



EDVENTURES | POLICY SUITE

Online Safety and Digital Communications Policy

Document reference	EDV-POL-006
Legal entity	EJFVENTURES LTD (company number 16938508), trading as Edventures
Version	1.0 — harmonised edition
Policy owner	Edward Fairnington, Owner and Responsible Manager
Approved by	Edward Fairnington
Approval date	16 October 2026
Effective date	16 October 2026
Next scheduled review	16 October 2027
Review frequency	Annually, or earlier following significant change or incident
Approval signature	_____

1. Policy Statement

Edventures is committed to providing a safe, respectful and responsible digital environment for everyone involved in its activities.

The organisation recognises that online safety is an important part of safeguarding children, young people and adults, and that inappropriate use of technology can create risks relating to privacy, exploitation, harassment, personal information and professional boundaries.

This policy establishes clear expectations for digital communication, online conduct, social media, photography, information security and the management of online safeguarding concerns.

Edventures will take reasonable and proportionate steps to prevent online harm, promote professional conduct and ensure that concerns are identified, reported and addressed appropriately.

All individuals acting on behalf of Edventures must comply with this policy.

2. Purpose

The purpose of this policy is to:

- Protect children, young people and adults from online harm.
- Establish professional boundaries for digital communication.

- Prevent inappropriate or unauthorised contact with participants.
- Protect personal and sensitive information.
- Regulate the use of photography, video and social media.
- Ensure online safeguarding concerns are recognised and appropriately reported.
- Establish responsibilities for approved digital systems and devices.
- Support compliance with applicable safeguarding and data protection legislation.
- Ensure that digital technology used during activities is appropriately assessed and supervised.

Online safety arrangements will be proportionate to the nature of Edventures activities, the age and needs of participants and the level of digital interaction involved.

3. Scope

This policy applies to all activities organised or delivered by Edventures, including:

- Children's and young people's climbing clubs.
- Adult wellbeing experiences.
- Outdoor education and adventure activities.
- Activities delivered at hired schools, climbing centres or other venues.
- Communications connected with bookings, participation and administration.
- Marketing, social media and website activity.
- Digital record-keeping and information sharing.
- Use of digital devices or online content during sessions.

Edventures independently manages its participant communications, safeguarding arrangements and information security.

Where Edventures hires a school or another venue, the venue's digital systems, network restrictions and online safety requirements will apply where those systems are used or where compliance is required by the hire agreement.

Hiring school facilities does not automatically make Edventures subject to the school's internal communication systems or transfer responsibility for Edventures participant information to the school.

The relevant responsibilities must be established through the venue hire agreement and associated arrangements.

4. Roles and Responsibilities

4.1 Owner and Designated Safeguarding Lead

Edward Fairnington, Owner of Edventures, acts as the Designated Safeguarding Lead (DSL).

The DSL has overall responsibility for:

- Maintaining and reviewing online safeguarding arrangements.
- Assessing risks associated with digital activities.
- Receiving and responding to online safeguarding concerns.
- Ensuring appropriate referrals to external safeguarding agencies.
- Maintaining secure safeguarding records.
- Reviewing incidents and identifying necessary improvements.
- Ensuring workers understand professional communication boundaries.
- Keeping safeguarding knowledge current through appropriate external learning and professional development.

The DSL must ensure that safeguarding concerns are addressed promptly and that safeguarding decisions are documented.

Where the DSL is unavailable, staff must follow the alternative reporting arrangements in Section 10.

4.2 Privacy Lead

Edward Fairnington also acts as the Edventures Privacy Lead.

The Privacy Lead is responsible for:

- Overseeing data protection arrangements.
- Maintaining the Data Security Procedure.
- Authorising digital systems and managing access permissions.
- Reviewing the handling and retention of personal information.
- Receiving and assessing suspected data breaches.
- Determining whether incidents require notification to external authorities.
- Maintaining appropriate records of information security incidents.
- Reviewing third-party systems and data processing arrangements.

The Privacy Lead is an operational responsibility and does not constitute a formal appointment as a Data Protection Officer.

Edventures will review whether a statutory Data Protection Officer appointment is required if its data processing activities change.

