Moving Mountains Data Protection & Privacy Policy

1. Purpose and Scope

This policy ensures Moving Mountains Trust manages personal data legally, securely, and transparently. It sets strict requirements for collecting, storing, and transferring personal data within the UK and internationally between our charity and direct-implementation NGO partners in Kenya and Nepal.

This policy applies to all personal data handled by trustees, staff, volunteers, and overseas partners, regardless of whether it is stored digitally or in paper formats.

2. Legal and Regulatory Framework

The charity operates in compliance with international data standards and the following legal structures:

- **United Kingdom:** The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.
- **Kenya:** The Data Protection Act 2019 (regulated by the Office of the Data Protection Commissioner - ODPC).
- **Nepal:** The Individual Privacy Act 2018 (2075).

3. Data Protection Principles

All personal data processed by the charity must be handled according to these core rules:

- **Lawfulness & Transparency:** Collected only with clear, legal justification and informed consent.
- **Purpose Limitation:** Used strictly for the specific reason it was collected (e.g., donor tracking, project reporting).
- **Data Minimization:** Only collecting the absolute minimum amount of information required.
- **Accuracy:** Kept up to date and corrected promptly when errors are identified.
- **Storage Limitation:** Erased or completely anonymized once it is no longer needed.
- **Security & Confidentiality:** Locked and protected against unauthorized access, loss, or theft.

4. International Data Transfers (UK to Kenya & Nepal)

4.1 Legal Bases for Cross-Border Sharing

Because Kenya and Nepal sit outside the UK's standard GDPR adequacy zone, personal data (such as names, addresses, or photos of beneficiaries or donors) cannot be transferred freely without protection. We enforce security using two mechanisms:

- **Standard Contractual Clauses (SCCs):** Data-sharing agreements built directly into our Memorandums of Understanding (MoUs) with partners in Kenya and Nepal.
- **Explicit Consent:** Explicit, written approval from the individual before any of their data crosses international borders.

4.2 Restricting Beneficiary Data

To maximize security for overseas project participants:

- **Anonymization:** If requested, partner NGOs in Kenya and Nepal must strip out identifying details (real names, exact home locations) from case studies, project logs, and financial receipts before emailing them to the UK.
- **Pseudonyms:** If requested, real names must be replaced with unique ID codes (e.g., Beneficiary KE-01) for standard monitoring and tracking spreadsheets.

5. Data Security and Access Controls

5.1 Digital Security Measures

- **Cloud Storage:** All charity files, financial documents, and partner reports must be kept on secure, encrypted cloud platforms (e.g. password-protected Microsoft 365 or Google Workspace accounts).
- **Device Encryption:** Any laptop, tablet, or smartphone used to access charity emails or files must be password-protected or use biometric locks.
- **Account Controls:** Staff must use complex passwords and activate **Two-Factor Authentication (2FA)** across all banking, Wise, Ulster Bank, CAF, email, and cloud accounts.
- **Public Wi-Fi:** Staff travelling in Kenya or Nepal are strictly prohibited from accessing charity data via unencrypted public Wi-Fi networks unless using a secure Virtual Private Network (VPN).

5.2 Physical Data Security

- Physical papers containing personal details (background checks, volunteer applications, written consent forms) must be stored in locked filing cabinets at the charity's registered Northern Ireland office.
- Paper records must never be left unattended during international travel.

6. Data Retention and Destruction

- **Financial Records:** Gift Aid claims, Ulster Bank logs, and Wise transfer files will be kept for **7 years** to meet HMRC and CCNI audit requirements.
- **Safeguarding Vetting:** Background certificates must be securely destroyed within **6 months** of checking, though a permanent record of the check date and outcome will be logged.
- **Secure Destruction:** Digital files must be permanently purged from hard drives and cloud trash folders. Paper documents must be cross-cut shredded.

7. Individual Data Rights

Under UK law, any donor, volunteer, or beneficiary has the right to manage their personal information. They can request to:

- See exactly what information the charity holds about them (Subject Access Request).
- Fix mistakes in their data.
- Have their data completely deleted from our systems (the right to be forgotten).

The charity will fulfill all valid data requests within **30 calendar days** without charging a fee.

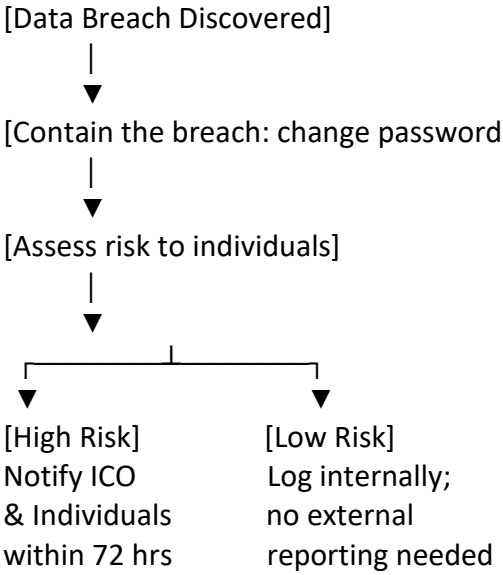
8. Data Breach Notification Procedure

8.1 Containment and Internal Reporting

- Anyone who notices a data breach (e.g., a lost work phone, a misdirected email containing partner data, or a hacked account) must notify the Data Protection Lead within **24 hours**.
- The Lead will instantly take steps to stop the breach, such as freezing accounts or erasing lost devices remotely.

8.2 External Regulatory Deadlines

- **To the ICO:** If the breach risks harming individuals (e.g., identity theft or safety exposure), the charity must report it to the UK Information Commissioner's Office (ICO) within **72 hours**.
- **To the CCNI:** Serious breaches that disrupt charity operations must also be reported to the Charity Commission for Northern Ireland via a Significant Incident Report.
- **International Partners:** If the breach involves data held by partners in Kenya or Nepal, the local partner must simultaneously notify their respective regulators.



9. Review

The Board of Trustees will review this policy every two years, or earlier if legislation, CCNI guidance or the charity's activities change.