Data Breach Procedure

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

Document Control

Owner	**Head of Governance**
Approver	Audit, Risk & Finance Committee (ARF)
Version	1.1 (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
1.0	**Jan 2026**	Initial draft prepared and circulated to selected Board and Committee members, and to our IT provider, for review. Not approved.	Head of Governance	Not applicable – draft
1.1	**Feb 2026**	Minor amendments following reviewer feedback; clarified reporting routes (including IT escalation), improved alignment with Data Breach Register/related documents; removed internal comment threads. No material changes to breach workflow or responsibilities.	Head of Governance	ARF Committee

1. Purpose

This procedure explains what to do when personal data is lost, accessed, disclosed, altered, or destroyed accidentally or unlawfully. It ensures quick action, legal compliance, and the protection of individuals.

2. What counts as a personal data breach?

- Lost, stolen, or misplaced.

- Sent to the wrong person.
- Accessed without permission.
- Altered or deleted without authorisation.
- Exposed via malware, phishing, or system failure.
- Physical documents left unsecured.
- Emergency/off-site information not returned or shredded.

3. Immediate actions within the first 24 hours

(all employees, freelance instructors, contractors, board members, and relevant third-party processors such as IT or payroll providers)

- Stop further loss if possible (e.g., recall email, secure documents, changing passwords, lock but do not delete user or system accounts).
- Ensure any log files are secured and can not be modified or deleted
- Report immediately to: **governance@pyb.co.uk**
- Provide what happened, what data is involved including the type of data (e.g., financial, health, safeguarding, etc.) who may be affected, whether the data was encrypted or otherwise protected and your contact number.
- Do not investigate yourself, delete evidence, or contact external parties.
- If the incident involves IT systems, devices, accounts, or email, also notify the IT Service Desk immediately so they can support containment.

4. Triage & assessment (Data Protection Lead)

The DPL logs the incident and assesses type of breach, sensitivity, volume, affected individuals, risk level, recoverability, the potential harm that may be caused and whether the breach is ongoing. Technical support may be requested from external IT providers.

5. Containment & mitigation

- Reset passwords or disable accounts.
- Recall emails or request deletion by unintended recipients.
- Restore or secure files.
- Secure physical records.
- Remotely disable or lock devices where possible. Remote wipe may be used only if the risk of not wiping is higher; the rationale must be documented.

For off-site activities: treat any lost emergency information as high risk and confirm what was carried and who may be affected.

6. Assessing whether we must notify the ICO

The DPL determines whether the breach is likely to result in a risk to individuals' rights and freedoms. If so, the breach must be reported to the ICO within 72 hours. Factors include

sensitivity, likelihood of harm, vulnerability (e.g., under-18s), volume and whether data is in untrusted hands.

7. Informing affected individuals

If the breach poses a high risk, individuals are informed without undue delay. Notifications explain what happened, what data was involved, possible consequences, what we are doing, any steps that they can take to protect themselves and how they can contact the DPL.

8. Recording & documentation

All breaches, reportable or not, are recorded in the Data Breach Register, including details of the incident, the root cause, affected data, risk assessment, actions taken, ICO notifications, technical or procedural improvements to prevent recurrence and other learning points.

9. Lessons learned & follow-up

The DPL reviews causes, updates controls and processes, and arranges refresher training where necessary. Significant incidents may be shared with the ARF Committee.

10. Roles & responsibilities

All employees, freelance instructors, contractors, and board members: report breaches immediately and follow instructions.

Data Protection Lead: leads investigations, logs breaches, handles ICO and individual notifications, coordinates technical support and maintains the breach register.

Leadership Team/Heads of/Senior Instructors: support containment, ensure compliance and review processes after incidents.

External IT provider: supports technical investigation and containment.

11. Related documents

- Data Protection Policy v2.1.
- Data Processor Register.
    - Includes details of IT, payroll, and other third-party processors, including links to their relevant privacy and security policies
- Records of Processing Activities (ROPA).
- Data Breach Register.

12. Review

This procedure is reviewed annually or after any significant breach or change in legal requirements.

13. Glossary

Key Terms

- **DPL (Data Protection Lead):** The person responsible for assessing breaches, coordinating investigations, notifying the ICO and affected individuals, and maintaining the breach register.
- **ICO (Information Commissioner's Office):** The UK regulator for data protection, which must be notified of certain personal data breaches within 72 hours.
- **ROPA (Record of Processing Activities):** A record that outlines the categories of data we process, purposes, recipients, and retention; referenced as a related document in this procedure.
- **Processor:** A third party that processes personal data on our documented instructions (e.g., outsourced IT or payroll providers).
- **MTT (The Mountain Training Trust):** The data controller and responsible organisation.
- **MTL (Mountain Training Limited):** The wholly owned subsidiary included in the scope of this procedure.