REBOOT
EDUCATION

Online Safety Policy 2026

Person responsible for this policy:	Paul Arch
Policy author:	Paul Arch
Date Approved by Directors:	January 2024
Date to be Reviewed:	January 2026
Date of next Review:	January 2027
Policy displayed on website:	Yes

ONLINE SAFETY POLICY

1. Aims

Reboot Education will:

1. Maintain robust, proportionate systems to protect learners, staff and volunteers from online harm on-site and during off-site learning arranged by the provision.
2. Deliver a whole-community approach to online safety (including **mobile and smart technologies**), empowering pupils and adults to use technology safely, responsibly and respectfully.
3. Operate clear mechanisms to **identify, assess, record, intervene and escalate** concerns, including those that originate online but present offline risks.

2. Scope

This policy applies to all students, parents/carers, staff (including contractors and agency staff), volunteers, visitors, and any third-party providers who use Reboot Education systems or deliver education on our behalf (including **alternative provision** partners).

3. Legislative and Guidance Framework

This policy reflects and should be read alongside:

- **Keeping Children Safe in Education (KCSIE) 2025** (statutory from 1 Sept 2025).
- **Working together to improve school attendance** – statutory guidance from 19 Aug 2024 (attendance as a safeguarding concern).
- **Filtering & Monitoring** – DfE **digital and technology standards** (updated 2 Feb 2026) and "Plan technology for your school" self-assessment.
- **Generative AI: product safety standards / expectations** (DfE, Jan 2025; last updated Jan 2026).
- **Alternative Provision** – updated DfE statutory guidance (Feb 2025) and accompanying practitioner guide.
- **Prevent Duty Guidance (2023)** – statutory (in force from 31 Dec 2023).
- **Searching, screening and confiscation** (DfE).
- **UKCIS**: Sharing nudes and semi-nudes – advice for education settings (updated Mar 2024).
- **Ofcom & Online Safety Act 2023 implementation context** (sector response 2025).

4. Definitions and Risk Framework (the "4Cs")

Our approach is based on the **4 key categories of online risk**:

- **Content** – exposure to illegal/inappropriate/harmful content, including **pornography, hate content, extremism, self-harm**, and now explicitly **misinformation, disinformation and conspiracy theories**.
- **Contact** – harmful online interactions (e.g., grooming, coercion, sexual/criminal exploitation, financial scams).
- **Conduct** – harmful behaviours (e.g., bullying/harassment, creation/sharing of indecent imagery, "sexting", upskirting, abusive content).
- **Commerce** – risks such as **scams, phishing, gambling, in-app purchases** and exploitative advertising.

5. Roles and Responsibilities

5.1 Company Directors

- Hold overall responsibility for online safety and ensure this policy is implemented, monitored, and **annually reviewed** alongside a proportional risk assessment.
- Ensure leadership understands and oversees **filtering and monitoring** arrangements and receives regular reports from the DSL/IT lead.

5.2 Designated Safeguarding Lead (DSL)

The DSL (and deputies) has lead responsibility for online safety, including to:

- Embed, communicate and monitor this policy; manage incidents; liaise with external agencies; and ensure accurate **logging and escalation**.
- Oversee annual **filtering/monitoring** self-assessment and action plan; ensure mis/disinformation and **AI-generated risks** are covered in controls and curriculum.
- Treat **attendance concerns** that indicate risk as safeguarding matters and coordinate escalation with attendance leads and local partners.

5.3 ICT Support / External Providers

- Maintain secure networks and devices; implement **appropriate filtering and monitoring**; review effectiveness **at least annually**; and advise leaders/DSL on risk and exceptions.

5.4 All Staff and Volunteers

- Read KCSIE Part 1 and follow this policy; model safe online behaviour; enforce acceptable use; report concerns immediately to the DSL.

5.5 Parents/Carers

- Support the Acceptable Use Agreement (AUA) and reinforce safe use at home; raise concerns via the DSL/company directors.

5.6 Visitors/Community Users

- Where relevant, follow the AUA and site protocols when accessing Reboot systems.

6. Education, Curriculum and Awareness

6.1 Pupils

We teach pupils to **use technology safely, respectfully and responsibly**, recognise unacceptable behaviour, and report concerns. Coverage includes privacy, social media literacy, critical thinking about **mis/disinformation**, risks in online relationships, and how data is shared/used. Teaching is adapted for SEND and vulnerable learners.

6.2 Staff

Induction and annual training cover: current online harms (including AI/Deepfakes), sexual violence/harassment, cyber-bullying, digital footprints, UKCIS guidance on **nudes/semi-nudes**, and **attendance as safeguarding**.

6.3 Parents/Carers

We provide guidance through newsletters/briefings on device safety, platforms, **mis/disinformation**, parental controls, and reporting routes.

7. Filtering, Monitoring and Cyber Security

Reboot Education maintains **appropriate filtering and monitoring** systems to provide a safe online environment without unreasonably impeding teaching and learning. **Leaders and the DSL** understand how systems work, receive **regular reports**, and conduct a **documented annual review** using DfE's "Plan technology for your school" tool. Actions, exceptions, and rationales are recorded.

