KARAMOJA TUMAINI NETWORK · KTN

IT and AI Use Policy

Technology in service of children, used safely and honestly

Policy Category Governance Policy · Classification: Public
Adopted by the Board of Directors April 2026
Status Version 1.0 · Effective April 2026 · Next review April 2029

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

OUR COMMITMENT

Karamoja Tumaini Network commits to using technology in service of its mission, safely, lawfully and honestly. We will protect the devices, systems and data the work depends on, guard the personal information of every child and adult in our records, and keep our digital spaces safe for the children who reach us through them.

We will use artificial intelligence deliberately: as a tool that serves human judgement, never replaces it, with a person answerable for every output, and honesty about what a machine helped produce. We will measure our performance, report it to our Board, and improve year on year.

WHY IT MATTERS

KTN's Data pillar is its distinctive strength: a child-tracking system that follows each child for two years is also a database of the most sensitive information an organisation can hold. Technology powers the mission and carries its sharpest risks at once: a phished password, a lost laptop, an untrained AI prompt can expose a child faster than any physical failure. Using these tools well is not an IT matter. It is child protection.

WHERE IT APPLIES

Every device, account, system, network and dataset used for KTN work, whether KTN's or personal; every person who uses them: board members, staff, volunteers, consultants and partners; at every office and field location, online and offline, regardless of the source of funding.

HOPE · HEAL · EMPOWER

A child's information can find a child. We hold it as carefully as we hold the child.

IT AND AI USE POLICY · KARAMOJA TUMAINI NETWORK

Contents

Version 1.0 · Effective April 2026 · Next review April 2027

List of Tables iv
List of Figures iv
Policy Approval iv
A Statement of Commitment from the Board vi
Document Control vii
Version Control Register viii
Amendment History Register viii
Distribution List ix
Contact Information ix
Acronyms and Abbreviations x
Executive Summary xi

1 Purpose, Scope and Definitions 2
1.1 Purpose and rationale 2
1.2 Scope and application 2
1.3 Definitions and key terms 2

2 Principles, Governance and Accountability 5
2.1 Guiding principles 5
2.2 Governance, roles and accountability 5
2.3 The Board 5
2.4 Executive and management 5
2.5 The technology and data function 5
2.6 The safeguarding lead 6
2.7 Every staff member, volunteer and partner 6
2.8 The Technology and Data Governance group 6

3 Acceptable Use of Information Technology 8
3.1 General conduct 8
3.2 Accounts, passwords and multi-factor authentication 8
3.3 Devices, personal devices and remote work 8
3.4 Email, internet and messaging 8
3.5 Social media and public communication 9
3.6 What is never allowed 9

4 Cybersecurity and Resilience 11
4.1 The control baseline 11
4.2 Identity and access 11
4.3 Devices, updates and malware 11
4.4 Backup, encryption and recovery 11
4.5 Network and connectivity 11
4.6 People and awareness 11
4.7 Incident response 11
4.8 Business continuity 12

5 Data Governance and Information Management 14

5.1 The data protection principles....14
5.2 Lawful basis, consent and children's data....14
5.3 Classifying and handling data....14
5.4 Keeping data only as long as needed....14
5.5 The rights of data subjects....14
5.6 Data protection impact assessments....14
5.7 Cloud hosting and cross-border transfer....15
5.8 Registration with the Personal Data Protection Office....15

6 Digital Child Safeguarding 17
6.1 The principle....17
6.2 Images, identity and consent....17
6.3 The longitudinal child database....17
6.4 Online platforms and contact with children....17
6.5 Artificial intelligence and children's data....17

7 Artificial Intelligence Governance 19
7.1 KTN's position on artificial intelligence....19
7.2 Responsible AI principles....19
7.3 Permitted, restricted and prohibited uses....19
7.4 Classifying the risk of an AI use....20
7.5 Approval and human oversight....20
7.6 Verifying AI output....20
7.7 Generative AI and everyday staff use....20
7.8 Transparency and disclosure....20
7.9 Third party and embedded artificial intelligence....21
7.10 Watching what comes next....21

8 Vendors, Growth and Sustainable Technology 23
8.1 Cloud services and vendor management....23
8.2 Digital transformation and growth....23
8.3 The direction of travel....23
8.4 The maturity model....23
8.5 Environmental sustainability of technology....23

9 Compliance, Enforcement and Review 25
9.1 Monitoring, measurement and compliance....25
9.2 Indicators and the Board dashboard....25
9.3 Annual compliance review....25
9.4 Maturity targets....25
9.5 Legal and regulatory alignment....25
9.6 Uganda's law....25
9.7 Regional and international standards....25
9.8 Breaches, enforcement and protection....26
9.9 Review and amendment....26
9.10 Records, Audit Trail and Retention....26

9.10.1 The audit trail 26
9.10.2 Retention periods 27
9.10.3 Protection, review and disposal 27
10 Annexes 29
Annex A. Legal and regulatory validation register....29
Annex B. International standards and frameworks benchmark....30
Annex C. AI risk assessment matrix....30
Annex D. AI use approval form....31
Annex E. AI output verification checklist....31
Annex F. Data protection impact assessment template....32
Annex G. Vendor and cloud service due diligence checklist....32
Annex H. Cyber incident response checklist....33
Annex I. AI incident response checklist....33
Annex J. Business continuity quick checklist....33
Annex K. Digital safeguarding assessment tool....33
Annex L. Technology governance maturity model....34
Annex M. Board technology dashboard....34
Annex N. Annual compliance review tool....35

List of Tables

The following tables are used throughout this policy.

No.	Table	Where
1	Definitions of key terms	Section 1.3
2	Permitted, restricted and prohibited AI uses	Section 7.3
3	AI risk levels and what each requires	Section 7.4
4	Legal and regulatory validation register	Annex A
5	International standards and frameworks benchmark	Annex B
6	AI risk assessment matrix	Annex C
7	AI use approval form	Annex D
8	Data protection impact assessment template	Annex F
9	Technology governance maturity model	Annex L
10	Board technology dashboard	Annex M

List of Figures

This policy contains no numbered figures. Its content is carried in the tables listed above and in the registers and checklists at the annexes.

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 IT and AI Use Policy was considered and approved by the Board of Directors of Karamoja Tumaini Network in April 2026 and takes effect from that date as a governance instrument of the organisation. Compliance with it is mandatory for everyone within the scope set out in Section 1.2. It is the policy by which KTN keeps its technology and its handling of children's information trustworthy, and it sits above the convenience, cost or speed of any system, tool or model. The resolution reference and the signatures below complete the formal record of adoption.

Field	Detail
Policy status	Approved
Approval authority	Board of Directors
Approval date	April 2026
Effective date	April 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 SIGNATURES

Chairperson, Board of Directors
Karamoja Tumaini Network · April 2026

A Statement of Commitment from the Board

Karamoja Tumaini Network exists to protect children, and more and more of that protection runs through technology. We hold the records of children who are among the most vulnerable in Uganda, we follow each child for up to two years after they return home, and we keep that information in systems rather than in a locked cabinet. The same care we take with a child in person, we must take with the child's data. The Board regards the trust that lets KTN hold this information as one of the most valuable things the organisation has.

