

Briefing Paper Online Use,
Filtering and Monitoring
January 2026



Date: October 2025

Version: 1.0

Audience: All RedEverywhere Staff

Author: Marcus Isman-Egal - Designated Safeguarding Lead

1. Purpose of this Briefing

This briefing provides clear guidance to all RedEverywhere staff on:

- Appropriate and safe use of online systems in line with Keeping Children Safe in Education 2025.
- Filtering and monitoring expectations.
- What online content and platforms are **allowed, restricted, or blocked**.
- How decisions on online use are made, reviewed, and recorded.

This forms part of our **safeguarding and online safety strategy**.

2. Legal and Statutory Framework

This policy aligns with:

- Keeping Children Safe in Education (KCSIE) 2025
- UKCIS Guidance: *Filtering and Monitoring Standards for Schools and Colleges*
- Prevent Duty
- Data Protection Act 2018 and UK General Data Protection Regulation
- Safer Internet Centre guidance and CEOP reporting protocols.

3. Roles and Responsibilities

Role	Responsibility
DSL / DDSL	Oversee filtering and monitoring, approve changes, escalate risks.
IT & Network Administrator	Implement technical controls, maintain filtering logs.
All Staff	Comply with online use expectations, report concerns, do not bypass controls.
Students	Follow Acceptable Use Policy and report any unsafe content.

All decisions must **prioritise safeguarding, data protection, and compliance** with statutory duties.

4. Principles for Online Use

- Access to the internet must **enhance learning, support teaching**, or aid operational delivery.
- All online activity is subject to **filtering, monitoring, and logging**.
- Any request to unblock or allow new sites/platforms must go through the DSL and COO/Business Manager for approval.
- Content that is illegal, harmful, extremist, violent, sexual, or unrelated to education is strictly **prohibited**.
- Personal use of organisational devices or networks is **not permitted during working hours**.

5. Filtering & Monitoring Standards

- RedEverywhere uses **real-time filtering and monitoring tools** in line with UKCIS standards.
- Activity logs are **reviewed regularly** to identify patterns of risk, including nudification, cyber-flashing, trolling, or extremist content.
- Alerts are escalated immediately to the DSL for action.

6. Examples of What is Allowed / Blocked

Category	Allowed	Blocked	Notes
Education & Curriculum	GCSE / Functional Skills platforms, BBC Bitesize, Khan Academy, AQA UAS, Teams, Office 365		Must support learner outcomes.
Safeguarding & Well-being	CEOP, Childline, NSPCC, Operation Encompass, Safer Schools		Promotes safety and support.
Social Media	LinkedIn (staff), YouTube (restricted mode – curriculum use only)	TikTok, Instagram, Snapchat, Facebook (student use)	Reviewed termly; restricted access.

Category	Allowed	Blocked	Notes
Streaming		Netflix, Amazon Prime, Disney+	Not relevant to education delivery.
Gaming		All gaming platforms	No gaming permitted on organisational networks.
Messaging	Microsoft Teams chat, secure internal email	WhatsApp (web), Discord, Telegram	Encrypted or unmonitored platforms blocked.
AI / Emerging Tech	Controlled AI platforms for curriculum use	Unmoderated chat platforms	Usage reviewed on a case-by-case basis.

7. Decision-Making and Change Control

- Any staff request to change site access must be submitted via **COO or Business Manager & DSL approval form**.
- All decisions (approved, declined, or pending) will be **logged** on DCPro.
- Logs are reviewed termly as part of RedEverywhere's **safeguarding and compliance audit**.

8. Reporting Concerns

- Any **inappropriate or accidental access** must be reported immediately to the DSL.
- Use the RedEverywhere Incident Reporting Form.
- Serious incidents will be logged, investigated, and, where appropriate, referred to external agencies (e.g., LADO, Police, CEOP).

9. Training & Awareness

- All staff receive **annual online safety training**.
- DSL/DDSLs receive enhanced training on filtering, monitoring, and online harms.
- Parents and students receive awareness information through workshops and Safer Schools updates.

Online Access Decision Log – RedEverywhere

Date	Site / Platform	Request ed by	Decision (Allow/Block)	Reason for Decision	Approved by	Review Date
DD/MM/YY	Example: YouTube (Restricted)	Teaching Staff	Allow (Restricted)	Educational use	DSL & IT	Termly
DD/MM/YY	TikTok	Student	Block	Safeguarding & distraction risk	DSL	Termly
DD/MM/YY	CEOP Website	Safeguarding Lead	Allow	Safeguarding support	DSL	Annual

RED

RED
Everywhere