



EDClass E-Safety, Filtering and Monitoring Policy

POL075

Issue number 3

Approved by Sam Warnes

EDClass E-Safety, Filtering and Monitoring Policy

EDClass provides a fully remote, supervised alternative education platform designed to break barriers to learning for pupils accessing education off-site, within internal alternative provision (IAP), isolation, medical pathways, or via rotated seat allocations. Operating exclusively online requires a digital safeguarding infrastructure that is secure, compliant, and continuously monitored.

This policy defines the technological, operational, and pedagogical controls deployed by EDClass to ensure:

- ✓ Compliance with the DfE Filtering and Monitoring Standards for Schools and Colleges and KCSIE 2026.
- ✓ Alignment with the Online Education Accreditation Scheme (OEAS).
- ✓ A safe digital ecosystem that mitigates the "Four Cs" of online risk: Content, Contact, Conduct, and Commerce.
- ✓ Robust, automated identification and rapid human triage of digital welfare concerns, cyberbullying, radicalisation, and acute self-harm indicators.

Statutory and Regulatory Architecture

This policy operates in strict alignment with UK law, statutory education standards, and digital safety frameworks:

- ✓ **Keeping Children Safe in Education (KCSIE 2026):** Implementing statutory duties regarding appropriate filtering and monitoring on educational digital networks, systems, and platforms.
- ✓ **DfE Meeting Digital and Technology Standards in Schools and Colleges:** Meeting all statutory baseline technical standards for filtering, monitoring, and network firewalls.
- ✓ **DfE Online Education Accreditation Scheme (OEAS):** Satisfying accreditation standards for safeguarding systems, recorded sessions, auditable interaction trails, and digital pupil well-being.
- ✓ **The Equality Act 2010:** Ensuring that filtering and monitoring policies do not discriminate against protected groups, prevent access to necessary identity-support resources (e.g., LGBTQ+ or mental health support), or compromise accessibility for learners with Special Educational Needs and Disabilities (SEND).
- ✓ **UK GDPR and Data Protection Act 2018:** Ensuring network monitoring, video recording, chat interception, and keystroke/text-scanning strictly satisfy lawful processing thresholds under substantial public interest exemptions.
- ✓ **The Prevent Duty (Counter-Terrorism and Security Act 2015):** Filtering terrorist and extremist material and monitoring ideologically motivated risk signals.

Leadership, Roles, and Governance Hierarchy

Safeguarding decisions maintain absolute operational precedence over system functionality, technical configurations, and curricular pathways.

Kim, Head of Safeguarding (Lead DSL):

- ✓ Holds ultimate operational authority over platform filtering parameters, keyword interception dictionaries, and safeguarding monitoring queues.
- ✓ Holds organisational seniority over the Head of SEND and curricular leads regarding all risk-mitigation measures and access permissions.
- ✓ Directs live incident interventions and manages formal escalations with commissioning school DSLs, Multi-Agency Safeguarding Hubs (MASH), and law enforcement.
- ✓ Conducts weekly reviews of intercepted traffic logs and leads the statutory annual filtering and monitoring review.

IT and Systems Security Lead:

- ✓ Configures, manages, and stress-tests the multi-layer DNS/web filtering appliances and platform inspection microservices.
- ✓ Ensures that real-time keyword/phrase detection systems function continuously across all chat, search, and submission inputs.
- ✓ Conducts system penetration tests, bypass attempts, and vulnerability assessments alongside third-party auditors.

Head of SEND:

- ✓ Coordinates with the Head of Safeguarding to ensure accessibility tools (e.g., screen readers, OpenDyslexic typography, text-to-speech engines) are not impeded by filtering controls.
- ✓ Analyses monitoring data to identify when neurodivergent learners display distress, cognitive overload, or communication dysregulation.

Online Teaching Staff and wellbeing staff:

- ✓ Maintain continuous live supervision during platform delivery sessions.
- ✓ Identify digital red flags, enforce professional boundaries, and log observations within the internal incident management system.

Commissioning Schools and Multi-Academy Trusts (MATs):

- ✓ Maintain statutory home-school responsibility for enrolled pupils.
- ✓ Supply complete safeguarding profile indicators during automated intake and act promptly upon receiving filtered-risk escalations from EDClass.

