

TRAINING CAVE



Policy Title	Online Safety (E-safety)
Version	2.0
Effective Date	27.01.26
Current Issues/ Review Date	24.09.2026
Next Review Date	24.09.2027
Approved By	Jack Sunderland Director Training Cave Club Ltd

1. Purpose

Training Cave Club Ltd will protect children and young people from online harm while helping them use technology safely, responsibly and purposefully. Online safety is part of safeguarding, not a separate technical issue. It includes conduct on Training Cave systems and relevant activity on personal devices, social media, messaging, gaming, livestreaming and artificial intelligence services where this affects a learner's safety or the organisation's work.

This policy explains the controls expected when digital technology is used, the conduct required of personnel and learners, and the response to an online concern. It must be read with the Child Protection and Safeguarding Policy.

2. Organisational Status and Scope

Training Cave is an independent alternative provision and boxing provider. It is not a maintained school, academy, independent school or pupil referral unit. Keeping Children Safe in Education and school technology standards are therefore used as relevant safeguarding good practice and commissioner assurance, rather than described as statutory duties that automatically apply to Training Cave.

This policy applies to employees, self-employed workers, coaches, tutors, mentors, volunteers, contractors, agency staff, learners, members and visitors. It covers organisation-owned or managed equipment and accounts, internet access supplied by Training Cave, personal devices used during provision, and online conduct outside Training Cave where there is a safeguarding, professional-boundary or organisational connection.

Training Cave does not currently provide routine remote learning or off-site educational visits. Before either is introduced, the Director and DSL must approve the platform, supervision, privacy, communication and emergency arrangements.

3. Legal and Guidance Framework

This policy has regard to the following, where applicable to Training Cave's status, activities and contracts:

- Children Act 1989 and Children Act 2004 safeguarding principles;
- UK GDPR and Data Protection Act 2018;
- Computer Misuse Act 1990;
- Sexual Offences Act 2003;
- Protection from Harassment Act 1997;
- Online Safety Act 2023 and current communications offences;
- Prevent duty guidance where applicable, and proportionate safeguarding practice concerning radicalisation;
- Keeping Children Safe in Education 2026, used proportionately as relevant good practice;
- Department for Education filtering and monitoring standards, used proportionately; and

- UK Council for Internet Safety guidance on sharing nudes and semi-nudes.

4. Online Risk Model

Online risks will be considered under four connected areas. A concern may involve more than one area.

Area	Examples
Content	Pornography; violence; self-harm or suicide material; hate; extremism; misinformation; harmful health or body-image content; age-inappropriate material.
Contact	Grooming; coercion; sexual or criminal exploitation; impersonation; unwanted contact; radicalising influence; contact from unknown adults.
Conduct	Cyberbullying; harassment; discriminatory abuse; sharing personal information or sexual imagery; recording others without permission; harmful challenges; misuse of AI.
Commerce	Scams; phishing; gambling; financial exploitation; misleading advertising; in-app purchases; identity theft; blackmail or sextortion.

5 Responsibilities

5.1 Director and management

- Approve proportionate technical, procedural and supervision controls before learners use Training Cave internet access, accounts or devices;
- Ensure responsibilities are allocated between safeguarding, management and any IT support;
- Provide training, resources and an escalation route; and
- Review incidents, system limitations and whether controls remain suitable for the learner risk profile.

5.2 Designated Safeguarding Lead

The DSL has lead safeguarding responsibility for online safety. The DSL will assess concerns, coordinate support, decide on parent or carer and commissioner involvement, make or support referrals, and review relevant monitoring or incident information. Technical staff do not make safeguarding decisions in place of the DSL.

5.3 All Personnel

Personnel must follow approved communication and device arrangements, maintain professional boundaries, supervise use appropriately, model safe behaviour, protect accounts and data, and report concerns immediately. They must not investigate a safeguarding concern beyond obtaining the minimum information needed to establish immediate safety and make a report.