It is also one of the most easily lost. A breach, a careless message, a device left unlocked, or a tool used without thought can expose a child long after the moment of carelessness has passed, and harm done in the organisation's systems is harm done in the children's name. The Board does not treat technology as a back office matter. It treats it as a test of whether KTN can be trusted with what it knows about children.

This policy is how the Board answers that test. Two commitments sit above the rest and are never traded away for convenience or speed: children's safety comes before any system, and KTN does not use a tool, a vendor or a model that it cannot use safely and lawfully for children. Around those two, the policy builds the ordinary disciplines of a serious organisation. Protect the data. Secure the systems. Govern artificial intelligence with a person always responsible and always able to overrule it. Register and account for how children's information is used. Grow into new technology without losing control of it. Safeguarding comes before any technical or financial goal, every time.

The Board therefore commits to lead on this. We will approve and uphold this policy, resource the security, training and registration it requires, and stand behind any member of staff who refuses to use a tool that would put a child at risk. We will expect honest measurement and honest reporting, including of our mistakes and of anything that put a child's information at risk, because an organisation that hides its failures cannot learn from them. This policy binds every one of us, from the boardroom to the field and to every device and account that carries KTN's name.

Chairperson, Board of Directors
Karamoja Tumaini Network

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

Document Control

Field	Detail
Policy title	IT and AI Use 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); permitted to operate as a Non-Governmental Organisation by the National Bureau for Non-Governmental Organisations under permit number INDP000745-NB, file number MIA/NB/2026/06/7454
Version	1.0
Status	Approved and adopted by the Board of Directors
Approval date	April 2026
Effective date	April 2026
Policy owner	Karamoja Tumaini Network, acting through its Board of Directors
Policy custodian	The technology and data function, on behalf of the Executive Director
Applies to	All board members, staff, volunteers, interns, consultants, contractors and partners who use KTN systems, data or devices, or who act in KTN's name online; covering every device and place, all information technology and data, cloud services, the longitudinal child database, and every use of artificial intelligence
Reads alongside	The Strategic Plan 2026 to 2030; the Advocacy and Communications Policy; the Child Safeguarding Policy; the Protection from Sexual Exploitation and Abuse Policy; the Code of Conduct; the Whistleblowing Policy; the Gender Equality and Social Inclusion Policy; the Health, Safety and Security Policy; and the data protection duties under the Data Protection and Privacy Act, 2019 (Cap. 97)
Definitions	Key terms are defined in Section 1.3; acronyms and abbreviations are listed at the front of this document
Review frequency	At least once every twelve months, or earlier where required by a change in law, a major technology change, a serious incident, or the direction of the Board (Section 9.9)
Next scheduled review	March 2027

Version Control Register

Version	Date	Description of change	Approved by
1.0	April 2026	First edition. Full policy developed and benchmarked against Ugandan law and recognised international standards for information security, artificial intelligence governance, data protection and child online protection, with verified legal citations and a forward looking outlook on emerging technology, then 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; new Section 9.10; cross-references throughout; annex headings	Presentation and completeness update. List of Tables, List of Figures and an Executive Summary added; ten tables captioned; Contents rebuilt as one live field listing sub-headings and annexes; new Section 9.10, Records, Audit Trail and Retention; twenty-one cross-references to a superseded section scheme corrected; roman page numbering applied to the front matter; closing page added; Chairperson's signature applied to the Policy Approval page. Approved by the Executive Director as an administrative update under Section 9.9.	Executive Director

Distribution List

Recipient	Format	Date issued
Board of Directors	Electronic copy and one signed print copy for the corporate record	On approval
Executive Director and all staff	Electronic copy; included in the staff induction pack; signed acknowledgement returned by those with access to KTN systems	On approval
The technology and data function	Master copy, with the registers and tools in the annexes	On approval
Agencies, contractors and partners	Relevant extracts and this policy's clauses issued with their agreements	With each agreement
Donors	Full copy in due diligence and assessment packs	On request
Public	A summary is 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

Field	Detail
Policy owner	Karamoja Tumaini Network
Policy custodian	The technology and data function, on behalf of the Executive Director
Report a concern about data or a child	The Designated Safeguarding Lead, immediately, under the Child Safeguarding Policy
Report a security incident or data breach	The technology and data function, at once; serious matters reach the Executive Director (Sections 4.7 and 9.8)
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
Email	info@karamojatumaini.org
Website	www.karamojatumaini.org

Acronyms and Abbreviations

Acronym	Meaning
AI	Artificial Intelligence
AU	African Union
CHS	Core Humanitarian Standard on Quality and Accountability
CIS	Center for Internet Security
DPIA	Data Protection Impact Assessment
DPPA	Data Protection and Privacy Act, 2019 (Cap. 97)
DSL	Designated Safeguarding Lead (as named in the Child Safeguarding Policy)
EU	European Union
GDPR	General Data Protection Regulation
GESI	Gender Equality and Social Inclusion
ISO	International Organization for Standardization
KTN	Karamoja Tumaini Network
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
NITA-U	National Information Technology Authority, Uganda
PDPO	Personal Data Protection Office
PSEA	Protection from Sexual Exploitation and Abuse
UNCRC	United Nations Convention on the Rights of the Child

Key terms used in this policy are defined in Section 1.3.

Executive Summary

This is Karamoja Tumaini Network's authoritative framework for how technology, data and artificial intelligence are used in its work. It was adopted by the Board of Directors and applies to every person who acts for KTN, on every device and in every system, whether the work is done in an office, in a village in Napak, or on a phone on the road.

KTN's protection of children now runs through technology. The longitudinal child database that follows each child for two years after reintegration is the organisation's sharpest instrument and its heaviest liability in the same file. This policy treats that plainly: the security baseline in Chapter 4, the data governance rules in Chapter 5 and the digital safeguarding rules in Chapter 6 exist because a leaked record can put a child back within reach of the people who harmed them.

The policy does five things. It sets the acceptable use of KTN's technology and the conduct expected of everyone who touches it. It sets a cybersecurity baseline a small organisation can actually maintain. It governs how personal data is classified, held, shared and destroyed, in line with the Data Protection and Privacy Act. It governs artificial intelligence: what KTN permits, what it restricts, what it forbids, and where a named person must remain accountable for a decision. And it sets the monitoring, review and enforcement arrangements that let the Board see whether any of it is working.

It is written for what KTN is: a young, Karamojong-led organisation with two offices and a small team, working where power and connectivity are not guaranteed. The requirements are proportionate to that, and the maturity model at Annex L is the honest measure of how far the organisation has actually travelled rather than what it intends.

1

CHAPTER ONE

PURPOSE, SCOPE AND DEFINITIONS

What this policy is for, who and what it binds, and the words it uses precisely.

1 Purpose, Scope and Definitions

1.1 Purpose and rationale

Karamoja Tumaini Network runs on trust and on evidence. We hold sensitive information about children who are among the most vulnerable in Uganda, we follow each child for up to two years after they return home, and we publish what we learn so the wider sector can learn with us. None of that is possible without technology that works and that can be trusted, and without artificial intelligence used carefully where it genuinely helps.

This policy exists for four reasons. To keep children safe when their information is held, moved or analysed. To meet our duties under Uganda's law and the standards our partners and funders expect. To let staff use technology and artificial intelligence with confidence, knowing what is allowed and what is not. And to let the organisation grow into new tools without losing control of the things that matter. The policy is deliberately practical. It states what we do, what we will not do, who decides, and how we check.