The Four Cs: Risk Taxonomy and Digital Safeguards

EDClass designs its digital safeguards to mitigate the four established areas of online risk:

Risk Category	Nature of Digital Threat	EDClass Technological and Procedural Safeguards
Content	Exposure to illegal, inappropriate, or harmful material (pornography, violent extremism, self-harm promotion, hate speech, gambling).	Multi-layer DNS/URL filtering, Internet Watch Foundation (IWF) dynamic blocklists, CTIRU terrorist blocklists, restricted external hyperlink architecture.
Contact	Interaction with malicious adults or peers (online grooming, CSE/CSA, sexual harassment, predatory recruitment, radicalisation).	Zero unmoderated pupil-to-pupil communication; no external messaging access; all 1:1 teacher interaction recorded and conducted within monitored boundaries.
Conduct	Pupil behaviours that cause harm (cyberbullying, sexting / youth-produced sexual imagery, digital harassment, sharing personal data, hacking).	Automated algorithmic text-scanning, real-time message interception, digital behaviour repair pathways, structured Acceptable Use Agreements.
Commerce	Financial exploitation, digital scams, online gambling, hidden advertising, microtransactions, predatory monetisation.	Complete blocking of commercial transactional gateways, zero advertisement delivery within platform, disabled third-party script tracking.

Appropriate Filtering Architecture

EDClass maintains a secure, closed digital learning environment. Rather than allowing open internet access, the platform combines a secure web gateway with strict whitelisting and dynamic content classification.

Dynamic filtering and inspection engine

- ✓ **EDClass digital platform environment:** Operates as a closed perimeter web gateway controlling all network access.
- ✓ **Dynamic filtering and inspection engine:** Inspects all traffic in real time against three mandatory protective baselines:

- ✓ Real-time blocklists intercepting Child Sexual Abuse Material (CSAM).
- ✓ Dynamic blocking of violent extremist media and terrorist domains.
- ✓ Direct prohibition and blocking of unapproved VPNs, proxies, and circumvention tools.
- ✓ **Routing decision pathways:**
 - ✓ **Unauthorised content (connection terminated):** Intercepts illegal or high-harm content, unmoderated chat/social media, pornography, gore, gambling, hate speech, and harassment. The connection is instantly terminated and an alert is dispatched to the Safeguarding Team queue.
 - ✓ **Verified educational (secure access granted):** Permits verified access to core subject pathways, DfE and exam board resources, approved mental health support services, and vetted digital research feeds. The session is logged, timestamped, and continuously monitored.

Filtering Standards and Implementation

- ✓ **Illegal Material Blocking:** The system continuously integrates real-time blocklists from the Internet Watch Foundation (IWF) to block child sexual abuse material (CSAM) and the Counter-Terrorism Internet Referral Unit (CTIRU) to prevent access to known terrorist sites.
- ✓ **Age-Appropriate Category Restrictions:** Filtering blocks access to adult content, pornography, suicide/self-harm promotion, weapons, illicit substances, gambling, and unapproved gaming platforms.
- ✓ **Prevention of Circumvention:** The platform actively blocks Virtual Private Networks (VPNs), unapproved proxy networks, anonymous search engines (e.g., Tor), bypass extensions, and alternative DNS providers.
- ✓ **Over-Blocking Mitigation:** Safeguards are calibrated to avoid "over-blocking" essential educational, pastoral, and welfare resources. Learners are not blocked from accessing legitimate mental health support, Childline helplines, or educational RSE content delivered in line with statutory guidance.

Appropriate Monitoring: Real-Time Interception and Triage

In compliance with KCSIE 2026, EDClass enforces active, continuous monitoring across all platform interactions, combining automated algorithmic text scanning with human pedagogical supervision.

Appropriate monitoring: Real-time interception and triage

- ✓ **Real-time text / input submission:** Captures all text typed across live chat, notes, assignments, interactive whiteboards, and platform search fields.
- ✓ **Automated scanning engine:** Evaluates all inputs in real time against risk-indexed libraries to assign threat levels.
 - ✓ **Triage and escalation workflows: Priority 1: acute threat (critical emergency escalation):**
 - ✓ *Triggers:* Active suicidal ideation, imminent self-harm triggers, CSAM / CSAE, sexual abuse disclosures, or immediate weapon/violence risks.