5.4 Learners and members

Learners and members must follow instructions and acceptable-use expectations, respect other people and their privacy, keep login details secure, avoid harmful or illegal activity, and

report anything that makes them or someone else feel unsafe. A child will not be blamed or punished merely for making a good-faith disclosure or seeking help.

6. Learner Devices and Internet Access

Training Cave Club Ltd does not provide learners with Wi-Fi, computers, tablets, user accounts or any other form of internet access.

Learners are not permitted to connect to or use Training Cave Club Ltd's staff or business network.

Where learners bring personal phones, tablets or other connected devices, any internet access is through their own mobile-data service. Training Cave Club Ltd cannot filter or monitor learners' personal mobile-data connections or the content accessed through them.

Personal-device use during sessions will be managed through clear instructions, appropriate supervision, behaviour expectations and individual risk-management arrangements where necessary.

Learners may be instructed to switch off, put away or safely store their personal devices where their use:

- Disrupts learning, coaching or physical activity
- Creates a health and safety risk
- Affects another person's privacy
- Involves inappropriate recording or photography
- Raises a behaviour or safeguarding concern

Staff will remain alert to concerning online behaviour or content that is reported or becomes visible during a session. Staff will not routinely inspect learners' personal devices, messages, accounts or browsing history.

Training Cave Club Ltd does not have the statutory search powers available to specified school staff. Staff may ask a learner to show relevant content or hand over a device voluntarily, but consent must be genuine.

If a learner refuses and there is a safety or safeguarding concern, staff may:

- Ask the learner to stop using and put away the device
- End the learner's participation in the activity safely
- Inform the Designated Safeguarding Lead
- Contact the learner's parent or carer
- Inform the referring school or commissioner
- Contact the police or emergency services where necessary

Any safeguarding concern involving a personal device or online activity will be recorded and managed under the Child Protection and Safeguarding Policy. Staff must not attempt to conduct their own investigation.

If Training Cave Club Ltd introduces learner Wi-Fi, devices, online accounts, remote learning or digital learning platforms in the future, these must not be used until appropriate safeguarding, privacy, supervision, security, filtering and monitoring arrangements have been assessed and approved.

7. Acceptable Use of Devices, Accounts and Systems

- Technology must be used only for an authorised and lawful purpose during Training Cave activity.
- Users must not access, create, store or share harmful, abusive, discriminatory, sexual or illegal material; attempt to bypass security; install unauthorised software; access another person's account; or damage systems or data.
- Passwords must not be shared. Multi-factor authentication will be used where available and appropriate for staff accounts.
- Learners may use personal phones or wearable devices only within the rules set for the session. Staff may require a device to be put away or stored safely where it affects safety, learning, privacy or safeguarding.
- Concerns involving a personal device will be managed under section 6 and the Child Protection and Safeguarding Policy.

8. Staff Conduct, Professional Boundaries and Communication

Personnel must use approved organisational channels for contact with children and parents or carers. Communication must be necessary, professional, capable of appropriate oversight and limited to suitable times. Personal social-media accounts, disappearing-message functions, secret conversations and private contact that cannot be accounted for must not be used with learners.

- Personnel must not add or follow current learners through personal social-media accounts, share personal contact details, or engage in sexualised, intimidating or over-familiar communication.
- A pre-existing family, community or boxing relationship that makes personal contact unavoidable must be declared to management and covered by a written boundary arrangement.
- One-to-one video or online contact is not permitted unless specifically approved, risk assessed and arranged so that appropriate oversight and records are maintained.
- Personnel must not use personal email or cloud storage for learner records and must not upload learner information to unapproved apps or services.
- Any accidental boundary crossing, inappropriate contact or concerning message must be reported promptly rather than deleted or concealed.

9. Images, Recordings, Livestreams and Publicity

Images, video, audio and livestreaming can create safeguarding, privacy and reputational risks. Training Cave will obtain and record the appropriate permissions

and explain the intended use. Consent for publicity is separate from images needed for safeguarding, incident evidence or another lawful operational purpose.