1.2 Scope and application

This policy applies to everyone who acts for KTN: staff, board members, volunteers, interns, consultants and implementing partners. It applies wherever the work happens, in the office, in the field across the corridor, or remotely, and on any device used for KTN work, whether owned by KTN or by the individual.

It covers all information technology and information the organisation uses: computers, phones and tablets; accounts, email and messaging; networks and internet access; cloud services and the systems that hold KTN data, including the longitudinal child tracking database; websites and social media managed in KTN's name; and every use of artificial intelligence, whether built into a tool KTN buys, accessed through a public service, or developed with a partner.

Partners and contractors who handle KTN data or systems are bound by the relevant parts of this policy through their agreements with KTN. Where a partner cannot meet these standards, KTN does not share children's data with them.

1.3 Definitions and key terms

Plain definitions, so the policy reads the same way to everyone.

Term	What it means here
Personal data	Any information that can identify a person, on its own or combined with other information. A child's name, photograph, location, family details or case record are all personal data.
Special or sensitive data	Personal data that needs extra care, including data about a child, health information, and information about abuse, trafficking or legal matters. Almost all of the data KTN holds about children is sensitive.
Data subject	The person the data is about. For most of KTN's data, the data subject is a child.
Data controller	The organisation that decides why and how personal data is used. KTN is a data controller and is registrable as such with Uganda's Personal Data Protection Office.

Data processor	A person or company that handles data on KTN's instructions, such as a cloud provider. Processors are bound by written terms.
Artificial intelligence	Software that performs tasks normally needing human judgement, such as recognising patterns, generating text or images, translating language, or producing a prediction or recommendation.
Generative AI	Artificial intelligence that creates new content, such as a chatbot that writes text or a tool that makes an image. Public examples include large language model assistants.
AI system owner	The named person responsible for a particular use of artificial intelligence at KTN, from approval through to monitoring and retirement.
Processing	Anything done with data: collecting, storing, organising, using, sharing, or deleting it.
Incident	Any event that puts data, systems or people at risk, including a lost device, a suspected breach, a phishing attempt, or an AI output that could cause harm.

Table **1**. *Definitions of key terms used in this policy.*

2

CHAPTER TWO

PRINCIPLES, GOVERNANCE AND ACCOUNTABILITY

The principles that decide the undecided, and who owns technology decisions.

2 Principles, Governance and Accountability

2.1 Guiding principles

Every rule in this policy flows from a small set of principles. They are drawn from KTN's own values and from the international standards in Annex B, and they are the test we apply when a situation is not covered by a specific rule.

1. Children first. The safety, dignity and best interests of children come before convenience, cost or speed. This principle overrides the rest when they are in tension.
2. Lawful and accountable. We process data and use technology within the law, we can show why each use is justified, and someone is named as responsible for each.
3. Only what is needed. We collect, hold and share the least data required for a clear purpose, and we keep it only as long as that purpose lasts.
4. Human judgement stays in charge. Technology and artificial intelligence support decisions about children; they never make them alone. A person is always responsible for the outcome.
5. Secure by habit. Security is part of how we work every day, not a task left to one person or one moment.
6. Open about what we do. We are honest about how we use data and artificial intelligence, including with the children and families we serve, in language they understand.
7. Fair and inclusive. We watch for bias and exclusion in the tools we use, and we do not let technology widen the gaps it should help close.
8. Built to last and to grow. We choose tools and habits that the organisation can sustain and that can adapt as technology changes.

2.2 Governance, roles and accountability

Good technology governance is mostly about clear responsibility. The roles below set out who does what, so that nothing important falls between people. This structure grows with the organisation; in a small team one person may hold more than one role, but the responsibilities remain distinct.

2.3 The Board

The Board owns this policy, approves it and any material change, and holds management to account for it. At least twice a year the Board reviews the technology dashboard in Annex M, with attention to safeguarding, data protection and any serious incident. The Board treats a major data breach or an artificial intelligence failure that could harm a child as a matter to be informed of without delay, not at the next scheduled meeting.

2.4 Executive and management

The Executive Director is accountable for this policy in practice, ensures the resources and training it needs, and reports to the Board on compliance. Management makes sure the controls described here are in place, that staff are trained, and that the annual compliance review in Annex N is completed.

2.5 The technology and data function

Day to day responsibility for systems, security and data protection sits with the technology and data function, which in a small organisation may be a single named officer supported by trusted external help. This function

performs the role a data protection officer would, including maintaining the record of processing, leading data protection impact assessments, managing the relationship with the Personal Data Protection Office, and being the first point of contact for any incident. It also keeps the register of approved artificial intelligence uses.

2.6 The safeguarding lead

The safeguarding lead is responsible for the digital safeguarding provisions in Section 6, works with the technology and data function on anything that affects children's data, and reviews any incident involving a child. Digital safeguarding decisions follow the Child Safeguarding Policy where the two meet.

2.7 Every staff member, volunteer and partner

Everyone who uses KTN systems is responsible for following this policy, protecting the data and devices in their care, completing the training required of them, and reporting any incident or concern promptly and without fear. Reporting a mistake early is treated as responsible behaviour, not as fault.

2.8 The Technology and Data Governance group

As the organisation grows, a small Technology and Data Governance group, chaired by the Executive Director and including the technology and data function and the safeguarding lead, meets at least quarterly. It reviews the artificial intelligence register, the cybersecurity risk register, open incidents, and progress against the maturity model in Annex L. Until the group is formally constituted, these reviews are carried out by management.

3

CHAPTER THREE

ACCEPTABLE USE OF INFORMATION TECHNOLOGY

What acceptable use of KTN's devices, accounts and networks means.

3 Acceptable Use of Information Technology

This section sets the everyday standard for using KTN technology. The rule of thumb is simple: use KTN systems for KTN work, treat the information in your care as if it were about your own family, and assume that what you do on KTN systems can be reviewed for legitimate reasons.

3.1 General conduct

1. Use KTN accounts, devices and systems mainly for KTN work. Limited reasonable personal use is acceptable where it does not affect security, cost or your duties.
2. Keep your work and your access to data within what your role requires. Do not look at children's records you have no need to see.
3. Do not use KTN systems for anything unlawful, for harassment, or for content that would shame the organisation or harm a child.

3.2 Accounts, passwords and multi-factor authentication

1. Each person has their own account. Do not share accounts or passwords, and do not use someone else's login.
2. Use a long, unique password for each KTN system. A passphrase of several words is both stronger and easier to remember. A password manager is the recommended way to keep them.
3. Turn on multi-factor authentication wherever a system offers it, especially for email, cloud storage and the child database. This single step prevents most account compromises.

3.3 Devices, personal devices and remote work

1. Lock every device with a password, PIN or biometric, and set it to lock itself when idle.
2. Where staff use their own phones or computers for KTN work, the device must be kept up to date, protected by a screen lock, and free of obvious risks. KTN data on a personal device remains KTN's and must be removable when someone leaves.
3. When working in the field or remotely, avoid handling sensitive data on shared or public computers, and avoid unsecured public wireless networks for anything involving children's data.
4. Report a lost or stolen device at once, so access can be cut off and any data protected.