- ✓ *Actions:* Message blocked instantly; high-priority emergency alert dispatched to Kim / Lead DSL; direct phone call made to Commissioning School DSL; 999 emergency services / MASH engaged if immediate harm is present.
- ✓ **Priority 2: welfare concern (internal pastoral triage):**
 - ✓ *Triggers:* Bullying, hate speech, inappropriate language, low-level distress markers, or emerging disengagement.
 - ✓ *Actions:* Logged on the secure safeguarding portal; reviewed by a Deputy DSL within 2 hours; formally communicated in writing to Commissioning School DSL within 4 operational hours.

Automated Keyword and Sentiment Analysis

- ✓ **Algorithmic Scanning:** All text typed within live chats, collaborative whiteboards, system searches, and submitted work is processed in real time by an automated scanning engine.
- ✓ **Risk Dictionaries:** The platform maintains comprehensive, regularly updated keyword and phrase dictionaries covering:
 - ✓ Suicidal intent, self-harm methodologies, and severe mental health crises.
 - ✓ Sexual violence, child sexual exploitation (CSE), and youth-produced sexual imagery terminology.
 - ✓ Radicalisation terms, extremist symbols, and hate speech targeting protected characteristics.
 - ✓ Peer-on-peer abuse, cyberbullying, physical threats, and coercive control language.

Live Session Capture and Supervised Environments

- ✓ **Tamper-Evident Session Logging:** Every live interaction—including teacher video feeds, audio exchanges, interactive whiteboard marks, and chat dialogues—is recorded, time-stamped, and archived within encrypted UK data centres.
- ✓ **No Unmoderated Peer Access:** The platform prevents unsupervised peer-to-peer breakout rooms, unmonitored private chats, or direct file sharing between learners. All peer collaboration occurs within moderated, teacher-present environments.

Automated Onboarding, Dynamic Seat Allocation, and Policy Application

EDClass provides flexible, multi-purpose seat allocations across inclusion departments, isolation rooms, internal alternative provision (IAP), medical home-tuition, and part-time timetabling:

- ✓ **Automated Baseline Application:** When a commissioning school purchases or rotates an EDClass seat to a new pupil, the student profile is provisioned automatically without administrative delays.
- ✓ **Pre-set Safeguarding Envelopes:** From the first minute of login, the platform's filtering policies, keystroke monitoring, and alerting configurations are applied to that seat automatically based on age, key stage, and documented risk status.

- ✓ **Focus on Ongoing Reviews:** Moving away from manual onboarding meetings allows pastoral and safeguarding teams to focus their resources on continuous learner reviews, monitoring digital safety logs, and assessing attendance patterns alongside commissioning school SENDCo and DSL teams.

Incident Classification and Escalation Pathways

Incidents identified through automated filtering alerts, teacher observation, or direct learner disclosures are managed through structured response workflows:

Incident Priority	Criteria and Risk Level	Immediate Platform Action	Target Communication Window
Priority 1: Critical / Acute Harm	Imminent danger to life, active suicide attempt, acute self-harm disclosure, severe physical/sexual abuse disclosure, possession of child abuse imagery.	Content blocked; session isolated; instant emergency alert dispatched to Kim (Head of Safeguarding) and Lead DSLs.	Immediate (< 15 Minutes): Direct phone call to Commissioning School DSL. Emergency services (999) / MASH engaged if school uncontactable and pupil in immediate danger.
Priority 2: Serious Safeguarding / Welfare	Disclosures of historic abuse, domestic disturbance indicators, severe bullying, radicalisation concerns, persistent hate speech.	Incident flagged and recorded on safeguarding portal; session notes preserved; risk evaluation initiated.	Within 4 Hours: Written safeguarding notification transmitted via secure encrypted channels to Commissioning School DSL.
Priority 3: Digital Misconduct / Minor Infraction	Isolated swear words, off-topic gaming searches, low-level disruption, testing filtering parameters.	Content blocked; automated behavioural warning generated; learner redirected to behaviour repair module.	Daily Digest: Logged on daily school attendance and engagement reports; managed internally via pastoral intervention.

Acceptable Use Framework and Virtual Classroom Conduct

Access to the EDClass virtual platform is governed by clear behavioural expectations designed to protect learners and educators.