4.3 Session Leaders and Instructors

Session leaders and instructors must:

- Follow Edventures-approved communication procedures.
- Maintain professional boundaries with participants.
- Supervise the use of digital technology during activities.
- Report inappropriate online contact or safeguarding concerns.
- Protect information accessed during their duties.
- Use only authorised systems and communication channels.
- Obtain appropriate authorisation before capturing or sharing participant images.

- Follow incident reporting and safeguarding procedures.

Session leaders must not introduce new digital systems or online activities involving participants without appropriate authorisation.

4.4 All Workers

All employees, freelance instructors, contractors and volunteers must comply with this policy.

Everyone has a responsibility to report online safety concerns and suspected information security incidents promptly.

Workers must not attempt to investigate serious safeguarding concerns independently.

5. Approved Digital Communication Channels

Edventures will communicate with participants, parents, carers and partner organisations through authorised professional systems.

The following categories of communication channels are approved, subject to confirmation and recording in the Approved Digital Systems and Communications Register:

- Official Edventures business email accounts.
- The official Edventures website: <https://ed-ventures.co.uk>.
- The authorised booking and registration platform.
- Official Edventures Facebook and Instagram accounts for public information, marketing and initial enquiries.
- Other communication platforms specifically approved by the Owner following an appropriate safeguarding and information security review.

Email and the approved booking platform will be the preferred methods for formal participant communications.

Social media direct messaging may be used for routine initial enquiries but must not be used for private or ongoing personal communication with children or young people.

Staff must not use personal email accounts, personal social media profiles or unauthorised messaging applications for Edventures participant communications.

Additional communication systems may only be introduced with the Owner's approval.

The Approved Digital Systems and Communications Register will identify each system, its purpose, authorised users, relevant controls and review arrangements.

6. Communication with Children and Young People

All communications involving participants under 18 must maintain clear professional boundaries.

Routine communications concerning bookings, participation, attendance, payment, session arrangements and collection must normally be directed through an authorised parent or carer.

Where an organisation makes a group booking, communications may be directed through its authorised group organiser for matters relating to that booking.

This does not remove the need to communicate with parents or carers directly where required for safeguarding, consent or emergency arrangements.

Staff must not:

- Initiate personal or private digital relationships with children or young people.
- Add or follow participants through personal social media accounts for purposes connected with Edventures.
- Communicate using disappearing-message functions or secret accounts.
- Share personal contact details without appropriate authorisation and justification.
- Send messages of a personal, inappropriate or unrelated nature.
- Arrange meetings or activities privately outside authorised Edventures arrangements.
- Use digital communications to intimidate, discriminate against, harass or exploit participants.

Where an operational reason makes direct communication with an older young person necessary, the DSL must authorise the arrangement following an appropriate safeguarding assessment.

Such communication must take place through an approved channel, have a clearly defined purpose and be appropriately recorded and transparent.

If a young person contacts a worker directly, the worker must respond professionally, avoid unnecessary private engagement and redirect routine arrangements through the authorised parent or carer wherever appropriate.

A safeguarding disclosure received through digital communication must be managed under the safeguarding procedure and must not be ignored merely because it arrived through an unapproved channel.

7. Professional Conduct and Online Boundaries

Workers must maintain the same standards of professional behaviour online as they do during face-to-face activities.

Communications must be respectful, appropriate, relevant to Edventures activities and capable of appropriate organisational oversight.

Workers must not:

- Publish offensive, discriminatory or inappropriate material in connection with Edventures.
- Disclose confidential information concerning participants or colleagues.
- Share images or information obtained through their work for personal purposes.

- Make unauthorised public statements on behalf of Edventures.
- Discuss identifiable safeguarding incidents on social media.
- Use online platforms to establish inappropriate relationships with participants.
- Encourage participants to contact them through personal accounts.

Any inappropriate digital contact, personal boundary concern or suspected abuse must be reported to the DSL.

Where the concern involves the DSL, the alternative safeguarding reporting procedure must be followed.

8. Photography, Video and Social Media

Edventures recognises that photography and video can support marketing, communication and the recording of activities.

However, identifiable images of participants constitute personal information and must be handled appropriately.

8.1 Permissions and Consent

Before capturing or using identifiable images, Edventures must establish the purpose, appropriate lawful basis and any required consent.

