Data Protection Policy

The Mountain Training Trust (MTT) & Mountain Training Limited (MTL)

Document Control

Owner	**Head of Governance**
Approver	Audit, Risk & Finance Committee (ARF)
Version	2.1 (2026)
Operational date	19/03/2026
Review cycle	Annual or on material change
Applies to	MTT, MTL and Plas y Brenin (managed by MTT)
Scope	Trustees, employees, volunteers, contractors, and any other person processing personal data on behalf of MTT, MTL and Plas y Brenin.
Data mediums	Paper records; emails; databases; cloud systems; portable devices; CCTV; audio/visual recordings; messaging platforms; and any other electronic or physical storage medium.

Change History

Version	Date	Summary of changes	Author	Approver
2.0	**Jan 2026**	Full modern rewrite; merged data transfer & encryption.	Head of Governance	Not applicable – draft for review
2.1	**Feb 2026**	Minor amendments following reviewer feedback; clarified descriptions (lawful bases, training, processor register, ROPA notes); removed internal comment threads; no material policy changes.	Head of Governance	ARF Committee

1. Key Points

- MTT is the Data Controller. Plas y Brenin (PyB) is MTT's operating name. MTL, as MTT's wholly owned subsidiary, is in scope when it processes personal data on behalf of, or jointly with, MTT/PyB.
- The Board of Trustees retains overall accountability for data protection compliance.
- We follow the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 principles: lawfulness, fairness, transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity/confidentiality; accountability.
- Our main lawful bases for processing are contract, legitimate interests, legal obligation, consent (where appropriate), and vital interests (for emergencies).
- Sensitive (special category) data is minimised. Medical and emergency details for off-site safety are carried only when necessary and are securely shredded on return the same day.

- Retention is kept to the minimum necessary (see table). Incident/safeguarding records are retained for longer due to risk and insurance needs.
- All incidents or rights requests go to the single mailbox: **governance@pyb.co.uk**
- Third-party processors act only on our instructions under Article 28 contracts. We keep a processor register.
- International transfers occur only with appropriate safeguards (e.g., UK adequacy, International Data Transfer Agreement (IDTA), UK Addendum) and a Transfer Risk Assessment where required.
- Training is mandatory at induction, with annual refreshers for roles that handle personal data. High-risk roles receive additional role-specific training.
- This policy is reviewed at least annually and overseen via the ARF Committee as part of governance and risk management.

2. Who we are & scope

The Mountain Training Trust (MTT) manages Plas y Brenin (the National Outdoor Centre) on behalf of Sport England. For data protection purposes, MTT is the legal entity and Data Controller; Plas y Brenin (PyB) is MTT's operating name for delivery of training, courses, and events. Mountain Training Limited (MTL) is a wholly owned trading subsidiary. This policy applies when MTL processes personal data on behalf of, or jointly with, MTT/PyB. It applies to all personal data handled in any format (digital, paper, audio/visual) by staff, freelance instructors, contractors, and board members.

3. Data protection principles (UK GDPR)

- Lawfulness, fairness, transparency: We process data lawfully and in ways people would expect, using clear privacy information.
- Purpose limitation: We collect data for specific, legitimate purposes and do not use it for incompatible purposes.
- Data minimisation: We only collect what we need and keep access to a minimum.
- Accuracy: We keep data accurate and up to date where required.
- Storage limitation: We keep data only as long as necessary and then dispose of it securely.
- Integrity & confidentiality: We protect data with appropriate technical and organisational measures.
- Accountability: We can evidence our compliance (policies, Record of Processing Activities (ROPA), Data Protection Impact Assessment (DPIA), training, audits).

4. Roles & responsibilities

Role	Summary responsibilities
Data Controller: MTT (includes PyB operating name; MTL in scope as subsidiary)	Sets policy; ensures lawful bases, minimisation, security, and retention; approves processors and international transfers; oversees compliance and risk.

Data Protection Lead (DPL): Head of Governance	Advises on UK GDPR/DPA; maintains ROPA and DPIAs; manages Subject Access Requests (SARs); coordinates incidents/breaches and Information Commissioner's Office (ICO) liaison; maintains the single mailbox; reports to senior leadership and ARF (as agreed).
Leadership Team / Heads of / Senior Instructors	Embed controls in operations (access, training, secure systems, retention); complete DPIAs where needed; escalate incidents without delay.
Employees, freelance instructors, contractors, board members	Handle data only as authorised; use approved systems; complete training; report suspected incidents immediately to the DPL mailbox.