3.4 Email, internet and messaging

1. Treat email and messaging as places where mistakes travel fast. Check the recipient before sending anything about a child, and never put a child's full identifying details in an unprotected message.
2. Be alert to phishing: unexpected links, urgent requests for money or passwords, and messages that do not look quite right. When in doubt, do not click, and ask the technology and data function.
3. Use approved tools for sharing files. Do not move children's data through personal email or consumer messaging apps that KTN has not assessed.

3.5 Social media and public communication

Social media follows the Brand Style Guide and the rules on writing about children in Section 6. In short: one idea per post, a calm and specific voice, never a child's hardship used to attract attention, and no identifying image of a child who could be put at risk. Only authorised people post in KTN's name. The handle is the one set out in the Brand Style Guide; personal opinions are not posted as KTN's.

3.6 What is never allowed

1. Sharing a child's identifying information or image publicly without the consent required by Section 6.
2. Installing software from untrusted sources, or disabling security protections, on a device used for KTN work.
3. Using KTN systems to access, store or share illegal content, or any material that sexualises or endangers children. Any such material encountered is reported immediately under the Child Safeguarding Policy.
4. Moving children's data into an unapproved tool, including a public artificial intelligence service, except as Section 7 allows.

4

CHAPTER FOUR

CYBERSECURITY AND RESILIENCE

Keeping systems and people safe from compromise, and ready to recover.

4 Cybersecurity and Resilience

KTN's security approach follows the structure of the recognised frameworks in Annex B, in particular the functions of the NIST Cybersecurity Framework and the priority controls of the CIS Controls, scaled to the size of the organisation. The aim is not a fortress but a sound, maintainable baseline that protects children's data and keeps the work running.

4.1 The control baseline

KTN organises its security around six tasks, in plain terms: know what we have, protect it, watch for trouble, respond when it happens, recover, and govern the whole through clear responsibility. The specific controls below put that into practice.

4.2 Identity and access

1. Access to systems and data follows need. People are given the least access their role requires, and access is reviewed when roles change and removed promptly when someone leaves.
2. The child database and other sensitive systems are restricted to named, trained users, with multi-factor authentication and a record of who has access.

4.3 Devices, updates and malware

1. Devices used for KTN work run supported, updated software, with security updates applied promptly. Out of date systems are the most common way in for attackers.
2. Reputable malware protection is kept active and current on computers used for KTN work.

4.4 Backup, encryption and recovery

1. Important data, above all the child database, is backed up regularly, with at least one copy held separately, and the ability to restore it is tested, not assumed.
2. Sensitive data is encrypted in transit and, where the tools allow, at rest, so that a lost device or intercepted message does not become a breach.

4.5 Network and connectivity

Office and field connections use protected networks. Sensitive work is not done over open public wireless without protection such as a trusted virtual private network.

4.6 People and awareness

Because most incidents begin with a person, every staff member and volunteer receives security awareness training on joining and at least once a year, covering passwords, phishing, devices and safe handling of children's data.

4.7 Incident response

When something goes wrong, speed and honesty limit the harm. Any suspected incident is reported at once to the technology and data function, which follows the Cyber Incident Response Checklist in Annex H:

contain the problem, assess what was affected, protect the people involved, fix the cause, and record what happened and what was learned. An incident involving a child's data is also reported to the safeguarding lead, and a personal data breach is handled under the duties in Section 5, including notifying the Personal Data Protection Office and affected people where the law requires.

4.8 Business continuity

KTN identifies the few systems the work cannot run without, above all the child database and communications, and keeps a simple plan, summarised in Annex J, for carrying on if they are lost: where the backups are, who to call, and how to operate in the meantime. The plan is reviewed each year and after any major disruption, including those caused by insecurity or power and connectivity loss in the field.

5

CHAPTER FIVE

DATA GOVERNANCE AND INFORMATION MANAGEMENT

How information is classified, stored, shared, retained and destroyed.

5 Data Governance and Information Management

This section sets out how KTN handles personal data. It follows Uganda's Data Protection and Privacy Act and reflects the wider standards in Annex B, including the principles shared with the General Data Protection Regulation. Because almost all of KTN's data concerns children, the cautious reading of every rule applies.

5.1 The data protection principles

KTN processes personal data in line with the principles in Uganda's law: lawfulness and fairness, a clear and specific purpose, collecting only what is needed, keeping it accurate, holding it no longer than necessary, keeping it secure, and being able to account for all of this. These principles are not paperwork. They are the practical test for every form, database field and data sharing arrangement.

5.2 Lawful basis, consent and children's data

KTN only collects personal data where it has a proper basis and a real need, tied to its work of prevention, response, reintegration, education, advocacy or evidence. For children, consent is handled with particular care: it is sought from the child in an age appropriate way and from a parent or guardian or recognised caregiver, it is informed, and it can be withdrawn. Where seeking consent is not possible or not in the child's interest, the most protective lawful basis is used and the reasoning is recorded. A child's data is never used for a new purpose the child and guardian were not told about without fresh consideration.

5.3 Classifying and handling data

KTN sorts its information by how sensitive it is, so that the strongest protection goes where it is most needed. As a working rule, anything that identifies a child, or concerns abuse, trafficking, health or legal matters, is treated as the most sensitive class, with restricted access, encryption where possible, and no movement into unapproved tools. Less sensitive information, such as general organisational documents, is handled with proportionate care.

5.4 Keeping data only as long as needed

KTN keeps personal data for as long as the child's safety and the work require, including the follow up period of up to two years after reintegration and any period the law requires, and then disposes of it securely. A simple retention schedule records how long each kind of record is kept and when it is reviewed. Secure disposal means data is deleted or destroyed so it cannot be recovered.

5.5 The rights of data subjects

People whose data KTN holds, and their guardians, have rights under Uganda's law, including to know what is held, to have errors corrected, and in defined circumstances to have data erased or to object to its use. KTN handles such requests fairly and within the time the law allows, in language the person understands, balancing a child's rights with the duty to keep the child safe.

5.6 Data protection impact assessments

Before starting anything that could carry real risk to people's data, such as a new database, a new way of collecting children's information, or a new use of artificial intelligence on personal data, KTN completes a data protection impact assessment using the template in Annex F. The assessment names the risks, sets out how they are reduced, and is approved before the activity begins. A high residual risk is referred upward before proceeding.

5.7 Cloud hosting and cross-border transfer

KTN takes a cloud first approach, which keeps data more secure and available than local storage a small organisation could manage alone. Because cloud services often store data outside Uganda, KTN follows the cross-border rules in Uganda's law: personal data is transferred or stored abroad only where the destination offers protection at least equivalent to Uganda's, or where consent allows, and KTN keeps records of the legal basis and safeguards for each arrangement. These records are kept ready for inspection. Cloud providers are assessed under Section 8.1 and Annex G, and bound by written terms before any children's data is placed with them.

5.8 Registration with the Personal Data Protection Office

As an organisation that collects and processes personal data, KTN is required to register as a data controller with Uganda's Personal Data Protection Office, to renew that registration each year within the time allowed, and to submit the annual compliance report the law requires. Maintaining this registration is a standing responsibility of the technology and data function. The Personal Data Protection Office has confirmed that this duty applies to every entity handling the data of Ugandan citizens, and has begun enforcing it.

6

CHAPTER SIX

DIGITAL CHILD SAFEGUARDING

Protecting children in and from KTN's digital spaces.

