

Digital and Online Safeguarding Policy

Supporting Education Group – Qualifications & Training Practice

Issue Date:	October 2026
Next Review Date:	September 2027
Updated:	v1.0 Oct 26
Author:	Chris Garcia / Anita de Villiers
Job title of originator/author:	Director of Quality & Compliance / Head of Safeguarding

Table of Contents

Contents

Digital and Online Safeguarding Policy	1
Supporting Education Group – Qualifications & Training Practice.....	1
Purpose and Intent	3
Immediate Action and Reporting	3
Scope.....	4
Principles	4
Digital risk framework	4
Governance and responsibilities.....	5
1 Qualifications & Training Governance Board	5
2 Director of Quality & Compliance	5
3 Group DSL and safeguarding network.....	5
4 IT, digital and information governance	5
5 Managers and delivery staff	5
6 Learners	5
Safe systems, platforms and procurement.....	6
Filtering and monitoring	6
Safe online delivery and communication.....	7
1 Virtual classrooms and one-to-one sessions	7
2 Email, messaging and social media	7
3 Images, recordings and personal information.....	7
Artificial intelligence and emerging technology.....	8
	1

Prevent and harmful online influence.....	8
Reporting, response and evidence	9
1 Reportable concerns.....	9
2 Response process	9
3 Evidence handling.....	9
4 Allegations or concerns about staff.....	9
Training, communication and learner education.....	10
Quality assurance and review.....	10
Appendix A: Digital Risk Categories.....	11
Appendix B: Platform Approval Checklist.....	11
Appendix C: Key External Framework	12

Purpose and Intent

The purpose of this policy is to set a single, consistent standard for digital and online safeguarding across Supporting Education Group Qualifications and Training practice and its training providers, Best Practice Network (BPN), Eden Training Solutions and LMP Education. It protects learners, children, young people, adults at risk, employees and other stakeholders from harm arising through digital technology, online content, communications and technology-enabled behaviour.

This policy supports safe and inclusive access to learning across face-to-face, online, workplace and blended delivery. It must be read alongside the Safeguarding and Child Protection Policy, Prevent and Radicalisation Policy, data protection and information security requirements, acceptable-use arrangements, the Employees Code of Conduct and relevant incident procedures.

Where an online concern involves a child, an adult at risk, abuse, exploitation, radicalisation, an allegation about an adult working with learners, serious criminality or immediate danger, the organisation's safeguarding procedures take priority.

Immediate Action and Reporting

If you identify, witness or receive a digital or online safeguarding concern:

- ✓ If there is an immediate risk to life or serious harm, call 999 without delay.
- ✓ Do not investigate the concern yourself, confront an alleged perpetrator, delete material or delay reporting to gather further evidence.
- ✓ Listen, remain calm and do not promise confidentiality.
- ✓ Preserve relevant messages, links, usernames, dates, times and screenshots where it is safe and lawful to do so.
- ✓ Record what you saw or were told factually, using the person's own words where possible.
- ✓ Employees must report the concern immediately through MyConcern. If MyConcern is unavailable, contact the Safeguarding Hub at safeguardinghub@supportingeducation.com.
- ✓ If you believe a concern has not been acted upon appropriately, escalate it to the Practice Head of Safeguarding, an authorised senior leader or the relevant external safeguarding agency.

This policy sets a single practice-wide standard for protecting learners, staff and other users from harm arising through digital technology, online content, communications and technology-enabled behaviour. It supports safe access to learning while recognising that no technical control can remove all risk.

The policy covers safeguarding, conduct, operational and technical controls. It must be read with the organisation's wider safeguarding framework. Where a concern involves a child, an adult at risk, radicalisation, exploitation, abuse, a staff allegation or an immediate threat, safeguarding procedures take priority.

Where statutory guidance applies directly to a particular provider or programme, that provider must comply with it. Across the wider Qualifications & Training Practice, the same expectations are adopted

as an organisational safeguarding standard unless a documented reason requires a different approach.

Scope

This policy applies to all employees, workers, associates, tutors, trainers, assessors, coaches, volunteers, governors, contractors, agency staff and learners across Best Practice Network, Eden Training Solutions and LMP Education. It applies whenever organisational work, learning, communication, systems or data are involved, including personal devices used for work.

- ✓ Learning platforms, virtual classrooms, video calls and recorded sessions.
- ✓ Email, messaging, discussion boards, social media and online communities.
- ✓ Organisation-owned, managed, loaned and bring-your-own devices.
- ✓ Websites, cloud services, applications, plug-ins and third-party tools.
- ✓ Artificial intelligence, automated decision support, chatbots, synthetic media and content-generation tools.
- ✓ Online assessments, e-portfolios, remote invigilation and evidence capture.
- ✓ Workplace, home, centre-based, blended and subcontracted delivery.