Where consent is relied upon, it must be freely given, specific, informed and capable of withdrawal.

For children, Edventures must obtain appropriate permission from a person with parental responsibility where required, taking account of the child's age, understanding and rights.

Participation in an Edventures activity does not automatically constitute consent for photographs or video to be used.

The absence of marketing consent must not disadvantage a participant's ability to take part.

8.2 Taking Photographs and Videos

Only authorised workers may take photographs or recordings on behalf of Edventures.

Workers must:

- Check the relevant permissions before taking images.
- Respect participants who do not wish to be photographed.
- Consider any safeguarding restrictions.
- Use approved devices and storage arrangements.
- Avoid capturing unnecessary personal or sensitive information.
- Ensure recording does not compromise supervision or activity safety.

Personal devices must not be used to capture participant images unless a specific, documented exception has been approved, with secure storage and deletion arrangements established.

8.3 Publishing Images

Before publication, Edventures must check the intended audience, platform and permissions.

Images must not be published where this could create an identifiable safeguarding risk.

Edventures will avoid unnecessarily combining participant images with full names, school information, precise location details, personal circumstances or routine attendance information.

The publication of live location information or detailed timetables identifying children's whereabouts must be avoided unless specifically justified and safeguarded.

Only authorised individuals may publish material through official Edventures accounts.

8.4 Withdrawal of Consent

Where consent is withdrawn, Edventures will stop the relevant future use and remove affected material from systems and channels under its control where required.

Edventures will explain that material already copied or independently shared by third parties may not be fully recoverable.

Consent and withdrawal decisions must be documented in the Photography and Media Consent Record.

8.5 Photography by Participants and Parents

Participants and parents or carers may be permitted to take photographs during activities where it is safe and consistent with venue arrangements.

They must be encouraged to respect other participants' privacy and avoid publishing identifiable images of others without appropriate permission.

Session leaders may restrict photography where it creates a safety risk or safeguarding concern.

9. Digital Devices and Online Activities

Digital technology may be used as part of Edventures activities where it supports learning, participation or operational requirements.

Before introducing digital equipment or online content, the session leader must assess relevant risks.

Considerations include:

- Participant age and understanding.
- Accessibility and additional needs.
- Suitability of the material.
- Supervision arrangements.
- Opportunities for inappropriate contact.
- Personal information collected or disclosed.
- Exposure to harmful or inappropriate material.
- Location sharing or tracking.
- Device security.
- Venue rules and network restrictions.

Participants must not be required to create personal social media accounts to access ordinary Edventures activities.

Where Edventures uses a hired venue's internet connection, the session leader must establish the applicable rules and available filtering arrangements.

Edventures must not assume that a venue's filtering or monitoring arrangements automatically provide sufficient protection for its activities.

Workers must ensure that personal device use does not compromise supervision or safety-critical instruction.

Any inappropriate content, online contact or device-related incident must be managed promptly.

10. Reporting Online Safeguarding Concerns

Online safeguarding concerns may include:

- Cyberbullying or online harassment.
- Grooming or inappropriate adult contact.
- Sexual exploitation or coercion.
- Threats or intimidation.
- Sharing of intimate or abusive images.
- Exposure to harmful content.
- Unauthorised disclosure of personal information.
- Online behaviour indicating a risk of abuse or neglect.

All concerns must be taken seriously.

10.1 Immediate Response

Where an online safeguarding concern arises, workers must:

1. Assess immediate safety and call 999 where someone is in immediate danger.
2. Protect the participant from further harm where reasonably practicable.
3. Listen calmly and avoid unnecessary or leading questions.

4. Avoid making promises of secrecy.
5. Report the matter to the DSL promptly.
6. Record the information factually using the Edventures safeguarding reporting arrangements.
7. Follow any instructions concerning external safeguarding referrals.

Workers must not conduct their own detailed investigation or confront a suspected perpetrator.

10.2 Preserving Evidence

Relevant evidence must be preserved appropriately and securely.

Workers must record identifying information such as dates, times, usernames, relevant URLs, messages or disclosures where lawful and safe.

Where child sexual abuse material is suspected, workers must not download, reproduce, forward or circulate the material.