6 Digital Child Safeguarding

This is the section the rest of the policy protects. Children's safety online and in our data is not one duty among many; it is the duty. Where this section and any other guidance differ, the most protective reading for the child wins. This section sits under the Child Safeguarding Policy and the Protection from Sexual Exploitation and Abuse Policy, and reflects the international child online protection standards in Annex B.

6.1 The principle

Children are people with names, not cases or content. We never trade a child's dignity or safety for a donation, a report or a faster process. Every digital decision about a child is made as if the child were our own.

6.2 Images, identity and consent

1. A child's full name and an identifying photograph are never published together in public material without informed consent from both the child and a guardian, in line with the Brand Style Guide.
2. Where a child could be put at risk, especially around trafficking, abuse or legal matters, identifying images are not used. Crop, angle away, or use only images cleared for the purpose, or a first name or a changed name with that change stated.
3. Abuse, trafficking and trauma are never described or shown in graphic detail, and a child's hardship is never used as a fundraising hook.

6.3 The longitudinal child database

KTN's database that follows individual children over time is its most sensitive asset and its most valuable one. It is protected accordingly: access is limited to named, trained users; multi-factor authentication is required; entries are kept accurate and minimal; the data is backed up and, where possible, encrypted; and every use is for a purpose the child and guardian were informed of. The database is covered by a data protection impact assessment that is reviewed when it changes.

6.4 Online platforms and contact with children

Where KTN uses digital tools that involve children, including any messaging, feedback or service platform, the tool is assessed for safety before use, contact with children follows the Child Safeguarding Policy, and private one to one digital contact between a staff member or volunteer and a child outside approved channels is not permitted. Feedback mechanisms for children are offered in Nga'Karamojong and in forms accessible to those who may not read or write.

6.5 Artificial intelligence and children's data

Children's personal data is not entered into public or unapproved artificial intelligence tools. Any use of artificial intelligence that touches children's data is treated as a high risk use under Section 7, requires approval and a data protection impact assessment, keeps a person responsible for every decision, and is tested for bias that could affect children unfairly. The standards for artificial intelligence affecting children draw on recognised guidance for child rights in the digital environment, listed in Annex B.

7

CHAPTER SEVEN

ARTIFICIAL INTELLIGENCE GOVERNANCE

Using artificial intelligence honestly, with a human answerable for every output.

7 Artificial Intelligence Governance

Artificial intelligence can help KTN do more for children: translating and reaching families in Nga'Karamojong, easing the burden of analysis on a small team, and finding patterns in long term data that no person could hold in mind. It also carries real risks: getting things wrong with confidence, hidden bias, and the temptation to let a machine decide what only a person should. This section lets KTN use artificial intelligence where it genuinely helps, within firm limits. It is built on the recognised responsible AI standards in Annex B and anticipates the direction of Uganda's emerging artificial intelligence rules and the international frameworks described in Section 9.7.

7.1 KTN's position on artificial intelligence

KTN uses artificial intelligence as a tool that supports people, never as a replacement for human judgement about a child. Adoption is deliberate and evidence led: a use is adopted because it demonstrably helps and can be governed safely, not because it is new. Cultural fitness matters as much as technical fitness, since a tool that does not work in Nga'Karamojong or that misreads the Karamoja context is not fit for KTN's purpose.

7.2 Responsible AI principles

KTN's use of artificial intelligence follows principles common to the OECD, UNESCO and the recognised management standards: it respects human rights and the best interests of the child; it keeps meaningful human oversight; it is transparent, so people know when artificial intelligence is in use and can question it; it is tested for fairness and watched for bias; it is secure and protective of data; and it is accountable, with a named owner for every use.

7.3 Permitted, restricted and prohibited uses

Category	How KTN treats it
Permitted with care	Lower risk uses that do not involve children's personal data, such as drafting and editing internal documents, summarising public material, translating general content, learning and research, and routine administrative help. Outputs are checked by a person before use.
Restricted, approval needed	Uses that touch personal data, analyse programme data, support a decision affecting a child or family, or face the public in KTN's name. These require approval under 10.5, a data protection impact assessment, and human oversight of every outcome.
Prohibited	Uses that are not allowed at KTN: entering children's identifying data into public artificial intelligence tools; any automated decision that affects a child without a person responsible and able to overturn it; profiling or scoring of children; manipulation, or covert use that hides from people that artificial intelligence is involved; and any use designed to evade this policy.

Table **2**. *Permitted, restricted and prohibited uses of artificial intelligence.*

7.4 Classifying the risk of an AI use

Before an artificial intelligence use is approved, its risk is classified, using an approach aligned with the international risk based standards and the direction of Uganda's emerging rules. The classification decides how much scrutiny and oversight the use needs. The matrix in Annex C guides this judgement.

Risk level	What it covers	What is required
Unacceptable	Prohibited uses listed in 10.3.	Not used.
High	Anything touching children's data, supporting decisions about a child, or facing the public in KTN's name.	Approval, data protection impact assessment, named owner, human oversight of every outcome, bias testing, and logging.
Limited	Uses with modest risk, such as translating or summarising non personal content used externally.	Approval, a check of outputs by a person, and disclosure where people interact with it.
Minimal	Low risk internal help that does not involve personal data.	General staff guidance and output checking; no separate approval needed.

Table 3. How the risk of an artificial intelligence use is classified, and what each level requires.

7.5 Approval and human oversight

A new use of artificial intelligence above minimal risk is approved before it begins, using the AI Use Approval Form in Annex D. Approval names the owner, the purpose, the data involved, the risks and how they are handled, and the way a person will oversee the outcomes. The technology and data function keeps the register of approved uses. For every approved use, a person remains responsible for the result, can understand and explain it in broad terms, and can overrule it. Artificial intelligence never has the final word on a decision that affects a child.

7.6 Verifying AI output

Artificial intelligence can be confidently wrong. Output is therefore checked before it is relied on or shared, using the AI Output Verification Checklist in Annex E. Facts, figures and quotations produced by a tool are confirmed against a trusted source, in keeping with KTN's rule that every statistic is sourced and dated. Artificial intelligence is not treated as a source in its own right.

7.7 Generative AI and everyday staff use

Staff may use approved generative artificial intelligence tools to help with everyday work such as drafting, editing and summarising, within these limits: no children's personal data and no confidential information is entered into a public tool; the output is the staff member's responsibility and is checked before use; and the work still meets KTN's voice and house style, which means no buzzwords, no invented certainty, and plain, specific writing. Artificial intelligence helps produce the draft; the person remains the author.

7.8 Transparency and disclosure

KTN is open about its use of artificial intelligence. Where a person interacts with an artificial intelligence tool rather than a member of staff, this is made clear. Where artificial intelligence has materially shaped public content, KTN is willing to say so. This openness reflects both KTN's honesty as an organisation and the transparency duties emerging in law.

7.9 Third party and embedded artificial intelligence

Much artificial intelligence reaches KTN inside tools it buys. Vendors are assessed under Section 8.1 and Annex G, including what artificial intelligence their product uses, what it does with KTN's data, whether it is used to train the vendor's models, and what assurance the vendor can give on safety and bias. A tool that cannot answer these questions is not used for sensitive work.