Principles

- ✓ Safeguarding is everyone's responsibility and concerns must be acted on promptly.
- ✓ The welfare and best interests of the child or adult at risk take priority.
- ✓ Online and offline harm are connected and must not be treated as separate issues.
- ✓ Controls must be proportionate to the learner group, delivery model, device ownership and known risks.
- ✓ Privacy and data protection support safe practice but do not prevent necessary safeguarding information sharing.
- ✓ Learners should be enabled to participate safely, not excluded from learning through unnecessarily restrictive controls.
- ✓ Decisions should be recorded, explainable, regularly reviewed and open to professional challenge.

Digital risk framework

The Practice will assess online safety through four connected areas. Risks may overlap and may occur on or away from organisational systems.

Governance and responsibilities

1 Qualifications & Training Advisory Board

- ✓ Approves this policy and receives assurance on implementation.
- ✓ Reviews significant incidents, trends, control weaknesses and lessons learned.
- ✓ Seeks assurance that filtering, monitoring, platform approval, staff training and learner education are effective and proportionate.
- ✓ Holds senior leaders to account for resourcing, risk treatment and timely improvement.

2 Director of Quality & Compliance

- ✓ Owns the policy and ensures alignment across the Practice.
- ✓ Escalates material risk to governance and relevant senior leaders.
- ✓ Ensures policy, audit and assurance activity is coordinated with safeguarding, quality, data protection, IT and operational teams.

3 Group DSL and safeguarding network

- ✓ Lead the safeguarding response to online concerns and ensure appropriate referral or advice.
- ✓ Maintain awareness of current online risks, local pathways and Prevent arrangements.
- ✓ Work with IT, data protection and delivery teams to ensure safeguarding needs inform technical and operational decisions.
- ✓ Provide professional challenge where controls or responses are insufficient.

4 IT, digital and information governance

- ✓ Maintain secure systems, identity controls, logging, patching and proportionate access restrictions.
- ✓ Support filtering and monitoring arrangements and ensure alerts reach named, trained reviewers.
- ✓ Preserve technical evidence and support incident containment without compromising safeguarding decisions.
- ✓ Assess suppliers, data flows, integrations and changes before deployment.
- ✓ Supporting Education Group & its partners hold the accreditation Cyber Essentials.

5 Managers and delivery staff

- ✓ Model safe professional behaviour and set clear expectations.
- ✓ Use only approved systems and communication routes.
- ✓ Carry out proportionate checks before online sessions and respond to warning signs.
- ✓ Report concerns immediately and do not conduct their own safeguarding investigation.

6 Learners

- ✓ Use systems responsibly and follow acceptable-use expectations.

- ✓ Protect login details and personal information.
- ✓ Report harmful content, contact or behaviour and seek help when needed.
- ✓ Respect others, professional boundaries, copyright and assessment rules.

Safe systems, platforms and procurement

No new platform, application, browser extension or AI tool may be introduced for delivery or learner communication without proportionate approval. Approval must consider safeguarding, privacy, security, accessibility, age suitability, contractual controls, data location, moderation, recording, deletion and exit arrangements.

- ✓ A named business owner and clear purpose.
- ✓ A completed risk assessment proportionate to the tool and users.
- ✓ Supplier due diligence, including terms, privacy information and incident notification.
- ✓ Minimum necessary access, role-based permissions and multi-factor authentication where available.
- ✓ Controls for guest access, recording, chat, file sharing, external links and user-generated content.
- ✓ Accessible alternatives for learners who cannot safely or reasonably use the standard tool.
- ✓ A review date and process to withdraw access when no longer required.

Filtering and monitoring

Filtering is preventative and restricts access to illegal, inappropriate or harmful content. Monitoring is reactive and identifies potentially harmful activity for review. The Practice will apply each control according to the systems it manages, the age and vulnerability of learners, device ownership, delivery location and the extent of technical control available.

- ✓ Assign named strategic, safeguarding and technical responsibilities.
- ✓ Maintain documented filtering and monitoring arrangements for managed networks and devices.
- ✓ Test that controls work and do not create unreasonable barriers to education, accessibility or protected characteristics.
- ✓ Review arrangements at least annually and whenever there is a significant systems change, incident or emerging risk.
- ✓ Ensure alerts are reviewed by trained staff within defined timescales and escalated through safeguarding procedures where appropriate.
- ✓ Inform users clearly and lawfully about monitoring.
- ✓ Record limitations where learning takes place on employer, home or personally owned networks and use alternative controls, education and supervision.
- ✓ Consider AI-generated text, images, audio and video when reviewing filtering and monitoring capability.

