



Cornerstone Academy Trust

Online Safety Policy

Trust-wide policy for all pupils and adults working for or on behalf of the Trust

Policy owner	Designated Trust Safeguarding Lead and Online Safety Lead
Approval body	Education Committee
Updated	October 2026
Review cycle	Annual, or earlier following a change in law or guidance
Next review	Autumn Term 2027 or earlier if legislation, statutory guidance or technology materially changes
Applies to	All schools and operations of Cornerstone Academy Trust

This policy should be read alongside the Trust Safeguarding and Child Protection Policy, Behaviour Policy, Staff Code of Conduct, Acceptable Use arrangements, Data Protection Policy, Cyber Security Policy and Artificial Intelligence Policy.

1. Purpose

Cornerstone Academy Trust is committed to protecting children and the wider Trust community from online harm while enabling safe, responsible and effective use of digital technology. Online safety is an integral part of safeguarding and applies across the Trust's seven-campus, one-school operating model.

Safeguarding is everyone's responsibility. Online concerns will be considered using a child-centred approach and managed through the Trust safeguarding arrangements where a child may be at risk.

2. Scope

This policy applies to pupils, staff, trustees, volunteers, contractors, visitors and community users where they use Trust digital systems or where online conduct has a relevant safeguarding, welfare, behaviour, professional or security connection with the Trust.

- Trust-owned devices, networks, accounts, cloud services, learning platforms and communications systems.
- Personal devices and services used on Trust premises or for Trust business, subject to the Trust's rules.
- Online activity outside school where it creates a safeguarding concern or otherwise falls within an applicable Trust policy or legal responsibility.

3. Statutory and guidance framework

The Trust will have regard to current law, statutory guidance and relevant national standards. Key reference points for 2026/27 include:

- Keeping Children Safe in Education 2026 (KCSIE), including its online safety, safeguarding, staff allegation and child-on-child abuse requirements.
- DfE Filtering and Monitoring: Core Standard, updated September 2026.
- DfE Mobile Phones in Schools statutory guidance, applicable from 1 September 2026.
- UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people.
- DfE Generative AI: Product Safety Standards and current DfE guidance on generative AI in education.
- UK GDPR, Data Protection Act 2018, Computer Misuse Act 1990, copyright law and other applicable legislation.

4. The four areas of online risk

The Trust's online safety arrangements address the four broad areas of risk identified in safeguarding guidance:

Content: being exposed to illegal, inappropriate or harmful material.

Contact: being subjected to harmful online interaction with other users.

Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Commerce: risks such as online gambling, inappropriate advertising, phishing and financial scams.

Risks overlap. Online safety education, safeguarding responses, filtering and monitoring, behaviour expectations and technical controls will therefore operate together.

5. Governance and accountability

5.1 Board of Trustees

- approve or oversee approval of this policy under the Trust scheme of delegation;

- seek assurance that filtering and monitoring systems are appropriate and that the provision is formally reviewed at least annually;
- receive proportionate safeguarding and online safety assurance, including significant themes and improvement actions;
- ensure trustees receive appropriate safeguarding and online safety awareness, with relevant trustees receiving sufficient information to provide effective challenge; and
- seek assurance that online safety is embedded within safeguarding, curriculum, behaviour, data protection and technology governance.

5.2 CEO, Executive Headteacher and senior leaders

- ensure this policy and associated procedures are implemented consistently;
- provide resources and oversight for safeguarding, filtering, monitoring, cyber security and staff training;
- ensure serious incidents are escalated under the correct safeguarding, HR, data protection or security procedure; and
- ensure new technology and material changes in working practice are considered for online safety risk.

5.3 Designated Safeguarding Lead

The DSL holds lead safeguarding responsibility for online safety. The DSL will work with deputies, the Online Safety Lead, senior leaders and IT/EdTech colleagues while retaining safeguarding decision-making responsibility.

- receive and triage online safeguarding concerns;
- ensure safeguarding records and referrals are made in accordance with Trust procedures;
- understand the filtering and monitoring arrangements and receive relevant safeguarding alerts or reports;
- contribute to reviews of filtering and monitoring; and
- ensure responses to child-on-child abuse, harmful sexual behaviour and concerns involving adults follow the Trust safeguarding framework.

5.4 Online Safety Lead

- coordinate implementation and review of this policy;
- lead or coordinate the Online Safety Group;
- support curriculum mapping, staff awareness and parent/carers engagement;
- identify emerging online safety themes and recommend improvements; and
- work closely with the DSL so that safeguarding concerns are not managed solely as technical or behavioural incidents.

5.5 IT/EdTech and service providers

- implement and maintain agreed technical controls, filtering, monitoring and security arrangements;
- provide senior leaders and the DSL with information needed to understand and review technical safeguarding provision;
- maintain appropriate access controls, logging, patching, device management and security in accordance with the Trust Cyber Security Policy; and
- escalate relevant safeguarding or security alerts promptly through agreed routes.