7.10 Watching what comes next

Technology will keep changing, and so will the risks and the opportunities. KTN scans the horizon in a light but deliberate way: the technology and data function keeps note of relevant new tools, new risks, and new rules, and brings anything significant to the governance group. A promising new technology is piloted in a contained way, with a risk assessment, before it is adopted widely. The maturity model in Annex L sets the direction of travel.

8

CHAPTER EIGHT

VENDORS, GROWTH AND SUSTAINABLE TECHNOLOGY

Choosing vendors deliberately, growing without outgrowing controls, and counting technology's environmental cost.

8 Vendors, Growth and Sustainable Technology

8.1 Cloud services and vendor management

KTN depends on outside providers for much of its technology, which is sensible for an organisation of its size but means KTN's data is only as safe as the providers it chooses. Before a new tool or service that will hold KTN data is adopted, it is assessed using the checklist in Annex G: what data it will hold, where that data lives, how it is secured, what happens to the data if KTN leaves, what artificial intelligence it uses, and what the provider commits to in writing. Providers that will handle personal data sign terms that bind them to protect it and to act only on KTN's instructions. Cost is weighed alongside security, reliability and the protection of children's data, never above them.

8.2 Digital transformation and growth

This policy is meant to enable growth, not to freeze the organisation in place. KTN will take on new tools as it scales across the corridor, and this section sets the direction so that growth stays controlled.

8.3 The direction of travel

KTN improves its technology in step with its capacity to govern it. New systems are introduced in phases, proven on a small scale before they are relied on widely, and chosen for whether the organisation can sustain them. Priorities over the plan period include strengthening the child database and its security, maturing data protection practice to full registration and routine impact assessments, and building the evidence and dashboard capability that the Data pillar of the Strategic Plan depends on. Earned income work, including monitoring and evaluation consulting and a planned programme of artificial intelligence for social impact, is governed by this policy like any other use of technology.

8.4 The maturity model

KTN measures its progress against the technology governance maturity model in Annex L, which describes what good looks like across governance, security, data protection, artificial intelligence and digital safeguarding, from a basic starting point to a mature state. The model is used once a year to see how far KTN has come and where to focus next, and it gives funders an honest picture of the organisation's digital maturity.

8.5 Environmental sustainability of technology

KTN's technology choices reflect its commitment to the environment, in keeping with the Environmental Policy. In practice this means keeping devices in use for their full working life rather than replacing them early, disposing of old electronics responsibly rather than as ordinary waste and removing any data first, preferring providers with credible energy and sustainability practices where there is a real choice, and being mindful that some artificial intelligence carries a significant energy cost, which is one factor among others when deciding whether a heavier tool is justified. These are modest measures for a small organisation, applied with common sense.

9

CHAPTER NINE

COMPLIANCE, ENFORCEMENT AND REVIEW

How compliance is measured, the law this policy answers to, what happens when it is broken, and the review that keeps it current.

9 Compliance, Enforcement and Review

9.1 Monitoring, measurement and compliance

A policy that is not checked is a policy that drifts. KTN measures whether this policy is working and acts on what it finds, in the same outcome focused spirit as the rest of its work.

9.2 Indicators and the Board dashboard

A small set of indicators, set out in Annex M, gives the Board a clear view of technology and data health: whether training is current, whether data protection registration and impact assessments are up to date, how many incidents occurred and how they were handled, the state of backups, and the status of approved artificial intelligence uses. These are reported to the Board at least twice a year. They are measures, not targets dressed as achievements; where a measure is weak, that is shown plainly.

9.3 Annual compliance review

Once a year, management completes the compliance review in Annex N, which checks this policy against what is actually happening, confirms the legal citations in Annex A are still current, and produces a short list of actions with owners and dates. The review is shared with the Board.

9.4 Maturity targets

KTN sets a realistic direction on the maturity model in Annex L and reviews progress each year. Targets are described as targets, with the current position stated honestly alongside them, so that progress is real and not asserted.

9.5 Legal and regulatory alignment

KTN operates within Uganda's law and aligns with recognised international standards. This section summarises the framework; Annex A gives the verified detail, with the status and date of each instrument, and Annex B lists the standards KTN benchmarks against. The legal landscape is changing quickly, especially for artificial intelligence, so this section is reviewed each year.

9.6 Uganda's law

The central instrument is the Data Protection and Privacy Act, with its 2021 Regulations, overseen by the Personal Data Protection Office under the National Information Technology Authority. It sets the principles in Section 5, the registration duty in Section 5.8, and the rules on consent, sensitive data and cross-border transfer that shape how KTN handles children's information. The right to privacy is also protected by the Constitution. Cybercrime is addressed by the Computer Misuse Act; KTN notes that the 2022 amendment to that Act was set aside by the Constitutional Court in 2026 on procedural grounds, while the core offences of the original Act continue, and that the area may be legislated again. Other relevant laws include those on electronic transactions and signatures, the interception of communications, access to information, and the protection of children. KTN also follows the direction of Uganda's emerging national strategy on artificial intelligence and the National Information Technology Authority's digital plans.

9.7 Regional and international standards

At the regional level, KTN has regard to the African Union's Convention on Cyber Security and Personal Data Protection and its Continental Artificial Intelligence Strategy, which calls for AI adapted to African languages and contexts, a principle close to KTN's own. Internationally, KTN aligns its data protection practice with the

principles shared by the General Data Protection Regulation, and its artificial intelligence practice with the OECD and UNESCO principles, the recognised management and risk standards, and the emerging international rules on artificial intelligence, including the European Union's Artificial Intelligence Act and the Council of Europe's framework convention. KTN is not bound by all of these, but it treats them as the benchmark a serious organisation should meet, and as a guide to where regulation is heading. Annex B maps the full set.

9.8 Breaches, enforcement and protection

This policy carries weight. A breach of it is taken seriously, in proportion to the harm and the intent. A genuine mistake reported promptly is treated as part of how a learning organisation stays safe, and the person is supported, not punished, for coming forward. A deliberate or reckless breach, especially one that endangers a child or a child's data, is a disciplinary matter and may also be a legal one, handled under the Code of Conduct and, where relevant, the Child Safeguarding and Whistleblowing Policies. Anyone may raise a concern about a breach safely and, if they wish, in confidence, through the routes in the Whistleblowing Policy, without fear of retaliation. Suspected criminal acts and serious data breaches are reported to the relevant authorities as the law requires.

9.9 Review and amendment

The Board approves this policy and any material change to it. The technology and data function reviews it at least once a year, and sooner when the law changes, when a significant new technology is adopted, or when an incident shows the policy needs to be stronger. Each review confirms that the legal citations in Annex A remain current and that the standards in Annex B are still the right ones. Minor updates, such as correcting a citation or a contact, may be made by management and recorded; substantive changes return to the Board. The version and date on the cover and in the document control table always show which copy is current.

9.10 Records, Audit Trail and Retention

A technology policy that leaves no trace cannot be audited, and a control KTN cannot evidence is a control KTN cannot claim. Every duty this policy creates leaves a record, made when the thing happens, protected from quiet alteration, and destroyed on a schedule rather than at anyone's discretion. This section reads with the Data Protection and Privacy Policy, which governs the personal data those records contain.

9.10.1 The audit trail

Recorded when it happens. An artificial intelligence approval under Section 7.5, a data protection impact assessment under Section 5.6, a vendor assessment under Section 8.1, an access grant or removal under Section 4.2 and an incident under Section 4.7 are entered in their register at the moment they occur, not reconstructed at review time.