Filtering and monitoring must not be treated as a substitute for professional supervision, safe curriculum design, learner education, staff vigilance or a prompt safeguarding response.

Safe online delivery and communication

1 Virtual classrooms and one-to-one sessions

- ✓ Use an approved organisational account and platform.
- ✓ Check participant identity, privacy settings, waiting-room controls and intended attendees.
- ✓ Use professional backgrounds and remove sensitive personal information from view.
- ✓ Set expectations for chat, cameras, microphones, recordings, screen sharing and conduct.
- ✓ Avoid personal contact details and off-platform communication.
- ✓ For children and vulnerable learners, apply programme-specific arrangements for parental, employer or setting involvement where required.
- ✓ Record only where there is a clear, approved purpose. Inform participants, control access and apply the agreed retention period.
- ✓ Report concerning behaviour, disclosures, unexplained third-party presence or unsafe home circumstances through safeguarding procedures.

2 Email, messaging and social media

- ✓ Keep communication necessary, professional, transparent and capable of organisational oversight.
- ✓ Do not use disappearing-message features for learner contact.
- ✓ Do not accept or initiate personal social-media connections with learners where this could compromise professional boundaries.
- ✓ Do not share confidential learner information in group chats or informal channels.
- ✓ Use group communications carefully, disclose recipients only where appropriate and establish moderation rules.
- ✓ Do not respond publicly to a safeguarding allegation or incident. Preserve evidence and escalate.

3 Images, recordings and personal information

- ✓ Obtain and record an appropriate lawful basis and any required consent before capturing or publishing images or recordings.
- ✓ Do not use personal devices to retain learner images or safeguarding evidence beyond the minimum necessary transfer process.
- ✓ Remove metadata, location details or identifying information where these are not needed.
- ✓ Consider whether apparently harmless content could reveal routines, locations, vulnerabilities or protected information.

Artificial intelligence and emerging technology

Artificial intelligence can support accessibility, administration and learning, but can also enable impersonation, harmful content, unreliable advice, bias, surveillance and the rapid creation or alteration of images, audio and video. AI use must remain human-led and must not weaken safeguarding accountability.

- ✓ Use only approved AI products for organisational work involving learners or organisational information.
- ✓ Do not enter safeguarding records, special-category data, confidential material or identifiable learner information into public AI tools unless the use has been formally approved.
- ✓ Treat AI output as unverified. A competent person must check accuracy, bias, appropriateness and context before use.
- ✓ Do not use AI to make a final safeguarding, disciplinary, admissions or support decision without meaningful human review.
- ✓ Report synthetic or manipulated media used for bullying, impersonation, coercion, fraud or reputational harm.
- ✓ Explain acceptable AI use to learners and distinguish support from substitution, deception or assessment misconduct.
- ✓ Review AI tools for age suitability, content controls, training-data use, retention, model changes and the ability to delete data.

Prevent and harmful online influence

Online spaces can expose individuals to extremist narratives, grievance-based communities, conspiracy material, propaganda and contact from those seeking to influence or exploit them. There is no single profile or indicator of susceptibility to radicalisation. Concerns must be considered in context and managed through safeguarding procedures.

- ✓ Staff must complete required Prevent training and understand the internal referral route.
- ✓ Concerns may include changes in language or behaviour, fixation on harmful material, attempts to access or share terrorist content, escalating isolation, expressions of support for terrorism or contact with concerning networks. No single factor is conclusive.
- ✓ Staff must not debate, investigate or attempt to deradicalise a learner themselves.
- ✓ The DSL will assess the available information, seek advice where needed and decide whether support, monitoring, a Prevent referral, Channel consideration or another safeguarding response is appropriate.
- ✓ Legitimate debate, lawful belief, political expression and protected speech must not be confused automatically with vulnerability to radicalisation.

Reporting, response and evidence

1 Reportable concerns

- ✓ Online abuse, bullying, harassment or discriminatory conduct.
- ✓ Grooming, exploitation, coercion, stalking, blackmail or unwanted contact.
- ✓ Radicalisation or terrorism-related concern.
- ✓ Self-harm, suicide-related or dangerous challenge content.
- ✓ Impersonation, deepfakes, manipulated media or non-consensual recording.
- ✓ Disclosure of abuse through an online channel.
- ✓ Unsafe professional boundaries or a concern about an adult working with learners.
- ✓ Significant data or cyber incidents where safeguarding may be affected.
- ✓ A failure in filtering, monitoring, access control or platform moderation that exposes users to harm.