Police or appropriate safeguarding advice must be sought about handling or preserving evidence.

10.3 External Referrals

The DSL will determine the appropriate safeguarding response in accordance with the Edventures Safeguarding and Child Protection Policy.

Where a child is at risk of significant harm, a referral must be made to the relevant local authority children's social care service or police as appropriate.

Workers may make a direct referral if necessary and must not delay safeguarding action because the DSL is unavailable.

10.4 Concerns Involving the DSL or Owner

Where a concern involves Edward Fairnington, workers must not be required to report it to him.

An allegation concerning an adult working with children that meets, or may meet, the applicable LADO criteria must be referred to the relevant Local Authority Designated Officer without delay and within one working day.

For activities within Bath and North East Somerset:

Local Authority Designated Officer (LADO)

Telephone: 01225 396810

Email: LADO@bathnes.gov.uk

For activities outside Bath and North East Somerset, the relevant local authority's LADO contact details must be identified in the activity or venue safeguarding information.

The LADO procedure applies to relevant allegations about adults working with children. It is not the routine referral route for every concern about a child's welfare.

Where the DSL is unavailable, workers must contact the appropriate safeguarding agency directly when necessary.

Edventures must ensure suitable arrangements for competent safeguarding support and decision-making during activities when the DSL is unavailable.

10.5 Adults at Risk

Where online concerns involve an adult with care and support needs who may be experiencing abuse or neglect and may be unable to protect themselves because of those needs, the DSL will consider the relevant local authority adult safeguarding referral route.

Adults' wishes, capacity, confidentiality and the legal basis for information sharing must be considered.

Where a person faces immediate danger, emergency services must be contacted.

10.6 Recording and Confidentiality

Safeguarding concerns must be recorded securely and separately from routine participant records, in accordance with the Edventures Safeguarding and Child Protection Policy.

Information must be shared only with those who have a legitimate need to know, subject to appropriate safeguarding and legal obligations.

Records must include the concern, relevant dates, actions taken, referrals made, decisions and reasons.

11. Data Protection and Information Security

Edventures will process personal information in accordance with the UK GDPR, Data Protection Act 2018 and other applicable requirements.

The organisation recognises its responsibility to protect participant, parent, carer and worker information.

11.1 Data Security

Edventures maintains a separate Data Security Procedure which establishes operational controls for:

- Approved systems and devices.
- Individual accounts and appropriate access permissions.
- Strong passwords and multi-factor authentication.

- Secure storage and transfer of information.
- Appropriate backup and recovery arrangements.
- Personal device restrictions.
- Data retention and secure deletion.
- Reporting of lost or compromised devices.
- Removal of access when workers leave or change roles.
- Reviewing relevant third-party service providers.

Workers must follow that procedure when handling Edventures information.

11.2 Access to Information

The Edventures Privacy Policy and relevant privacy notices explain how personal information is collected, used, shared and retained.

Privacy notices do not replace the operational security requirements established by this policy and the Data Security Procedure.

Workers must only access personal information necessary for their authorised responsibilities.

Safeguarding records, medical information and other sensitive records must have additional access restrictions.

Information must not be shared with hired venues unless there is an appropriate reason and lawful basis.

Hiring school premises does not automatically entitle the school to access Edventures participant booking or medical records.

11.3 Personal Data Breaches

Any suspected loss, unauthorised disclosure, misuse or compromise of personal information must be reported immediately to Edward Fairington in his capacity as Privacy Lead.

The Privacy Lead will:

1. Record the reported incident.
2. Take appropriate containment measures.
3. Identify the information and individuals affected.
4. Assess risks to individuals' rights and freedoms.
5. Determine any legal notification requirements.
6. Inform relevant organisations or individuals where required.
7. Record the outcome and corrective action.

Where a personal data breach is likely to result in a risk to individuals' rights and freedoms, Edventures must notify the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

Where a breach is likely to result in a high risk to affected individuals, those individuals must be informed without undue delay, subject to applicable legal requirements.

All personal data breaches must be documented, including decisions not to report.

11.4 Privacy Information

12. Staff Briefing and Competence

Before using Edventures communication systems or accessing participant information, workers must receive relevant instructions and policy information.