The artificial intelligence register is the spine. It holds every approved use, who owns it, its risk classification, the date it was approved and the date it is next reviewed. A tool that is not in the register is not in approved use, and that is the test applied at the annual compliance review.

Systems keep their own log. Every system holding personal data records who signed in, what they opened, changed or exported, and when. Logs for the longitudinal child database are retained for twelve months, with the last three months immediately retrievable, and are reviewed each quarter by the technology and data function for access that has no business reason behind it.

Every decision, with its reason. Approvals, refusals and exceptions are recorded with their date, the person who decided and the reason. That includes the two an auditor asks about first: a decision that an artificial intelligence use was low risk, and a decision that an incident did not need to be escalated.

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, can be reconstructed.

9.10.2 Retention periods

Records containing personal data are retained and destroyed under the schedule in the Data Protection and Privacy Policy, which governs where the two policies meet. For the records this policy creates, KTN proposes that system access logs are held for twelve months, security and artificial intelligence incident records for seven years, and the artificial intelligence register for as long as a tool is in use and three years after it is retired. These periods are proposals until the Board adopts them. Where a donor agreement, an open investigation, a police or court process 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.

9.10.3 Protection, review and disposal

Protected while held. Logs and incident records are held with access by named role, separate from personnel files, and are covered by the same backup and encryption rules as the systems they describe.

Reviewed once a year. The technology and data function reviews the registers annually against this section as part of the compliance review at Section 9.3, 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. Electronic records are deleted from live systems and from backups on their next cycle, and 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.

A

ANNEXES

ANNEXES

The working tools: registers, checklists, assessment forms and templates for daily use.

10 Annexes

The annexes are the working tools of this policy: the registers, checklists, assessment forms and templates referred to in the sections above. They are maintained by the policy custodian and may be updated without a full policy revision.

Annex A. Legal and regulatory validation register

This register records the instruments and standards this policy relies on, with their status and date as verified at the latest review. It exists so that any reader, including a funder or auditor, can see that the policy rests on real and current law. Entries should be reconfirmed at each annual review, since this is a fast moving area.

Instrument	Status and date	Relevance to KTN
Constitution of the Republic of Uganda, 1995, Article 27	In force. Guarantees the right to privacy.	The constitutional basis for protecting personal data.
Data Protection and Privacy Act, 2019 (Cap. 97) (Cap. 97)	In force; commenced 2019. Supported by the Data Protection and Privacy Regulations, 2021.	The central data protection law. Sets KTN's principles, registration duty and transfer rules.
Personal Data Protection Office	Operational under the National Information Technology Authority since 2021; actively enforcing, including a 2025 decision confirming offshore entities must register.	Uganda's regulator. KTN registers and reports to it.
Computer Misuse Act, 2011	Original Act in force. The Computer Misuse (Amendment) Act, 2022 was declared null and void by the Constitutional Court in 2026 on procedural grounds; the area may be legislated again.	Governs cybercrime such as unauthorised access. KTN tracks any new legislation.
Electronic Transactions Act and Electronic Signatures Act	In force.	Recognise electronic records and signatures KTN may rely on.
Access to Information Act, 2005 (Cap. 95)	In force.	Frames transparency duties and limits.
Children Act (Cap. 59), as amended 2016	In force.	The legal foundation for KTN's child protection work and duties.
Uganda national strategy on artificial intelligence and emerging technologies	In development as at 2026; a risk based approach is expected.	KTN aligns early with the likely direction, including registration of higher risk uses.
African Union Malabo Convention	Adopted 2014; entered into force 2023.	Regional baseline on cybersecurity and personal data protection.
African Union Continental Artificial Intelligence Strategy	Endorsed by the AU Executive Council in 2024.	Regional direction on responsible AI adapted to African contexts and languages.
General Data Protection Regulation (EU) 2016/679	In force in the European Union; a global reference.	KTN aligns its data protection practice with its shared principles.

EU Artificial Intelligence Act, Regulation (EU) 2024/1689	In force 2024, applying in phases to 2027 and beyond; a 2026 agreement defers the main high risk duties.	The leading international AI law. KTN treats it as a benchmark and a guide to future rules.
Council of Europe Framework Convention on Artificial Intelligence	Opened for signature 2024; the first binding international AI treaty.	An international benchmark for rights based AI governance.

Table 4. Legal and regulatory validation register.

Annex B. International standards and frameworks benchmark

The recognised standards KTN benchmarks against, and what each contributes to this policy. KTN does not seek formal certification against all of these, but uses them as the measure of good practice.

Standard or framework	What it contributes
ISO/IEC 27001 and 27002 (2022)	The structure for managing information security and the catalogue of controls behind Section 4.
ISO/IEC 42001 (2023)	The first management system standard for artificial intelligence; the model for KTN's AI governance in Section 7.
ISO/IEC 23894 and 38507	Guidance on managing AI risk and on the governance of AI in organisations.
NIST Cybersecurity Framework 2.0 (2024)	The six functions that organise KTN's security: govern, identify, protect, detect, respond, recover.
NIST AI Risk Management Framework and its generative AI profile	A practical approach to mapping, measuring and managing AI risk, reflected in Annex C.
CIS Critical Security Controls	The prioritised, practical controls a smaller organisation can implement first.
OECD AI Principles and UNESCO Recommendation on the Ethics of AI	The values behind KTN's responsible AI principles in Section 7.2.
UNICEF guidance on AI for children and Responsible Data for Children	Child specific standards for artificial intelligence and for handling children's data, behind Sections 5 and 6.
WeProtect Global Alliance standards	The reference for protecting children from online sexual exploitation and abuse.
Core Humanitarian Standard (2024) and Sphere	Accountability to the people KTN serves, including safe complaints and responsible data.
Principles for Digital Development and sector digital principles	Practical principles for responsible technology in development and humanitarian work.

Table 5. International standards and frameworks benchmark.

Annex C. AI risk assessment matrix

Used to classify a proposed artificial intelligence use before approval. Score the likelihood and the impact of things going wrong, with particular weight on any effect on a child, then read the risk level. Any use that could affect a child starts at high regardless of likelihood.

Question	Consider	Effect on classification
Does it use children's personal data?	Yes or no.	Any yes makes the use at least high risk.
Does it support a decision about a child or family?	Directly or indirectly.	Any yes makes the use at least high risk and requires human oversight of every outcome.
Does it face the public in KTN's name?	Outreach, chat, content.	Raises the level; requires disclosure and output checking.
Could it produce biased or unfair results?	Across sex, age, disability, district.	Raises the level; requires bias testing before and during use.
How serious is the worst plausible outcome?	From minor to harm to a child.	Harm to a child is treated as critical and may make the use unacceptable.
Can a person understand and overturn the result?	Yes or no.	If no, the use is not approved until oversight is built in.

Table 6. Artificial intelligence risk assessment matrix.

Annex D. AI use approval form

Completed for any artificial intelligence use above minimal risk, and held in the register by the technology and data function.

Field	Entry
Proposed use and purpose	what it is for, in plain terms
Owner	the named person responsible
Tool or service, and any artificial intelligence inside it	
Data involved	and whether any is children's personal data
Risk level	from Annex C, with reasoning
Data protection impact assessment	reference, if required
How a person oversees the outcome	
How outputs are checked	Annex E
Bias and fairness check	where relevant
Disclosure to users	where they interact with it
Approved by and date	
Review date	

Table 7. Artificial intelligence use approval form.