Learner Acceptable Use Rules:

- ✓ **Classroom Environment:** Learners accessing EDClass from home should log in from an appropriate, shared living space wherever possible (avoiding private bedrooms). Clothing must be suitable for a school environment.
- ✓ **Digital Decorum:** Chat functions are strictly reserved for academic instruction, teacher guidance, and constructive engagement. Verbal abuse, derogatory language, harassment, and intentional disruption are prohibited.
- ✓ **Identity and Security:** Learners must keep login credentials secure. Impersonating another learner or attempting to share access credentials results in immediate account suspension.
- ✓ **Recording Prohibition:** Learners and families must not record, take screenshots of, or publish audio/video of EDClass staff, classroom discussions, or peers to any external platform or social media service.

Staff Digital Professional Boundaries:

- ✓ **Platform Exclusivity:** Staff must never communicate with enrolled learners through personal email accounts, phone numbers, social media channels, or unapproved meeting platforms (e.g., Discord, WhatsApp, personal Teams).
- ✓ **Environment and Camera Standards:** Teachers must deliver lessons from professional environments, using approved neutral backgrounds, professional attire, and clear, monitored audio/video streams.
- ✓ **One-to-One Safeguarding Protocol:** When conducting one-to-one instructional interventions, teachers must operate strictly within monitored, logged application channels, maintaining transparency across all chats and video sessions.

Data Protection, Privacy, and Human Rights

The monitoring and filtering technologies deployed by EDClass are carefully calibrated to maintain safety while upholding data protection standards:

- ✓ **Lawful Processing Basis:** Processing monitoring telemetry, chat logs, and session recordings is lawful under UK GDPR Article 6 (1)(c) (Legal Obligation), Article 6 (1)(e) (Public Interest), and Article 9 (2)(g) alongside Schedule 1, Part 2, Paragraph 18 of the Data Protection Act 2018 (Safeguarding of Children and Individuals at Risk).
- ✓ **Data Protection Impact Assessment (DPIA):** A comprehensive DPIA covers all filtering, keystroke analysis, automated scanning, and session recording tools, assessing necessity, proportionality, and individual rights under Article 8 of the European Convention on Human Rights (ECHR).
- ✓ **Restricted Access and Audit Logs:** Safeguarding alerts, recorded sessions, and monitoring transcripts are stored in encrypted environments separate from standard

academic records. Access is restricted exclusively to authorised safeguarding personnel led by Kim (Head of Safeguarding).

- ✓ **Retention Periods:** Session recordings and safeguarding incident logs are retained in alignment with statutory educational safeguarding standards and IICSA recommendations (typically retained until the individual reaches age 25, or 26 for care-experienced learners).

Annual Assurance, Testing, and Compliance Audits

To ensure that filtering and monitoring capabilities remain effective against emerging cyber threats and online risks, EDClass conducts regular technical and governance checks:

TECHNICAL PENETRATION and BYPASS VERIFICATION: Bi-annual stress testing of web gateways, proxy evasion tools, and VPN blocking mechanisms using standardised technical frameworks.

POLICY and FILTERING AUDIT: Annual collaborative audit led jointly by Kim (Head of Safeguarding) and the IT and Systems Security Lead to review blocklists, assess over-blocking reports, and incorporate emerging online risks.

STAFF CPD and TRAINING: Mandatory annual e-safety and filtering training delivered to all educational and operational staff, covering threat trends, grooming indicators, and alert response protocols.

Simulated Bypass and Effectiveness Testing: Annual technical testing tests the platform's resilience against proxy bypasses, illicit content insertion, and emerging evasive tactics.

Continuous Professional Development (CPD): All teachers, pastoral mentors, and leadership staff complete annual training on online safety trends, cyber-bullying mitigation, online grooming identification, and effective alert triage.

Policy Approval, Governance Sign-off, and Review

This policy is reviewed annually to ensure alignment with DfE standards, emerging technology frameworks, and statutory updates.

- ✓ **Approved by:** Senior Leadership Team and Board of Directors
- ✓ **Operational Sign-off:** Kim, Head of Safeguarding (Lead DSL)
- ✓ **Publication Date:** 6th October 2026
- ✓ **Next Scheduled Review:** 16th August 2027