2 Response process

- ✓ Make the situation safe without increasing risk. Call 999 where there is immediate danger.
- ✓ Preserve available evidence. Avoid forwarding harmful material unnecessarily.
- ✓ Record the concern in MyConcern on the same working day, using factual language and the person's own words.
- ✓ Notify the DSL through the required route. A data or cyber incident must also be reported through the relevant incident process.
- ✓ The DSL assesses risk, immediate support, information sharing, external referral, parental or employer involvement and any need for a strategy discussion.
- ✓ Relevant leaders coordinate containment, platform action, communications and recovery without compromising safeguarding or criminal enquiries.
- ✓ Actions, decisions, rationale and outcomes are recorded. The case remains under review until safe to close.

3 Evidence handling

Staff should preserve URLs, account names, dates, times and a brief description of what was seen. They should avoid repeatedly viewing, copying or distributing harmful material. Illegal material must not be downloaded or stored outside an approved law-enforcement or organisational process. Advice must be obtained from the DSL and, where relevant, IT, data protection or the police.

4 Allegations or concerns about staff

Any concern about the conduct of an employee, worker, volunteer, contractor or associate must be reported through the safeguarding allegations or low-level concerns procedure. The person raising the concern must not investigate, alert the subject of the concern or attempt to resolve it informally.

Training, communication and learner education

- ✓ Induction and refresher training will cover online risks, reporting, professional boundaries, safe use of platforms, data handling, Prevent and the organisation's acceptable-use expectations.
- ✓ DSLs and relevant IT, digital and data protection staff will receive role-specific development.
- ✓ Learner education will be age and context appropriate and cover privacy, misinformation, scams, respectful behaviour, consent, reporting, AI, harmful content and help-seeking.
- ✓ Employers and delivery partners will be told how to report concerns and what the Practice expects where learning uses their systems or premises.
- ✓ Training and communications will be reviewed in response to incidents, audits, learner voice, technology changes and emerging risk.

Quality assurance and review

The Director of Quality & Compliance, Group DSL and relevant operational and technical leads will maintain a coordinated assurance cycle. Findings will be reported to the Qualifications & Training Governance Board and tracked to completion.

- ✓ Annual review of this policy and associated acceptable-use arrangements.
- ✓ Annual documented review of filtering and monitoring, and additional review after significant change or incident.
- ✓ Sampling of safeguarding records involving online harm to test timeliness, decision quality and closure.
- ✓ Platform and supplier review, including high-risk AI and communication tools.
- ✓ Training completion, knowledge checks and targeted follow-up.
- ✓ Learner, staff and employer feedback on safety, accessibility and confidence to report.
- ✓ Trend analysis covering incidents, alerts, recurring platforms, learner groups and control failures.
- ✓ Testing of escalation, contact and business-continuity arrangements.

This policy will be reviewed sooner where legislation or statutory guidance changes, a serious incident occurs, material weaknesses are identified, a new delivery model is introduced, or technology creates a significant new risk.

Appendix A: Digital Risk Categories

Risk area	Examples
Content	Illegal, hateful, violent, misleading, extremist, self-harm, exploitative or otherwise harmful content, including AI-generated material.
Contact	Grooming, coercion, scams, impersonation, unwanted contact, radicalising influence or unsafe contact with adults or peers.
Conduct	Bullying, harassment, sharing private information, discriminatory abuse, non-consensual recording, harmful challenges, academic misconduct or misuse of organisational systems.
Commerce and technology-enabled risk	Fraud, gambling-like features, persuasive design, phishing, data harvesting, malware, deepfakes, recommender systems and unsafe use of automated tools.

Appendix B: Platform Approval Checklist

- ✓ ☐ Business owner, purpose and intended users identified.
- ✓ ☐ Age suitability and learner vulnerability considered.
- ✓ ☐ Privacy, security, accessibility and safeguarding risks assessed.
- ✓ ☐ Data categories, location, retention, deletion and subcontractors understood.
- ✓ ☐ Roles, access, authentication, guest controls and leaver process defined.
- ✓ ☐ Chat, recording, moderation, file-sharing and external-link controls configured.
- ✓ ☐ Incident reporting and supplier notification timescales agreed.
- ✓ ☐ Alternative access arrangements available where needed.
- ✓ ☐ Training and user guidance prepared.
- ✓ ☐ Review date, success measures and exit plan recorded.

Appendix C: Key External Framework

- ✓ Keeping Children Safe in Education 2026.
- ✓ Working Together to Safeguard Children 2026.
- ✓ Prevent Duty Guidance for England and Wales.
- ✓ Department for Education filtering and monitoring core standard.
- ✓ Online Safety Act 2023.
- ✓ Data Protection Act 2018 and UK General Data Protection Regulation.

Legal and statutory references must be reviewed for relevance to each provider and delivery model. This policy is an operational safeguarding framework and is not a substitute for programme-specific legal advice.