The briefing must address:

- Approved communication channels.
- Professional online boundaries.
- Safeguarding reporting procedures.
- Confidentiality.
- Appropriate photography and video use.
- Data protection and information security.
- Reporting suspected data breaches.
- Relevant venue-specific arrangements.

Workers must confirm that they have read and understood the requirements applicable to their roles.

Where a worker's role requires formal safeguarding, online safety or data protection training, it must be obtained through an appropriate external provider.

Edventures does not provide in-house instructor qualification training or assessment.

The Owner must maintain appropriate records of relevant external training, professional qualifications, policy acknowledgements and access authorisations.

13. Monitoring and Compliance

Edventures may review the use of its organisational systems and accounts where lawful, necessary and proportionate.

Any monitoring must have a legitimate purpose, be appropriately communicated and comply with applicable data protection requirements.

Monitoring may include reviewing organisational communication records, investigating reported misuse and auditing access permissions.

Edventures will not undertake excessive or unjustified monitoring of personal communications.

Workers must cooperate with reasonable investigations and promptly disclose relevant incidents.

14. Breaches of Policy

A suspected breach of this policy will be assessed according to its nature, severity and potential impact.

Possible responses include:

- Corrective instruction or clarification.
- Additional external learning or professional development.
- Restriction or withdrawal of system access.
- Review of professional duties or supervision.
- Disciplinary action where applicable.
- Termination of contractual arrangements where justified.
- Referral to safeguarding agencies, police or other relevant authorities.

Where appropriate, Edventures will consider whether a referral to the Disclosure and Barring Service or a relevant professional body is required.

Any response must be proportionate and documented.

Safeguarding concerns and potential criminal matters must be handled through the appropriate external procedures rather than solely as an internal policy breach.

15. Record-Keeping

Edventures will maintain records appropriate to its digital communication and online safety arrangements.

These include:

- An Approved Digital Systems and Communications Register.
- Records of authorised users and system access reviews.
- Photography and media permissions.
- Online safety incident records.
- Safeguarding concerns and external referrals.
- Personal data breach records.
- Relevant staff policy acknowledgements.
- Applicable external training records.
- Policy review and revision records.

Records will be stored securely with appropriate access restrictions.

Retention periods will follow the Edventures records retention schedule and applicable legal requirements.

16. Policy Review and Continuous Improvement

This policy will be reviewed at least annually by the Owner.

An earlier review will take place where necessary following:

- A serious safeguarding or online safety incident.
- A significant personal data breach.
- A change in applicable legislation or statutory guidance.
- The introduction of new digital systems.
- A significant change in the nature of Edventures activities.
- Identification of a material weakness in existing procedures.

Reviews will consider incident findings, staff feedback, technological developments, safeguarding guidance and relevant changes to operating arrangements.

Changes will be recorded in the policy register and communicated to relevant workers.

17. Related Legislation and Guidance

This policy should be read alongside applicable legislation and guidance, including:

- Children Act 1989 and Children Act 2004.
- Safeguarding Vulnerable Groups Act 2006.
- Data Protection Act 2018 and UK GDPR.
- Online Safety Act 2023, where relevant to the services and activities concerned.
- Current *Working Together to Safeguard Children* statutory guidance.
- Relevant local safeguarding partnership procedures.
- Information Commissioner's Office guidance on information security and personal data breaches.

Edventures will monitor changes relevant to its operations and update this policy where necessary.

18. Document Control and Approval

Item	Details
Policy title	Online Safety and Digital Communications Policy
Policy reference	EDV-POL-006
Version	1.0
Organisation	Edventures
Policy owner	Edward Fairnington
Designated Safeguarding Lead	Edward Fairnington
Privacy Lead	Edward Fairnington
Approval date	16 October 2026
Effective date	16 October 2026

Next review date	16 October 2027
Review frequency	Annually, or earlier where required

Approval Declaration

I confirm that this policy has been reviewed and approved for implementation within Edventures.

I accept responsibility for ensuring that appropriate resources, procedures, staff instructions and safeguarding arrangements are established to support its effective operation.

Name: Edward Fairnington

Position: Owner, Edventures

Signature: *Original signed*

Date: 16 October 2026

End of Policy