- **Filtering** prevents access to illegal or harmful content (including extremist content), while **monitoring** captures potentially risky user activity for review and response.
- Controls explicitly consider **generative AI** (e.g., prompts producing harmful content, image manipulation, bypass attempts) and are configured to ensure AI tools **cannot circumvent** protections.
- Cybersecurity is a safeguarding control: leadership oversees patching, MFA, encryption, backups, incident response, and vendor risk.

Annual Evidence Pack (kept by DSL/IT): self-assessment report; risk assessment and exception log; leadership review minutes; testing results (on-site/off-site devices); and actions with timelines.

8. Responsible Use of AI (Students and Staff)

Reboot Education supports safe, age-appropriate use of **AI** subject to the following:

- AI tools used in education must meet **DfE product safety standards/expectations**; staff must risk-assess use, ensure content moderation is effective, and never use AI that bypasses filtering/monitoring.
- Students' use of AI is **supervised** and guided; staff explicitly teach risks (e.g., fabricated sources, hallucinations, bias, deepfakes).
- No AI tool may be connected to or process personal/sensitive data without explicit approval and a compliant legal basis.

9. Alternative Provision (AP)

Where Reboot Education commissions or partners with other AP providers:

- We obtain **written confirmation** of safeguarding checks and review placements **half-termly** for safety, attendance and suitability; we record full provider addresses (including satellite sites).
- We align to the updated **AP statutory guidance** and February 2025 LA/schools guide (e.g., oversight, reintegration planning).

10. Attendance as a Safeguarding Concern

Persistent or unexplained absence can indicate neglect, exploitation or other harms (including online). The DSL monitors patterns with attendance leads and escalates concerns per **statutory attendance guidance**.

11. Prevent Duty and Online Radicalisation

We assess risk of radicalisation (including online) and ensure proportionate staff training, referral pathways, and record-keeping in line with **Prevent duty guidance (2023)**.

12. Acceptable Use

All users sign **Acceptable Use Agreements** (AUAs). Visitors and suppliers using our systems agree to abide by site rules and supervision. AUAs cover account security, privacy, device use, AI use, and the prohibition of illegal/harmful content.

13. Personal Devices and Mobile/Smart Tech

Students may bring personal devices only with prior consent and must hand them in for secure storage on arrival; retrieval is at day's end. Breaches may result in proportionate sanctions and/or confiscation in line with DfE guidance.

14. Cyber-Bullying and Online Abuse

We educate, prevent, and respond to cyberbullying. Staff address abusive messaging, image-based abuse and peer-on-peer incidents swiftly, recording actions and considering police referral where **illegal material** exists.

15. Responding to Incidents and Misuse

- Staff report concerns immediately to the DSL. The DSL triages, records, informs parents (where appropriate), and liaises with agencies.
- **Nudes/semi-nudes:** Follow **UKCIS** guidance (do not view/possess unless exceptionally necessary to safeguard; never copy/share; consider referral).
- **Searching/screening/confiscation:** Staff may search devices or delete material where there is a lawful, good reason and in line with DfE guidance and this policy. Keep a clear audit trail; consider police referral where criminality is suspected.

16. Staff Use of Work Devices Off-Site

Staff must secure devices (MFA, encryption, time-out lock, updates), use them **only for work purposes**, and follow data protection and AI safety expectations. Concerns about device security must be raised with ICT support immediately.

17. Training and Induction

- **All staff**: safeguarding and online safety training at induction and **at least annually**, plus regular updates (briefings/emails/meetings). Content includes AI risks, mis/disinformation, cyber security, sexual harassment online, and UKCIS protocols.
- **DSL/Deputies**: enhanced safeguarding training (including online safety) at least every 2 years, and knowledge refreshed at least annually.

18. Monitoring, Review and Assurance

- **Incident data** (Appendix 4) is reviewed termly by DSL and reported to directors, informing curriculum, filtering/monitoring changes, and staff training.
- **Annual review** each September (or following major guidance changes), including: leadership sign-off; attendance-safeguarding interface; AP oversight; Prevent risks; AI controls; and DfE technology self-assessment outputs.

19. Linked Policies

- Child Protection & Safeguarding Policy (incl. peer-on-peer/sexual violence & harassment)
- Behaviour Policy
- Data Protection/Privacy Notices
- Attendance Policy (statutory guidance aligned)
- Searching, Screening & Confiscation (local procedures referencing DfE guidance)

CEOS's Signatures:	
Paul Arch	Viv Hunt

Version Control / Update Log

Change	Reason/Source	Date	Approved by
Policy rewritten to align with KCSIE 2025 (incl. mis/disinformation)	Statutory update	Jan 2026	CEOs
Added DfE Filtering & Monitoring annual review & leadership oversight	DfE digital standards (2026)	Jan 2026	CEOs
New AI safety section (DfE product safety standards/expectations)	DfE guidance (2025/26)	Jan 2026	CEOs
Attendance added as safeguarding	Statutory attendance guidance	Jan 2026	CEOs
Updated AP oversight duties	DfE AP guidance (2025)	Jan 2026	CEOs

Appendices

Appendix 1 – Acceptable Use Agreement (Students and Parents/Carers)

ACCEPTABLE USE OF THE PROVISION'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS

Name of Student:	

When I use Reboot Education devices, accounts or internet access, I will:

- Use them **responsibly and for learning only**, following staff instructions and provision rules.
- Keep my usernames/passwords private and log off when finished.
- Think critically about what I see online, including **misinformation, disinformation and conspiracy content**; ask a trusted adult when unsure.
- Report anything upsetting, illegal or worrying to a member of staff or my parent/carer straight away.
- Use AI tools only if permitted by staff, follow guidance on safe use, and never try to bypass filtering/monitoring.