5.6 Staff and volunteers

- follow the Staff Code of Conduct, Acceptable Use arrangements and safeguarding procedures;
- use Trust-approved communication channels for professional communications;
- report online safeguarding concerns immediately to the DSL or deputy DSL;
- not investigate child protection concerns independently or retain prohibited imagery;
- maintain professional boundaries and model safe, responsible digital behaviour; and

- complete required safeguarding, online safety, data protection and cyber-security training.

6. Online Safety Group

The Online Safety Group supports the DSL and Online Safety Lead. It does not replace the DSL's safeguarding responsibility.

Membership should include the DSL or deputy DSL, Online Safety Lead, relevant senior leader, nominated trustee, teaching/support staff representation and IT/EdTech representation where appropriate.

The Group will review policy implementation, online safety education, significant themes from incidents and alerts, filtering and monitoring assurance, stakeholder feedback and improvement actions. Material safeguarding or compliance concerns will be escalated without waiting for the next Group meeting.

7. Education and curriculum

The Trust will provide a planned and progressive online safety curriculum, supported by teaching across Computing, PSHE and Relationships and Health Education and reinforced through wider curriculum opportunities.

- teach pupils to evaluate the reliability, purpose and provenance of online information, including AI-generated content;
- teach safe and respectful participation online, including reporting routes and help-seeking;
- address privacy, personal data, scams, commercial risks, copyright and secure use of accounts;
- address harmful content, contact and conduct in an age-appropriate way;
- adapt learning for pupils with SEND, EAL or other vulnerabilities where necessary; and
- use relevant national resources and initiatives such as ProjectEVOLVE, CEOP education resources and Safer Internet Day without relying on year-specific links.

8. Filtering and monitoring

The Trust will provide appropriate filtering and monitoring as part of its safeguarding arrangements. Filtering is a preventative control intended to restrict access to illegal, inappropriate or potentially harmful content. Monitoring provides oversight of activity and alerts or reports that may require intervention.

- roles and responsibilities for filtering and monitoring will be clearly allocated between safeguarding, leadership and technical staff/providers;
- provision will be reviewed formally at least annually and additionally where safeguarding risk, working practice or technology changes indicate that review is needed;
- filtering and monitoring will consider relevant text, image, audio, video and AI-generated content;
- there will be clear routes for reporting inappropriate content and for managing authorised filtering changes;
- checks and reviews will be documented sufficiently to demonstrate oversight and follow-up;
- systems and responses will be proportionate to pupils' age, risk and educational need; and
- the Trust recognises that technical controls do not replace supervision, education, professional curiosity or safeguarding action.

9. Artificial intelligence and emerging technology

AI may support learning, teaching and school operations only where use is safe, lawful and consistent with the Trust Artificial Intelligence Policy. Human professional accountability remains with staff.

- approved educational AI products should be assessed for intended use, age suitability, safeguarding, filtering/monitoring, privacy, security and intellectual property implications;
- staff must not enter confidential or personal data into AI services unless the service and use have been approved for that purpose;
- AI outputs used for professional work must be checked critically for accuracy, bias and suitability;
- significant decisions affecting individuals must not be delegated to uncontrolled AI output; and
- pupils will be taught that AI-generated information and media can be inaccurate, misleading or manipulated.

10. Mobile phones and smart technology

In accordance with the DfE statutory guidance for the 2026/27 academic year, Trust schools will be mobile-phone-free environments by default throughout the school day. The detailed arrangements for bringing, storing or surrendering devices and for sanctions will be set out in the Behaviour Policy or a linked mobile phone procedure.

Any exception will be controlled and justified, for example where an individual adjustment is required because of disability, medical need or another relevant circumstance. Other communications or smart technology with similar functionality may be covered by the same rules.

Where the Trust operates an approved bring-your-own-device arrangement for laptops or tablets, it will be governed separately and will not make pupil mobile phones part of the BYOD scheme.

11. Acceptable use and professional communications

- Users will have access only to systems, services and information appropriate to their role and authorisation.
- Passwords and accounts must not be shared or used to impersonate another user.
- Users must not attempt to bypass filtering, monitoring, access controls or security safeguards.
- Staff communications with pupils and parents/carers must use approved professional channels and remain professional in content and tone.
- Trust systems must not be used for unlawful activity, harassment, discriminatory abuse, unauthorised commercial activity, deliberate security compromise or other prohibited conduct.
- Acceptable Use agreements or notices will define detailed expectations for relevant user groups.

12. Images, video and online publishing

Images, video and pupil work will be created, stored and published in accordance with the Trust Data Protection Policy, privacy notices, safeguarding arrangements and applicable image-use procedures.

- staff and volunteers must use approved devices and systems for Trust images and recordings;
- image use must take account of known safeguarding restrictions;
- the Trust will explain relevant purposes and arrangements for image use and obtain consent where consent is the applicable basis under Trust arrangements;
- personal data will not be published unnecessarily; and
- livestreaming and video-conferencing will be risk-managed and conducted through approved services and professional practices.

13. Online child-on-child abuse

Online abuse between children will be treated as a safeguarding matter and will not be dismissed as banter or normal online behaviour. The Trust will respond under its Safeguarding and Child Protection Policy, Behaviour Policy and other relevant procedures.

