Digital and Online Safety Policy

Frontier Learning Trust

Policy owner:	Head of Digital Development
Last reviewed on:	September 2026
Next review due by:	September 2027
Linked policies:	Safeguarding and Child Protection Policy Acceptable Use of Trust Systems Policy Staff Acceptable Use Agreement Student Acceptable Use Agreement
Approved by:	SLT

1. Purpose

This policy sets out how Frontier Learning Trust approaches digital and online safety across both sites. It exists alongside and is read in conjunction with the FLT Safeguarding and Child Protection Policy, which governs how all safeguarding concerns, including those arising from online activity, are identified, reported and managed. This policy does not replace or duplicate that document.

The purpose of this policy is to set out how the trust manages the digital environment to reduce risk, how it educates staff and students to navigate that environment safely, and how it responds when things go wrong. Reporting routes, the role of the Designated Safeguarding Lead, and communication with parents and carers are all set out in the Safeguarding and Child Protection Policy.

This policy applies to all staff, students, trustees, volunteers and contractors across Frontier Learning Trust.

2. Online Safety as a Safeguarding Issue

The trust recognises that online safety is a core safeguarding responsibility, not a separate or secondary concern. Digital technologies are central to education and daily life at both sites, and bring genuine benefit. They also create real risk, including risks that are specific to the age group the trust serves.

The majority of students at Woodhouse College and Imperial College London Mathematics School are aged 16 to 19. This age group faces a distinct online risk profile. The risks most relevant to the trust's community include:

- Self-generated intimate images and videos, including those created or manipulated using AI, shared with or without consent. KCSIE 2026 strengthens the language around this area, recognising deepfakes and AI-generated imagery as a significant and growing harm.
- Financially motivated sexual extortion, where young people are manipulated into sharing intimate images and then threatened. This is an increasing safeguarding concern for the 16-19 age group.
- Online harassment, abuse and bullying, including through social media, messaging platforms and gaming environments.
- Misogyny and harmful sexual behaviour promoted through online content, including through influencer culture and extremist communities. KCSIE 2026 explicitly recognises extreme misogyny as a safeguarding concern linked to harmful sexual behaviour.
- Grooming, exploitation and radicalisation, including online. The trust's Prevent responsibilities extend to online radicalisation.
- Harmful content including content that promotes self-harm, eating disorders, suicide or substance misuse.
- AI-generated child sexual abuse material and associated exploitation risks, as identified by the National Crime Agency's CEOP education programme.

Any online activity that gives rise to a safeguarding concern is managed in line with the FLT Safeguarding and Child Protection Policy. If you are concerned about a student, report it on MyConcern. The safeguarding team will determine what action is needed.

3. Managing the Digital Environment

3.1 Filtering and monitoring

The trust operates filtering and monitoring systems across its networks and devices in line with the DfE Filtering and Monitoring Standards. Filtering aims to block access to harmful or malicious concepts and communication. Monitoring is used to flag online behaviour that is harmful or in conflict with our codes of conduct.

Filtering and monitoring exist primarily to support safeguarding, not to police how people work.

In line with KCSIE 2026, the effectiveness of filtering and monitoring is reviewed at least once each academic year. This review is led by the Head of Digital Development and covers all internet-connected devices across both sites. A record of each review is maintained. The review considers whether filtering is appropriately calibrated, whether monitoring is identifying concerns at the right threshold, and whether any gaps exist.

Monitoring activity is overseen by the Designated Safeguarding Leads. Information arising from monitoring is handled in accordance with safeguarding and data protection requirements.

3.2 Access controls and account management

The trust manages access to its systems through secure account management, including multi-factor authentication and role-based access controls. Accounts are created and removed promptly when staff join, change role or leave. These controls reduce the risk of unauthorised access and support the trust's cyber security posture, which KCSIE 2026 recognises as a safeguarding issue in its own right.

3.3 Approved platforms

The trust operates within a Microsoft 365 environment. Communication between staff and students takes place through Microsoft 365 email and Teams. The use of unapproved platforms for communication or data storage creates safeguarding and data protection risk and is not permitted.

4. Education and Awareness

4.1 Staff

All staff receive safeguarding training that includes online safety, delivered at induction and refreshed annually. This training covers:

a. Recognising and responding to online safety concerns, including those arising from monitoring
b. The specific risks relevant to the 16-19 age group, including self-generated intimate imagery, financial sexual extortion, online misogyny and radicalisation
c. The trust's reporting process and the role of MyConcern
d. Responsible and professional conduct online, including staff-student boundaries on social media
e. Safe and appropriate use of AI tools

Additional guidance and updates are provided to staff through the staff hub and through digital training led by the Head of Digital Development.