I will **not**:

- Access or share illegal or harmful content; bully, harass or abuse others; or create/share indecent images.
- Log in as someone else, or try to bypass filters/security.
- Bring personal devices to lessons unless agreed; if permitted, I will hand them in at reception at the start of the day.

Monitoring and consequences: I understand the provision monitors use of its systems and that misuse may lead to sanctions and, where appropriate, police involvement.

Signed (Student):	**Date Signed:**

Parent/carer's agreement: I agree that my child can use the provision's ICT systems and internet when appropriately supervised by a member of provision staff. I agree to the conditions set out above for pupils using the provision's ICT systems and internet, and for using electronic devices in the provision, and will make sure my child understands these.

Signed (Parent/Carer):	**Date Signed:**

Appendix 2 – Acceptable Use Agreement (Staff, Contractors, Volunteers, Visitors)

ACCEPTABLE USE OF THE PROVISION'S ICT SYSTEMS AND INTERNET:

AGREEMENT FOR STAFF, VOLUNTEERS AND VISITORS

Name of staff member/volunteer/visitor:	

When using Reboot Education systems or devices (on-site or remotely), I will:

- Use systems **only for professional purposes** and keep data secure (MFA, encryption, updates).
- Follow child protection procedures and report safeguarding concerns immediately to the DSL.
- Use AI only where approved and in line with **DfE AI product safety standards/expectations**; never attempt to circumvent filtering/monitoring.
- Not access, create, store or share illegal or harmful material; not disclose confidential information; not install unauthorised software or connect unauthorised hardware.
- Obtain permission before taking/using pupil images and only on organisation devices, in line with data protection policy.

I understand Reboot Education **monitors** network and device use and may take disciplinary or legal action following misuse.

- I will only use the provision's ICT systems and access the internet in provision, or outside provision on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.
- I agree that the provision will monitor the websites I visit and my use of the provision's ICT facilities and systems.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside provision, and keep all data securely stored in accordance with this policy and the provision's data protection policy.
- I will let the designated safeguarding lead (DSL) and ICT technician know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will always use the provision's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signature:	Role:	Date:

Appendix 3 – Staff Online Safety Training Needs: Self-Audit

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	**Yes/No (add comments if necessary)**
I know who the **DSL** and deputies are and how to contact them	
I can identify signs of online abuse (bullying, harassment, sexual violence/harassment, image-based abuse).	
I understand **UKCIS** processes for incidents involving **nudes/semi-nudes**.	
I understand our **filtering/monitoring** arrangements, my role in them, and how to report concerns/exceptions.	
I can explain to pupils how to evaluate **mis/disinformation** and safely use **AI**.	
I know attendance patterns can indicate safeguarding concerns and how we escalate.	
I have completed Prevent training and understand our local risk indicators and referral routes.	
Training requested:	

Appendix 4 – Online Safety Incident Log (Secure Record)

Online Safety Incident Log	
Date/Time:	
Location/Device:	
Summary of Incident:	
Category (4Cs):	
Immediate Action	
Parents/Carers Informed?	
External Agencies	
Outcome/Follow-up	
Recorded by (name/signature)	

Notes: For any suspected illegal content or criminal behaviour, consult the DSL immediately; consider police referral. For **nudes/semi-nudes**, follow UKCIS guidance. For device searches, follow DfE **Searching, screening and confiscation** guidance and record rationale, persons present, and outcomes.

Appendix 5 – Annual Filtering & Monitoring Review (Template)

Annual Filtering & Monitoring Review	
Date completed:	**Completed by:**
Task:	**RAG Rating:**
Self-assessment using DfE **Plan technology for your provision** is completed.	
Recommendations from the self-assessment logged.	
Leadership oversight: report presented to directors on [date]; actions agreed.	
Scope & coverage: on-site networks; provision-owned mobiles; remote access; AP/site variants; BYOD restrictions.	
AI risks: prompts/outputs, image tools, deepfakes, data leakage; product checks align with **DfE AI standards**.	
Effectiveness testing: block/alert tests; staff/pupil feedback; incident trend analysis.	
Action plan with timelines produced.	

Appendix 6 – AI Classroom Use Principles (Quick Guide)

- Only use **approved** AI tools (risk-assessed).
- Never input personal/sensitive data; verify outputs with credible sources; cite where appropriate.
- Report unsafe or harmful AI behaviour to staff/DSL immediately.