



EDVENTURES | POLICY SUITE

## Data Security Procedure

|                              |                                                                  |
|------------------------------|------------------------------------------------------------------|
| <b>Document reference</b>    | EDV-POL-018                                                      |
| <b>Legal entity</b>          | EJFVENTURES LTD (company number 16938508), trading as Edventures |
| <b>Version</b>               | 1.0 — harmonised edition                                         |
| <b>Policy owner</b>          | Edward Fairnington, Owner and Responsible Manager                |
| <b>Approved by</b>           | Edward Fairnington                                               |
| <b>Approval date</b>         | 16 October 2026                                                  |
| <b>Effective date</b>        | 16 October 2026                                                  |
| <b>Next scheduled review</b> | 16 October 2027                                                  |
| <b>Review frequency</b>      | Annually, or earlier following significant change or incident    |
| <b>Approval signature</b>    | _____                                                            |

## 1. Purpose

Edventures is committed to protecting personal information against unauthorised access, accidental loss, alteration, disclosure, destruction and misuse.

This procedure establishes the organisational and technical controls used to protect personal information throughout its lifecycle, from collection and storage to authorised sharing, retention and secure disposal.

Edventures applies security measures proportionate to the sensitivity of the information, the risks involved and the nature of its activities.

## 2. Scope

This procedure applies to all personal data processed by Edventures in connection with:

- Youth climbing clubs and other activities involving children and young people.
- Adult wellbeing experiences and outdoor activities.
- Participant bookings, attendance, medical information and emergency contacts.
- Safeguarding concerns, incidents and accident records.
- Staff, freelance instructors, contractors and business administration.
- Activities delivered at hired school premises, climbing centres and other venues.
- Websites, booking systems, email, cloud storage, computers and mobile devices.

Edventures remains responsible for protecting information it controls when operating at hired venues.

Hiring school facilities does not automatically entitle the school or venue provider to access Edventures participant, medical or safeguarding records.

## 3. Responsibilities

### 3.1 Owner and Privacy Lead

Edward Fairnington, as Edventures' designated Privacy Lead, is responsible for:

- Maintaining oversight of data security.
- Approving systems, devices and storage locations.
- Authorising, reviewing and removing access permissions.
- Maintaining the Data Security and Systems Register.
- Assessing security incidents and potential personal data breaches.
- Determining when notification to the Information Commissioner's Office (ICO), affected individuals or relevant partners is required.
- Reviewing arrangements with external service providers.
- Ensuring appropriate records of security decisions are retained.

Where Edventures appoints additional workers or delegates responsibilities, the Privacy Lead retains overall oversight.

### 3.2 Workers and contractors

All individuals handling Edventures information must:

- Access only information necessary for their authorised duties.
- Protect account credentials and devices.
- Use approved communication and storage systems.
- Avoid discussing confidential information with unauthorised individuals.
- Report suspected data loss, disclosure or compromise immediately.
- Return or securely remove Edventures information when their role ends.

Freelance instructors must not retain participant information after their authorised operational need has ended.

## 4. Approved systems and information inventory

Edventures maintains a Data Security and Systems Register identifying:

- Approved applications, services and devices.
- Types of information held.
- System owners and authorised users.

- Authentication and access controls.
- Storage locations and relevant processors.
- Backup and recovery arrangements.
- Applicable retention and deletion requirements.

New systems must be reviewed and approved by the Privacy Lead before being used to process personal data.

Particular consideration must be given to systems containing children's information, medical details, safeguarding records and other sensitive personal data.

## 5. Access control and authentication

Access is granted on a least-privilege basis. Workers receive only the information necessary to perform their duties.

Edventures requires:

1. Individual user accounts wherever the system supports them.
2. Unique, strong passwords, preferably generated and stored using an approved password manager.
3. Multi-factor authentication (MFA) on email, cloud storage, booking and administrative systems wherever supported.
4. Immediate reporting of suspected credential compromise.
5. Prompt removal or modification of access when duties change or engagement ends.
6. Access permission reviews at least every six months.

Shared accounts are avoided. Where unavoidable, their use must be justified, controlled and documented.

Safeguarding records and sensitive medical information must have additional access restrictions appropriate to their confidentiality.

## 6. Devices and personal device use

Edventures information may be accessed using approved business devices or approved personal devices where appropriate security controls are in place.

Approved devices must:

- Use a secure screen lock and appropriate authentication.
- Run supported operating systems with security updates enabled.
- Use device encryption where supported.
- Be protected against unauthorised access.
- Not be shared with other individuals while Edventures information is accessible.
- Be reported immediately if lost, stolen or compromised.

Personal devices may only be used where authorised by the Privacy Lead.

Sensitive participant information must not be downloaded or stored locally on personal devices unless there is a documented operational need and appropriate protection.

Where offline access is essential for an activity, the minimum necessary information must be securely stored, protected during delivery and deleted when no longer needed.

## 7. Secure storage and backups

Personal information must be stored only within systems approved by Edventures.

Edventures will:

- Prefer approved cloud services with appropriate security and recovery arrangements.
- Avoid unnecessary duplication of records.
- Restrict access to confidential information.
- Use encryption and secure transfer mechanisms where appropriate.
- Maintain a documented backup and recovery arrangement for essential business records.
- Verify backup and recovery arrangements at least annually.

The Privacy Lead must record the actual backup arrangements for each system in the Systems Register, including whether backups are provider-managed or separately maintained by Edventures.

A successful recovery test or documented provider assurance must be recorded. Backup arrangements must not be assumed merely because a service uses cloud storage.