4.2 Students

Students receive online safety education as part of induction at both sites, and through tutorial and pastoral programmes throughout the academic year.

Education covers:

a. Understanding and managing their digital footprint and online reputation
b. Self-generated intimate imagery, consent, and the legal and personal consequences of sharing these images or videos
c. Recognising and responding to online harassment, coercion and exploitation
d. Critical evaluation of online content, including AI-generated content
e. Responsible and safe use of AI tools, in line with the trust's AI guidance
f. How to get help if something goes wrong online, including from the safeguarding team

Online safety education for students is not limited to formal sessions. Staff are expected to address online safety issues as they arise in the classroom and pastoral context.

5. Artificial Intelligence

AI presents both significant opportunity and specific safeguarding risk. KCSIE 2026 strengthens this section considerably, bringing AI-related harms into the definitions used throughout the guidance rather than treating them as a separate issue. This includes AI-generated and digitally altered nudes and semi-nudes (including so-called "deepfakes" and "deep nudes"), AI-generated child sexual abuse material, and contact risks arising from generative AI systems that simulate human conversation. KCSIE is clear that any incident involving a nude or semi-nude image, whether it is AI-generated, digitally altered, or genuine, and whether shared consensually or not, must be treated as a safeguarding concern and receive a proportionate safeguarding response.

The trust's approach to AI is set out in its published AI guidance, available on the staff hub and student hub. All use of AI by staff and students is expected to align with the trust's AI principles: Safety, Agency, Rigour and Integrity. Where AI use gives rise to a safeguarding concern, it is managed through the safeguarding process in the same way as any other concern.

Staff must only use AI tools approved by the Head of Digital Development when processing trust or student data. No personal, sensitive or safeguarding data should be entered into an AI tool unless it has been carefully anonymised in line with the trust's Data Protection Policy. This applies regardless of whether the tool has been approved for general use, as approval for use does not itself authorise the processing of identifiable pupil or staff data. Staff who are unsure whether information has been sufficiently anonymised should seek advice from the Head of Digital Development or the Data Protection Officer before proceeding.

Students are guided on appropriate AI use through the AI guidance and through subject-specific instruction from teachers, including awareness of the risks of AI-generated imagery and the harm this can cause to themselves or others.

6. Responding to Concerns

Where online activity gives rise to a safeguarding concern, it is managed in line with the FLT Safeguarding and Child Protection Policy. All concerns should be reported on MyConcern. The safeguarding team will determine what action is required, including whether to involve parents or carers, external agencies or the police.

Where online behaviour does not reach the threshold of a safeguarding concern but represents a breach of the trust's expectations, it is managed through the relevant behaviour or disciplinary process, as set out in the Acceptable Use Agreements and the Staff Code of Conduct or Student Behaviour Policy.

Serious incidents are reviewed by the Head of Digital Development and the relevant DSL to inform ongoing risk management, training and policy review.

7. Responsibilities

The Head of Digital Development is responsible for the technical management of the digital environment, the annual review of filtering and monitoring, and the maintenance of this policy.

The Designated Safeguarding Leads at each site are responsible for overseeing the safeguarding response to online concerns and for ensuring that online safety is embedded within the wider safeguarding framework. Their roles and responsibilities are set out in the Safeguarding and Child Protection Policy.

All staff share responsibility for promoting online safety, recognising risk, and reporting concerns promptly.

8. Monitoring and Review

This policy is reviewed annually by the Head of Digital Development. The annual review of filtering and monitoring effectiveness required by KCSIE 2026 is conducted at the same time and documented separately. Both are reported to the Audit and Risk Committee as part of the Head of Digital Development's termly board update.

This policy is read alongside the FLT Safeguarding and Child Protection Policy, which is reviewed annually by the Designated Safeguarding Lead and signed off by the Trustees.

9. Related Documents

- Safeguarding and Child Protection Policy
- Acceptable Use of Trust Systems Policy
- Staff Acceptable Use Agreement
- Student Acceptable Use Agreement
- Staff Code of Conduct
- Student Behaviour Policy
- Data Protection Policy
- Cyber Incident Response Plan
- AI Guidance (staff hub and student hub)
- DfE Filtering and Monitoring Standards
- Keeping Children Safe in Education 2026