5. Lawful bases we use (with examples)

- Contract: deliver courses/accommodation a person has booked; administer employment contracts.
- Legitimate interests: routine Centre operations, safety management, donor stewardship, B2B communications (subject to PECR for electronic marketing). We complete and document Legitimate Interests Assessments (LIAs) where required.
- Legal obligation: HMRC recordkeeping, safeguarding duties, H&S, employment law.
- Consent: email marketing to individuals, non-essential cookies, parental/guardian permissions (e.g., photography). Can be withdrawn.
- Vital interests: emergency situations to protect life or prevent serious harm, especially off-site.

6. Data we process

- Participants & clients (incl. under-18s): contact details, booking details, medical and emergency contact information, participation history, relevant consents.
- Parents/guardians and group organisers: contact details, relationship details, relevant consents.
- Employees and contractors (incl. freelance instructors): HR, payroll, training/qualification, safeguarding records.
- Supporters, donors, newsletter subscribers: contact details, preferences, donation/engagement history (if applicable).
- Visitors and website users: operational data needed for services; cookies/analytics per our Cookie Notice.
- Payment card information: MTT/PyB does not process or store payment card details. All card payments are handled directly and securely by our payment providers, and we only receive transaction confirmations, not full card details.

7. Equality, Diversity & Inclusion (EDI) data

We may invite people to share limited EDI information to understand participation patterns and remove barriers. It is always optional ("prefer not to say" available). EDI data is not used for operational decisions about individuals. Wherever practicable, it is kept separate from core records and anonymised/aggregated as early as possible for statistics and reporting. Any temporary identifiable processing is strictly access-controlled and reviewed for necessity and proportionality. Where special category data is processed, we rely on an appropriate Article 9 condition and document this within our ROPA.

8. Transparency & privacy information

We provide clear privacy information at the point of data collection and maintain an up-to-date Privacy Policy and Cookie Notice on the Plas y Brenin website, naming The Mountain Training Trust (MTT) as the Data Controller. Individuals can exercise their UK GDPR rights (access, rectification, erasure, restriction, portability, objection, and rights related to automated decisions). Requests should be sent to: **governance@pyb.co.uk** We will respond within one month (extendable by up to two months for complex requests).

9. Data minimisation & retention

We keep personal data only as long as necessary for its purpose, then dispose of it securely.
Retention periods apply to both paper and electronic records unless stated otherwise.
Retention periods may be extended where required for litigation, insurance claims, safeguarding investigations, or regulatory enquiries.

Key periods:

Record type	**Retention**
Course participant records (adults)	6 years after final activity
Under-18 participant records	Until age 21 (18 + 3 years)
Medical & emergency contact info (routine)	Held for duration of activity only; shredded same day on return
Medical/incident-related information	For incident/H&S period (see below)
Incident/accident/near-miss reports	10 years
Safeguarding/child-protection records	25 years, or until the child turns 30 (whichever is later)
Employee HR files	6 years after employment ends
Staff training/qualifications/competence	6 years after employment ends
Payroll records	6 years
Pension records	12 years
Financial records (incl. Gift Aid)	6 years (HMRC)
CCTV footage (if used)	30 days unless required for investigation

Suppression list entries (opt-out records) are retained indefinitely to ensure we do not send prohibited marketing communications.

10. Security – technical & organisational measures

- Access control & least privilege; Multi Factor Authentication (MFA) for remote/cloud access.
- Device security: full-disk encryption for laptops; Mobile Device Management for mobiles; timely patching/updates.
- Use Microsoft 365 (SharePoint/OneDrive) for secure storage and controlled access; avoid local/personal storage.

  All data stored in Microsoft 365 benefits from Microsoft's built-in encryption at rest and in transit.
- Logging/monitoring and secure configuration; staff awareness (incl. phishing).
- Secure disposal of paper and media (secure bins, certified shredding).
- Personal devices: only permitted where explicitly approved and configured to organisational standards (e.g., Mobile Device Management (MDM) enrolment, MFA, and encryption).

11. Secure data transfer & off-site emergency information

- Prefer sharing via approved M365 platforms with permissions, not email attachments.
- If sending outside our domain, encrypt attachments and share passwords separately. Do not include sensitive data in subject/body.
- Avoid removable media. If unavoidable, use AES-256 encrypted devices and remove data after transfer.
- Use secure portals/SFTP where provided (e.g., insurer/regulator).
- Post: address to a named recipient and use tracked delivery for sensitive/confidential items.

