; access to sensitive data limited and reviewed	
Passwords	Strong, not shared, not written down or sent in messages	

Check	Standard expected	Status and notes
Device protection	Screen locks, updates current, encryption where the device allows	
Field devices	Data synced and removed from devices promptly; lost devices reported	
Backups	Regular backups taken and a restore tested at least once	
Paper security	Sensitive files locked away; clean-desk rule observed	
Messaging	No children's or sensitive data on open WhatsApp, SMS or social media	
Sharing	Data sharing agreements in place for systematic sharing	
Disposal	Secure deletion and device wiping logged; no readable data on disposed kit	
Cross-border storage	Locations recorded; cross-border rules met for Ugandan citizens' data	

Annex I: Staff Confidentiality Declaration

Signed by every member of staff, volunteer, intern, peer educator, consultant and contractor before they handle personal data for KTN, and kept on file. The text below is the standard wording.

I understand that in my work with Karamoja Tumaini Network I will handle personal and confidential information, including information about children, families, survivors, research participants, colleagues and partners. I have read and understood the Data Protection and Privacy Policy and the Code of Conduct at Annex A. I agree to collect only the information needed for my work; to keep it secure and confidential; to use it only for its proper purpose; never to disclose it to anyone not entitled to it; never to expose the location or identity of a child or survivor; and to report any breach to the Data Protection and Privacy Officer within 24 hours. I understand that this duty continues after my engagement with KTN ends, that a breach may lead to disciplinary action up to dismissal or termination, and that misuse of personal data may be an offence under the Data Protection and Privacy Act, 2019 (Cap. 97).

Name and role	Signature and date

Annex J: Data Retention Schedule

The full schedule behind Section 4.8. Periods marked as set with advice are confirmed with the relevant authority, such as a Probation and Social Welfare Officer or legal counsel, because a child's best interests and Ugandan law, not convenience, decide them.

Record type	Retention period	Disposal method	Owner
Child case and reintegration files	Open case plus follow-up; core records long-term (set with advice)	Secure archive; shred or secure destruction	DPO with case lead
Safeguarding and abuse records	Long-term per Child Safeguarding and PSEA Policies	Reviewed destruction only	Safeguarding lead
Research data	Per data management plan and ethics approval	Anonymise or secure delete	MEAL Officer
Consent and media records	While in use plus agreed period after last use	Secure delete; shred	Communications
Beneficiary and programme records	Programme duration plus donor and audit period	Secure delete; shred	Programme Manager
HR and volunteer records	Per HR Policy and employment and tax law	Shred; secure delete	Finance and Admin
Finance, donor and supplier records	Per Finance Policy and tax law	Shred; secure delete	Finance and Admin
Routine email and operational data	As needed; reviewed periodically	Delete	All staff

Table 12. Data retention schedule. Destruction is logged, and a legal hold or open case suspends destruction until lifted.

Annex K: Annual Data Protection Compliance Checklist

The scope of the annual internal audit under Section 8.2, conducted by a staff member independent of day-to-day data duties, and the basis for the annual compliance report filed with the PDPO within ninety days of the financial year end. For each area the auditor records what was checked, the evidence seen, and any finding.

Audit area	What the auditor checks
Registration	PDPO registration current; renewal tracked; annual compliance report filed on time
Processing register	Annex B complete and current; a lawful basis recorded for every activity
DPIAs	Every qualifying new activity has a completed DPIA on file; the decision rule was followed
Consent and rights	Consent records kept; access, correction and withdrawal requests handled within time
Children's data	Heightened controls in Sections 4.4 and 4.5 applied; access limited and logged
Security	Annex H checklist completed on schedule; access reviews done; backups tested
Breaches	All known breaches logged; 24-hour reporting met; corrective actions closed with learning notes

Audit area	What the auditor checks
Sharing and partners	Data sharing agreements in place; processor and supplier clauses applied; cross-border rules met
Retention	Annex J applied; destruction logged; no data kept beyond its period without reason
Training	Induction and refresher coverage against the staff list; confidentiality declarations signed
Prior findings	Corrective actions from the previous audit closed, or escalation recorded

KARAMOJA TUMAINI NETWORK

SHIELDING PASTORALIST CHILDREN · BUILDING FUTURES · LEADING CHANGE

Behind every number is a child with a name.

KTN's records follow a child for two years after they go home. That is a debt of confidence, not a dataset. This policy is how KTN keeps it: nothing collected without reason, nothing held past its purpose.

Karamoja Tumaini Network

Hope · Heal · Empower

info@karamojatumaini.org · www.karamojatumaini.org

DATA PROTECTION AND PRIVACY POLICY · VERSION 1.0 · EFFECTIVE JUNE 2026