- Only approved equipment and accounts may be used for organisational photography or recording. Personal devices must not normally be used.
- Recording is prohibited in toilets, changing rooms and shower areas. Devices must not be used there in a way that could capture another person.
- Images will avoid unnecessary identifying information, embarrassing presentation or unsafe location details and will be stored and deleted in line with the retention arrangements.
- A learner's refusal or withdrawal of publicity consent will be respected for future use, subject to material already lawfully published and any overriding legal requirement.
- Livestreaming involving children requires prior management approval, a risk assessment, appropriate audience and interaction controls, and active supervision.

10. Social Media, Website and Public Accounts

Only authorised personnel may publish on behalf of Training Cave. Account access will be restricted, protected and removed promptly when a person's duties change. Posts, comments and direct messages will be moderated proportionately. Safeguarding disclosures received through a public account will be moved into the safeguarding process without promising confidentiality or conducting an investigation through social media.

Staff must not post confidential information, learner records, incident details, unapproved images or content that compromises professional trust. Personal expression must not reasonably suggest that a staff member speaks for Training Cave unless authorised.

11. Education and Support

Learners will receive age- and needs-appropriate guidance through discussion, direct teaching and in-the-moment support. Content will reflect SEND, SEMH, communication needs, trauma and differing levels of digital experience. It may cover privacy, consent, healthy relationships, misinformation, scams, gaming, harmful content, reporting tools, passwords, location sharing, sexual imagery, grooming, exploitation, radicalisation and help-seeking.

Safety education will not imply that a victim is responsible for abuse. Learners will be shown how to block and report contact, preserve relevant information safely and approach a trusted adult.

12. Generative Artificial Intelligence

Generative AI tools may produce inaccurate, biased, unsafe or convincing but false material and may retain information entered by users. Learner-facing use is

permitted only when the activity and tool have been approved, age restrictions are met, safeguards are suitable and a member of staff provides appropriate supervision.

- Personal, special-category, safeguarding or confidential information must not be entered into a public or unapproved AI service.
- AI output must be checked by a competent person before it is relied upon or shared. AI must not make final safeguarding, disciplinary, admission or support decisions about a person.
- Users must not create impersonations, deepfakes, sexualised images, abusive content, fraudulent messages or work intended to deceive.
- Learners must follow assessment and awarding-organisation rules and acknowledge AI assistance where required.
- Before adopting an AI tool, Training Cave will consider safeguarding, data protection, age assurance, filtering, moderation, intellectual property, accessibility and the provider's use of prompts and outputs.

13. Cyberbullying, Harassment and Harmful Behaviour

Cyberbullying, discriminatory abuse, threats, stalking, impersonation, non-consensual recording, doxxing, coercive sharing and other harmful online behaviour will be taken seriously whether they occur on or off the premises. Training Cave will assess safety, support the person affected, address harmful behaviour under the Behaviour Management and Relationships Policy and involve parents or carers, commissioners, platforms, police or other agencies as appropriate.

Restorative work will be used only when it is safe, voluntary and appropriate. It will not replace a safeguarding response or require a harmed learner to meet the person responsible.

14. Nude or Semi-nude Imagery and Sexual Online Harm

Any incident involving nude or semi-nude images, video or livestreams of a person under 18 must be reported immediately to the DSL. Staff must not view, copy, print, forward, store or save the imagery, ask a child to send or download it, or conduct a detailed interview. If imagery appears unexpectedly, the member of staff must close or turn away from it as soon as possible, record what happened without describing the image unnecessarily and report it.

Staff must not delete the imagery or instruct the child to delete it before the DSL has considered the UK Council for Internet Safety process and any police advice. The response will avoid blame or shame and will distinguish child-produced imagery from adult involvement. Suspected adult creation, possession or distribution of sexual imagery of a child is child sexual abuse and requires urgent safeguarding and police consideration.

Sexual extortion, threats to distribute imagery, coercion, grooming or immediate danger will be escalated without delay. Devices will not be searched by Training Cave staff under school powers that the organisation does not possess.

