Policy Summary

Data Protection and Cybersecurity Policy

Adopted June 2025

POLICY PURPOSE

As an organization working with highly vulnerable populations, FAITH recognizes that improper handling of data could expose participants to physical, social, or legal risks — so this policy ensures the security, confidentiality, integrity, and responsible use of all data FAITH collects, stores, or processes.

6	**4**	**Annual**	**June 2025**
Core data protection principles	Nepal laws and regulations complied with	Policy review cycle	Policy adopted

About this Policy

This policy guides FAITH to protect personal and sensitive data from misuse or unauthorized disclosure, define staff responsibilities for secure data handling, maintain trust with the communities FAITH serves, and comply with national and international data protection standards.

Scope

- Personnel — all FAITH employees, volunteers, consultants, interns, and partners who handle data.
- Data types — all personal, health, financial, and other sensitive information collected, stored, or processed.
- Platforms — digital tools (databases, cloud platforms, apps, devices) and physical storage (files, registers).
- Operations — all projects, advocacy work, research, training, and ICT-driven programs.

Key Definitions

- **Personal Data —** any information that can identify an individual, directly or indirectly.
- **Sensitive Data —** information that could harm an individual if disclosed, requiring extra protection.
- **Data Breach —** any accidental or deliberate exposure, theft, alteration, or loss of data.
- **Data Controller —** FAITH, as the organization responsible for determining the purposes and means of data processing.
- **Data Processor —** any third party or individual handling data on FAITH's behalf.

Core Principles

Principle	What it Means
Lawfulness, Fairness & Transparency	Data is collected and processed only for legitimate program objectives, with full disclosure to participants.
Data Minimization	Only data strictly necessary for the stated purpose is collected, to reduce risk exposure.
Accuracy	Data is regularly checked and updated to ensure reliability; errors are corrected promptly.
Storage Limitation	Data is retained only as long as required, then securely deleted or anonymized.

Principle	What it Means
Integrity & Confidentiality	Data is protected against unauthorized access, modification, or destruction.
Accountability	Decisions and processes around data collection, storage, and sharing are documented, and compliance is ensured.

Data Collection, Consent, and Sharing

- **Approval —** all data collection activities must be approved by FAITH management.
- **Informed Consent —** participants must understand the purpose, method, storage, sharing, and risks of data collection, communicated in clear, local-language, low-literacy-adapted terms.
- **Extra Care for Vulnerable Populations —** additional safeguards and guardian consent apply when collecting data from children, women at risk, sex workers, or persons with disabilities.
- **Sharing with Third Parties —** only with FAITH management authorization, a signed confidentiality agreement, and, where possible, anonymized or pseudonymized data, with all sharing activity logged.

Data Storage, Security, and Cybersecurity

Digital data is encrypted, stored on secure servers or trusted cloud platforms, and accessed only via role-based permissions, with regular automated backups. Physical records are kept in locked, access-logged cabinets. FAITH maintains cybersecurity through regular system updates, strong authentication (including multi-factor authentication for critical systems), staff training on phishing awareness, encryption of sensitive communications, and periodic security audits.

Data Breach Response

Any suspected breach must be reported immediately to the Data Protection Officer (DPO), who investigates, contains, and remediates it. Affected individuals are notified if their sensitive data is at risk, and a record of the breach, response actions, and lessons learned is maintained.

Staff Responsibilities

- Complete mandatory data protection and cybersecurity training.
- Report lost devices, suspicious emails, or security issues promptly.
- Follow FAITH's data protection guidelines; violations may lead to disciplinary action.
- Avoid using personal devices for sensitive data unless approved and secured.

Governance

Role	Responsibility
Data Protection Officer (DPO)	Oversees compliance, trains staff, responds to breaches, and ensures ethical handling of data.
IT Officer	Ensures technical security, monitors system vulnerabilities, and implements cybersecurity measures.
Project Managers	Ensure project-level adherence to the policy, including digital data collection, storage, and reporting.
Executive Leadership	Approves policies, allocates resources, and ensures organizational accountability.

Compliance and Review

FAITH adheres to Nepal's Individual Privacy Act (2018), Electronic Transactions Act (2008), Computer and Information Technology Crime Control Act (2009), the National Penal Code, Cyber Security By-law/Regulations, and international guidelines on privacy and human rights. This policy is reviewed annually, or sooner if there are significant changes in technology, regulations, or FAITH's operations, with compliance audits reported to senior management.