Annex E. AI output verification checklist

Run before relying on or sharing anything an artificial intelligence tool produced.

1. Are the facts, figures and quotations confirmed against a trusted, dated source, not taken on the tool's word?
2. Is anything sensitive, identifying or about a child absent from what was entered into the tool?
3. Has a person read the whole output and judged it correct, fair and appropriate?
4. Does it meet KTN's voice and house style: plain, specific, no buzzwords, no invented certainty?
5. Is it free of bias or language that could demean or endanger a child or group?
6. If it will be public, is any material role of artificial intelligence acknowledged where appropriate?

Annex F. Data protection impact assessment template

Completed before a new or changed activity that could carry real risk to people's data, and approved before the activity begins.

Section	Entry
Activity and purpose	
What personal data is involved	and whose, including children
Why the data is needed	and the lawful basis
How consent is handled	for children and guardians
Who has access, and how it is secured	
Where the data is stored	and any transfer outside Uganda
Risks to people	and how each is reduced
Residual risk	and whether it is acceptable
Approved by and date	
Review date	

Table 8. Data protection impact assessment template.

Annex G. Vendor and cloud service due diligence checklist

Completed before adopting a service that will hold KTN data, and kept on file.

1. What KTN data will it hold, and is any of it children's personal data?
2. Where is the data stored, and does that location offer protection at least equivalent to Uganda's?
3. How is the data secured, in transit and at rest, and how is access controlled?
4. Does the provider use KTN's data to train its own models, and can that be turned off?
5. What artificial intelligence does the product use, and what assurance is given on safety and bias?
6. What happens to KTN's data if KTN stops using the service, and can it be exported and deleted?
7. Will the provider sign terms binding it to protect the data and act only on KTN's instructions?
8. What is the provider's record on security incidents and reliability?

Annex H. Cyber incident response checklist

Followed by the technology and data function when an incident is suspected. Speed and honesty limit the harm.

1. Contain it: isolate the affected device, account or system to stop the problem spreading.
2. Assess it: work out what was affected, including whether any personal or children's data was involved.
3. Protect people: take steps to reduce harm to anyone affected, and tell the safeguarding lead if a child is involved.
4. Notify: where personal data was breached, follow the duty to inform the Personal Data Protection Office and affected people as the law requires.
5. Fix the cause: close the gap that allowed it, change passwords, restore from clean backups.
6. Record and learn: write down what happened, what was done, and what will prevent it next time; report to management and, if serious, the Board.

Annex I. AI incident response checklist

Followed when an artificial intelligence use produces a harmful, wrong or unfair result, or behaves unexpectedly.

1. Stop relying on the output and, if needed, pause the use.
2. Assess the harm, especially any effect on a child, and tell the safeguarding lead if a child is affected.
3. Correct anything wrong that has already been acted on or shared.
4. Find the cause: bad input, bias, a flaw in the tool, or misuse, and decide whether the use can continue safely.
5. Record the incident in the artificial intelligence register, and update the approval, the controls or the decision to use the tool.
6. Report a serious case to management and the Board, and to a vendor or authority where appropriate.

Annex J. Business continuity quick checklist

The minimum KTN keeps ready so the work can continue if key technology is lost.

1. The few systems the work cannot run without are listed, with the child database and communications first.
2. Recent backups exist, are held separately, and have been tested by actually restoring them.
3. A short contact list shows who to call for each critical system and provider.
4. A simple way to keep operating without the main systems is written down, including for field conditions where power or connectivity may fail.
5. The plan is reviewed each year and after any major disruption.

Annex K. Digital safeguarding assessment tool

Used before adopting any digital tool or activity that involves children, and reviewed when it changes.

1. Does the tool collect or show children's data, and is that strictly necessary?
2. Could a child be identified or put at risk through the tool, and how is that prevented?
3. How is consent from the child and guardian obtained and recorded?
4. Are contact channels with children controlled, with no private one to one contact outside approved routes?
5. Is a feedback or complaints route available to children in Nga'Karamojong and in accessible forms?
6. Does the tool meet the security and data protection standards in Sections 4 and 5?
7. Who is the named safeguarding owner for this tool or activity?

Annex L. Technology governance maturity model

A simple picture of progress across the areas this policy governs, from a basic starting point to a mature state. Used once a year to see how far KTN has come and where to focus. KTN states its current position honestly against each row.

Area	Basic	Developing	Mature
Governance	Policy exists; roles informal.	Roles defined; governance group meets; dashboard reviewed.	Governance routine; Board oversight embedded; continual improvement.
Security	Passwords and updates in place.	Multi-factor authentication, backups tested, awareness training annual.	Controls aligned to recognised frameworks; incidents rare and well handled.
Data protection	Aware of duties.	Registered with the regulator; impact assessments for new activities.	Registration and reporting routine; data protection part of every project.
Artificial intelligence	Ad hoc use; staff guidance issued.	Register of uses; approvals and output checking; risk classified.	AI governance routine; bias testing and oversight embedded; horizon scanning.
Digital safeguarding	Rules on images and consent followed.	Tools assessed before use; database protected and access controlled.	Digital safeguarding integral to all technology decisions; reviewed and assured.

Table 9. Technology governance maturity model.

Annex M. Board technology dashboard

The small set of measures reported to the Board at least twice a year. These are measures, not targets presented as results; where a measure is weak, it is shown plainly so the Board can act.

Measure	What it shows
Security awareness training	Share of staff and volunteers whose training is current.

Data protection registration	Whether registration with the Personal Data Protection Office is current and the annual report filed.
Impact assessments	Whether new activities involving personal data have a completed assessment.
Incidents	Number and type of incidents in the period, and how each was handled.
Backups	Whether backups are current and have been tested by restoring.
Artificial intelligence uses	Number of approved uses, any new high risk uses, and any AI incidents.
Open actions	Outstanding actions from the last compliance review, with owners and dates.
Maturity position	Current position on the maturity model and movement since last review.

Table 10. Board technology dashboard.

Annex N. Annual compliance review tool

Completed once a year by management and shared with the Board. It checks the policy against reality and produces a short, owned action list.

1. Is each part of this policy actually being followed? Note where practice and policy differ.
2. Are the legal citations in Annex A still current? Reconfirm status and dates, and update any that have changed.
3. Are the standards in Annex B still the right benchmarks?
4. Were all incidents in the year recorded, handled and learned from?
5. Is data protection registration current and the annual report filed?
6. Is the artificial intelligence register complete and accurate, with approvals and reviews up to date?
7. What is KTN's position on the maturity model, and what are the priorities for the year ahead?
8. Produce a short action list with named owners and dates, and report it to the Board.

KARAMOJA TUMAINI NETWORK

SHIELDING PASTORALIST CHILDREN · BUILDING FUTURES · LEADING CHANGE

Behind every number is a child with a name.

The systems KTN uses hold the names of children who were trafficked, abused or lost. This policy governs how they are used, and what must never be typed into them, however useful the answer might seem.

Karamoja Tumaini Network

Hope · Heal · Empower

info@karamojatumaini.org · www.karamojatumaini.org

IT AND AI USE POLICY · VERSION 1.0 · EFFECTIVE APRIL 2026