## 8. Information sharing and communication

Personal information may only be shared where there is a legitimate, lawful and documented reason.

Approved secure methods must be used, such as restricted-access cloud sharing, suitably protected email or an approved booking platform.

Before sharing, workers must:

- Verify the recipient.
- Confirm the purpose and lawful authority for sharing.
- Share only the minimum necessary information.
- Apply appropriate access and confidentiality restrictions.
- Record significant or sensitive disclosures.

Safeguarding information may be shared with relevant statutory agencies where necessary to protect a child or adult at risk. Consent is not always required or appropriate for such sharing.

Information must not be shared with a hired venue simply because Edventures uses its facilities.

Where information sharing is necessary for safety, safeguarding or a contractual obligation, the purpose and extent must be documented.

## 9. Data retention and secure disposal

Edventures follows its approved Data Retention Schedule, which sets out retention periods for each category of information.

The Privacy Lead reviews retention arrangements at least annually.

Information reaching the end of its retention period must be securely deleted, destroyed or anonymised, unless a documented legal or operational reason requires continued retention.

Secure disposal includes:

- Deleting information from active systems and synchronised locations where appropriate.
- Applying appropriate deletion or expiry controls to backups.
- Shredding confidential paper records.
- Securely erasing or disposing of retired devices.
- Removing access to records no longer needed by workers.

Safeguarding records, accident records and other information subject to legal retention requirements must not be destroyed prematurely.

Deletion must be suspended where records are required for an investigation, complaint, legal claim or regulatory process.

## 10. External service providers

Edventures reviews external providers that process personal data on its behalf.

Where required, a suitable written data processing agreement must be in place.

Reviews consider:

- Nature and sensitivity of the information processed.
- Security measures and access arrangements.
- Data hosting and international transfers.
- Subprocessors and relevant contractual protections.
- Breach notification arrangements.
- Data return and deletion at the end of the service.

Provider reviews are completed before introducing a relevant new service and periodically thereafter, proportionate to risk.

## 11. Data breaches and security incidents

A security incident may include:

- Sending participant information to the wrong recipient.
- Losing a device containing personal data.
- Unauthorised access to an account or record.
- Accidental deletion or alteration of information.
- Disclosure of confidential medical or safeguarding information.
- Ransomware, malware or suspected account compromise.

All suspected incidents must be reported immediately to Edward Fairnington, Privacy Lead, at [info@ed-ventures.co.uk](mailto:info@ed-ventures.co.uk), or directly by telephone where urgent.

The Privacy Lead must:

1. Take immediate steps to contain the incident and protect affected people.
2. Record when Edventures became aware of the suspected breach.
3. Establish what information and individuals may be affected.
4. Assess the likelihood and severity of risks to individuals' rights and freedoms.
5. Determine whether notification to the ICO is required.
6. Notify affected individuals without undue delay where the breach is likely to result in a high risk to their rights and freedoms, subject to applicable legal exceptions.
7. Notify relevant processors, insurers, venues or safeguarding agencies where necessary.
8. Record the investigation, decisions and corrective actions.

Where a personal data breach is notifiable to the ICO, notification must normally be made within 72 hours of becoming aware of the breach, where feasible. If later, the reasons for delay must be explained.

Not every security incident is a reportable personal data breach. Edventures must nevertheless document personal data breaches, including those not notified to the ICO, and the reasoning behind its decisions.

Security incidents involving safeguarding information must also be handled under the Safeguarding Policy.

## 12. Security awareness and competence

All workers handling personal information receive an appropriate briefing covering:

- Confidentiality and access restrictions.
- Password and device security.
- Secure handling of participant records.
- Recognising suspicious communications.
- Reporting incidents and suspected breaches.

- Secure deletion and return of information.

The Privacy Lead records completed briefings and any relevant externally obtained data protection qualifications or courses.

These briefings concern information security only. They do not constitute instructor training or replace relevant National Governing Body qualifications.

Edventures does not provide in-house instructor qualification training.

## 13. Monitoring and review

The Privacy Lead conducts:

| Activity                            | Minimum frequency                   |
|-------------------------------------|-------------------------------------|
| Access permissions review           | Every 6 months                      |
| Systems and devices register review | Every 6 months                      |
| Data retention review               | Annually                            |
| Backup and recovery review          | Annually                            |
| Processor and supplier review       | Annually, proportionate to risk     |
| Full procedure review               | Annually                            |
| Security incident review            | Following each significant incident |

Findings, corrective actions, responsible persons and completion dates must be recorded.

The procedure will also be reviewed following a significant system change, material data breach or relevant change in legal requirements.

## 14. Related documents

This procedure should be read alongside:

- Edventures Privacy Policy.
- Data Retention Schedule.

- Data Processing and Lawful Basis Register.
- Edventures Safeguarding Policy.
- Edventures Incident and Accident Reporting Procedure.
- Edventures Photography and Image Consent Procedure.
- Data Security and Systems Register.
- Data Breach and Security Incident Report Form.
- Data Access and Permissions Review Checklist.
- Staff Data Security and Confidentiality Declaration.

## 15. Approval and sign-off

Approved by                      Edward Fairnington, Owner

Signature                        *Original signed*

Date                                16 October 2026

Next scheduled review        16 October 2027

**Controlled supporting-document cross-reference (2026 consolidation)**

EDV-REG-DS-01 is the authoritative system and communication approval register, superseding EDV-REG-OS-01.

This note identifies the current supporting document without altering the substantive policy duties or replacing required operational approvals.