Off-site emergency information (instructors): carry only the minimum necessary, in a waterproof wallet under direct control; do not duplicate, photograph, or store on personal devices; return and shred on the same day. Loss or unauthorised access must be treated as a suspected personal data breach.

12. Working with processors & external providers

- All processors operate under Article 28 contracts and act only on our documented instructions.
- All supplier contracts involving personal data must include data security requirements; confidentiality obligations; incident reporting within agreed timeframes; restrictions on sub-processing; and controls on international transfers.
- Contracts are reviewed before signature by the DPL or Head of Governance to ensure adequacy.
- New suppliers that may access personal data must not be engaged without prior approval from the Data Protection Lead or Head of Governance.
- Proportionate due diligence is carried out before appointment. This may include reviewing security controls, data protection policies, certifications (e.g., Cyber Essentials, ISO 27001), incident history, and subcontracting/hosting arrangements.
- Higher risk suppliers (e.g., those handling special category data or providing core IT systems) may require enhanced checks and documented assurance.

- Supplier assurance is ongoing. Key suppliers are reviewed periodically; higher risk processors are reviewed at least annually. Reviews may include updated security information, certification checks, and assessment of any significant changes.
- Any concerns about a supplier's security or compliance must be escalated to the Data Protection Lead without delay. MTT/MTL may suspend or terminate processing where risks cannot be mitigated.
- A Data Processor Register is maintained and includes each processor's role, data processed, security assurances and contract status.
- Staff must not use unapproved systems, software, apps, or storage platforms ("shadow IT"). Any new tools or platforms must be approved before use.

13. International transfers

We transfer personal data outside the UK only where a lawful transfer mechanism is in place (e.g., UK adequacy regulations, ICO IDTA or the UK Addendum to EU Standard Contractual Clauses). Where required, we complete a Transfer Risk Assessment (TRA). All such transfers require DPL approval.

14. Data Protection Impact Assessment (DPIA) & Record of Processing Activities (ROPA)

We complete DPIAs for new or changed processing that is likely to result in high risk (e.g., large-scale special category data, new systems, or technologies). We maintain ROPAs that document purposes, lawful bases, categories of data/subjects, recipients, international transfers, and retention periods. We apply data protection by design and by default principles when introducing new systems or services.

15. Breach management

All suspected or actual personal data breaches must be reported immediately to the DPL mailbox. Notifiable breaches are reported to the ICO within 72 hours where required. Where a breach poses a high risk to individuals, we inform affected individuals without undue delay. Steps and roles are set out in the Data Breach Procedure. All breaches, whether notifiable or not, are recorded in the Data Breach Log which will include a risk assessment and outcome for each incident.

16. Training & awareness

All staff receive induction training. Induction training includes core cyber-security practices for all staff, including those with low-access accounts.

Refresher training frequency is determined proportionately based on role risk and data access level. Annual refreshers are prioritised for roles that access personal data or present higher risk (e.g., customer service, bookings, HR, and finance). Operational roles such as housekeeping, bar, and catering receive induction training and periodic awareness updates but do not require annual refreshers unless their access changes.

17. Review, audit & assurance

This policy is reviewed at least annually, or sooner on material change. Compliance is monitored through internal assurance (audits, incident reviews, training completion). Key measures may be reported to the ARF Committee as part of governance and risk management.

18. Glossary

Key Terms

- **GDPR (General Data Protection Regulation)** – UK data protection law (applied in the UK as the "UK GDPR").
- **DPIA (Data Protection Impact Assessment):** A required risk assessment for new or changed processing that may pose high risk.
- **ROPA (Record of Processing Activities):** A record describing what personal data we process, why, and how long for.
- **SAR (Subject Access Request):** A request from an individual asking for access to their personal data.
- **Lawful Bases:** The legal grounds we rely on to process personal data (e.g., contract, legitimate interests).
- **Special Category Data:** Sensitive data needing extra protection (e.g., health, ethnicity).
- **ICO (Information Commissioner's Office):** The UK regulator for data protection.
- **MDM (Mobile Device Management)**: A system that applies security settings to mobile devices (e.g., enforcing encryption, screen lock, and remote wipe).
- **MFA (Multi-Factor Authentication)**: A login method that requires an extra verification step (e.g., an app code), adding protection beyond a password.
- **IDTA (International Data Transfer Agreement):** A legal contract for transferring personal data outside the UK.
- **Processor:** A third party that processes personal data on our instructions only.