Relevant concerns can include bullying, harassment, coercion, threats, non-consensual image sharing, harmful or manipulated imagery, online sexual harassment and other technology-facilitated abuse. The DSL will determine the safeguarding response and external referral requirements.

14. Sharing nudes and semi-nudes

Incidents involving the sharing of nudes or semi-nudes by children and young people will be managed in accordance with current UKCIS guidance and the Trust Safeguarding and Child Protection Policy.

Staff must: report the incident to the DSL or deputy DSL immediately; not view, copy, print, share, store or save the imagery; not ask a child to share or download it; not conduct their own investigation; and not blame or shame a child involved.

If imagery is seen accidentally, the member of staff must stop viewing and report this to the DSL. The DSL will determine the next steps and any exceptional safeguarding decision in accordance with current guidance.

15. Reporting and responding to online safety incidents

All safeguarding concerns must be reported promptly through the Trust safeguarding system. Immediate action must prioritise the safety and welfare of the child or other person at risk.

- Preserve relevant information without unnecessarily accessing, copying or circulating harmful or illegal content.
- The DSL will assess safeguarding risk and decide on referrals or consultation with children's social care, police or other agencies as required by the Trust safeguarding procedures.
- Technical or cyber incidents will also be referred to the appropriate IT/security route, without delaying safeguarding action.
- Behavioural or disciplinary action will be proportionate and will not replace safeguarding action where safeguarding concerns exist.
- Parents/carers will be involved where appropriate and in accordance with safeguarding considerations.
- Decisions, actions, referrals and outcomes will be recorded appropriately.
- Following significant incidents, leaders will consider lessons for controls, curriculum, training and policy.

16. Concerns or allegations about adults

Any safeguarding concern or allegation relating to an adult working in or on behalf of the Trust must be managed under the Trust Safeguarding and Child Protection Policy and the applicable KCSIE procedures, including the Trust's arrangements for allegations that may meet the harm threshold and for low-level concerns.

Staff must not undertake an informal online safety investigation that could compromise safeguarding, police, LADO or HR processes. Where interim employment measures are considered, suspension will not be automatic and decisions will be made under the Trust's safeguarding and HR procedures.

17. Cyber security and data protection

Detailed technical controls are governed by the Trust Cyber Security Policy and Data Protection Policy. Online safety arrangements will nevertheless support:

- appropriate account and access control;
- timely software and security updating;
- secure device management;
- back-up and recovery arrangements;

- secure handling of personal and special-category data;
- reporting of suspected data breaches or cyber incidents; and
- staff awareness of phishing, scams, credential theft and other relevant threats.

18. Training and awareness

Online safety will form part of safeguarding training and induction, with updates provided as risks, technology and guidance develop. The DSL, Online Safety Lead, relevant leaders, IT/EdTech staff and trustees will receive role-appropriate development. Parents and carers will be supported through Trust communications, guidance and engagement opportunities.

19. Monitoring, assurance and review

The Trust will evaluate online safety arrangements using proportionate evidence such as safeguarding and behaviour themes, filtering and monitoring assurance, training completion, curriculum review, technical/security information and stakeholder feedback. Personal information will be handled in accordance with data protection requirements.

This policy will be reviewed annually and earlier when a material change in legislation, statutory guidance, technology, safeguarding risk or Trust practice requires it.

20. Related Trust documents

- Safeguarding and Child Protection Policy
- Behaviour Policy and Anti-Bullying arrangements
- Staff Code of Conduct
- Acceptable Use Agreements / procedures
- Artificial Intelligence Policy
- Cyber Security Policy
- Data Protection Policy and privacy notices
- Mobile phone procedure / Behaviour Policy provisions
- Managing Allegations and Low-Level Concerns arrangements
- Whistleblowing Policy
- Complaints Policy
- Accessibility and SEND policies where relevant

Appendix A: Online safety incident response

Stage	Required response
1. Concern identified	Protect anyone at immediate risk. Do not investigate prohibited imagery or suspected child protection material.
2. Report	Notify the DSL/deputy DSL immediately for safeguarding concerns. Also notify IT/security where a technical incident requires it.
3. DSL triage	Assess safeguarding risk, consider the child's needs and decide whether external consultation/referral is required.
4. Preserve safely	Retain relevant logs or information lawfully and

Stage	Required response
	proportionately. Do not copy or circulate prohibited imagery.
5. Act	Follow safeguarding, behaviour, HR, data protection or cyber-security procedure as applicable. Safeguarding takes priority where a child may be at risk.
6. Record and support	Record decisions and actions. Provide appropriate support and communication.
7. Review	Consider lessons for education, filtering/monitoring, technical controls, training and policy.

Appendix B: Key external reference points

- Keeping Children Safe in Education 2026
- DfE Filtering and Monitoring: Core Standard
- DfE Mobile Phones in Schools statutory guidance
- UKCIS Sharing nudes and semi-nudes guidance
- DfE Generative AI: Product Safety Standards
- UK Safer Internet Centre and CEOP education resources