15. Grooming, Exploitation, Radicalisation and Harmful Content

Concerns about grooming, sexual or criminal exploitation, county lines, radicalisation, self-harm or suicide material, eating-disorder content, dangerous challenges or contact from unknown adults will be treated as safeguarding concerns. Staff will listen, establish immediate safety, preserve available non-illegal evidence, and report to the DSL. Emergency services will be contacted where there is an immediate risk of serious harm.

16. Reporting and response

A concern may be reported verbally or in writing to any member of staff. The receiving person must report it immediately to the DSL or deputy and make a factual record. If the concern involves the DSL, it must be reported to the alternative person identified in the Child Protection and Safeguarding Policy. Staff must not promise secrecy.

The DSL will consider the child's wishes and welfare, immediate protection, parents or carers, the referring school or commissioner, children's social care, police, Prevent arrangements, platform reporting, specialist support and data-breach requirements. Parents or carers will normally be involved unless doing so could increase risk or prejudice an investigation.

Call 999 where there is an immediate threat to life or safety. A report to a platform or removal service does not replace a safeguarding or police referral where one is required.

17. Evidence and Devices

Ordinary abusive messages, usernames, dates, URLs and account details may be preserved by screenshot or factual note where safe and lawful. Staff must not preserve illegal sexual imagery of a child by copying or screenshotting it. A device that may contain evidence will be handled as little as possible, kept secure, and passed to police or dealt with under their advice where appropriate. Staff will not impersonate a child, contact a suspected offender, or run their own digital investigation.

18. Cyber Incidents and Personal Data Breaches

Phishing, malware, compromised accounts, unauthorised access, loss of a device, accidental disclosure and other cyber incidents must be reported immediately to

management. The user should disconnect a suspected device from the network if safe, but must not erase data or attempt an unapproved repair. Passwords and access may be secured and specialist support obtained.

Where personal data may be involved, the incident will also be managed under the Data Protection Policy. Training Cave will assess risk, document the response and notify the Information Commissioner's Office and affected people where legally required. A safeguarding response will proceed alongside, not wait for, technical investigation.

19. Parents, Carers, Schools and Commissioners

Training Cave will explain relevant device, communication, image and reporting arrangements to learners and, where appropriate, parents or carers and commissioners. Significant concerns will be shared lawfully and proportionately. Information supplied by a referring school about online risk, restrictions or safety planning will be incorporated into the learner's arrangements.

20. Records, Confidentiality and Monitoring

Online-safety concerns, decisions, referrals, actions and outcomes will be recorded securely in the appropriate safeguarding, behaviour, incident or data-breach record. Access will be limited to those who need the information. Records will distinguish fact, professional opinion and information supplied by others and will be retained under Training Cave's retention arrangements.

Management will review themes such as repeated contact, cyberbullying, personal-device misuse, image incidents, harmful online behaviour and gaps in supervision. This review will focus on safety and improvement and will not involve routine surveillance of learners' personal devices or communications.

21. Training and Review

Personnel will receive online-safety and professional-boundary information at induction and updates appropriate to their role. The DSL will maintain sufficient knowledge to respond to emerging online risks. This policy and related controls will be reviewed annually and sooner after a serious incident, material legal or guidance change, a new platform or service, or evidence that controls are ineffective.

22. Related Documents and Operational Records

- Child Protection and Safeguarding Policy;
- Behaviour Management and Relationships Policy;
- Anti-Bullying Policy;
- Data Protection Policy and personal-data breach procedure;
- Staff Code of Conduct and professional boundaries arrangements;

- Equality, Diversity and Inclusion Policy;
- acceptable-use expectations and device rules;
- photography, video and publicity consent records; and
- risk assessments for any future learner internet, device, platform or remote-learning provision.

23. Contact Details

Training Cave Club Ltd
Unit 10, Carrmills Business Centre
Birstall
WF17 9JX
Email: info@trainingcave.co.uk

The current DSL and deputy contact arrangements are identified in the Child Protection and Safeguarding Policy and displayed for personnel. Online safeguarding concerns must be reported immediately through that procedure rather than sent as a routine general enquiry.