Frank Field
Education Trust

Online Safety Policy

Policy Information:

Date prepared	October 2026
Implementation Date	October 2026
Frequency of Review	Bi-Annually
Review Date	October 2028

Approved by CEO:

Cath Green

Approved by Chair of Board:

David Wooff

Frank Field
Education Trust

Contents

Contents 2
1. Introduction 3
2. Purpose and Scope 3
3. Legislative and Regulatory Framework 3
4. Online Safety as Part of Safeguarding 3
5. Roles and Responsibilities 4
5.1 Trust Board 4
5.2 Chief Executive Officer 4
5.3 Principals and Senior Leaders 4
5.4 Designated Safeguarding Leads 4
5.5 ICT Leads and Technical Staff 4
5.6 Staff 4
5.7 Pupils 4
5.8 Parents and Carers 4
6. Education and Awareness 4
7. Artificial Intelligence and Emerging Technologies 5
8. Use of the Internet 5
9. Electronic Communications 5
10. Social Media and Online Platforms 5
11. Filtering and Monitoring 6
12. Remote Learning and Video Conferencing 6
13. Images, Video and Audio Recordings 6
14. Information Security 6
15. Personal Devices 7
16. Cyberbullying 7
17. Personal Data and Privacy 7
18. Incident Reporting and Response 7
19. Reporting Concerns 8
20. Communication, Monitoring and Review 8
21. Related Policies 8

1. Introduction

Frank Field Education Trust recognises that digital technology is an essential part of modern education, communication, and everyday life. Online services, digital devices, social media platforms, and emerging technologies provide significant opportunities to enhance learning, improve communication, and support the effective operation of the Trust's academies.

The Trust also recognises that technology can present safeguarding, wellbeing, privacy, and security risks if it is not used appropriately. Ensuring that pupils can benefit from technology while remaining safe online is therefore an important part of the Trust's wider safeguarding responsibilities.

This policy sets out the Trust's approach to promoting safe and responsible use of technology and establishes a consistent framework for managing online safety across its academies. It applies to pupils, staff, trustees, governors, volunteers, contractors, visitors, and any other person who accesses Trust systems, networks, devices, or digital resources.

2. Purpose and Scope

The purpose of this policy is to support a culture in which technology can be used confidently, responsibly, and safely. The Trust seeks to maximise the educational and operational benefits of digital technology while reducing associated risks and ensuring that effective safeguards are in place.

The policy covers internet access, email and electronic communication, social media, online platforms, filtering and monitoring, remote learning, video conferencing, images and recordings, artificial intelligence, personal devices, cyberbullying, information security and the reporting and management of online safety incidents.

This policy should be read alongside the Trust's Safeguarding and Child Protection Policy, Data Protection Policy, ICT Acceptable Use Policy, Behaviour Policy, Anti-Bullying Policy, Staff Code of Conduct, and information security arrangements.

3. Legislative and Regulatory Framework

This policy has been developed with regard to the Trust's safeguarding, educational and information governance responsibilities. It reflects the Education Act 2002, the Children Act 1989, the Children Act 2004, the Equality Act 2010, the UK General Data Protection Regulation, the Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025, and relevant duties relating to safeguarding and the use of technology.

The Trust also has regard to Keeping Children Safe in Education 2026, Working Together to Safeguard Children, the Prevent Duty guidance, and the Department for Education's digital and technology standards, including the standards for filtering, monitoring, and cyber security.

Technology, online harms, and regulatory expectations continue to evolve. This policy will therefore be reviewed regularly and updated where changes in legislation, statutory guidance, technology, or safeguarding risk make revision necessary.

4. Online Safety as Part of Safeguarding

Online safety is an integral part of safeguarding and child protection. Children increasingly use digital technology for education, social interaction, entertainment and communication both within and beyond the school environment. Although these technologies provide considerable opportunities, they may also expose children to content, contact, conduct, and commercial risks.

Children may encounter inappropriate or harmful content, bullying, harassment, exploitation, grooming, radicalisation, misinformation, scams, or other forms of online harm. Risks may arise through websites, social media, messaging platforms, live-streaming services, online games, artificial intelligence tools, and emerging technologies.

The Trust adopts a whole-school approach that combines education, appropriate supervision, technical controls, staff vigilance, and effective safeguarding procedures. Pupils will be supported to develop the knowledge, resilience and critical thinking skills needed to recognise risk, make informed choices, and seek help.

Any concern that a pupil may be experiencing harm through online activity will be managed in accordance with the Trust's Safeguarding and Child Protection Policy. Where appropriate, information will be shared and referrals made to Children's Social Care, the Police, the Local Authority, or another relevant agency.

5. Roles and Responsibilities

5.1 Trust Board

The Trust Board has overall responsibility for ensuring that appropriate online safety arrangements are established and maintained throughout the Trust. It will seek assurance that suitable policies, training, filtering, monitoring, cyber security, and safeguarding controls are in place and subject to regular review.

5.2 Chief Executive Officer

The Chief Executive Officer is responsible for ensuring that this policy is implemented across the Trust and that appropriate leadership, resources and reporting arrangements support effective online safety practice.

5.3 Principals and Senior Leaders

Principals and senior leaders are responsible for embedding online safety within academy safeguarding arrangements, ensuring that staff and pupils understand the standards expected of them and addressing material weaknesses or incidents promptly.

5.4 Designated Safeguarding Leads

Designated Safeguarding Leads are responsible for responding to online safety concerns that present a safeguarding risk, ensuring that concerns are recorded and assessed appropriately, and making referrals or seeking specialist advice where required.

5.5 ICT Leads and Technical Staff

ICT leads and technical staff support secure systems, filtering and monitoring arrangements, access controls, and incident response. They must promptly escalate activity that may indicate a safeguarding concern and work with safeguarding and senior leadership colleagues.

5.6 Staff

All staff must model safe and professional use of technology, follow Trust policies and academy procedures, maintain appropriate professional boundaries and report concerns without delay. Staff must provide appropriate supervision and must not assume that technical controls remove the need for professional vigilance.

5.7 Pupils

Pupils are expected to use technology responsibly, treat others respectfully, protect personal information, follow acceptable use requirements, and seek help if they encounter content, contact or behaviour that causes concern.

5.8 Parents and Carers

Parents and carers are encouraged to work in partnership with the Trust to support safe and responsible use of technology. The Trust will provide or signpost appropriate information where online safety concerns or emerging risks need to be communicated to families.

6. Education and Awareness

The Trust believes that education is one of the most effective ways to promote online safety. Online safety will be addressed through the curriculum, safeguarding education, pastoral support, and wider academy activity in a way that is appropriate to pupils' age, understanding, needs, and vulnerability.

Pupils will be supported to understand how to protect personal information, maintain healthy online relationships, recognise cyberbullying and exploitation, respond to scams and manipulation, evaluate information critically and manage their digital footprint and online reputation. Teaching will also address online gaming, social media, misinformation, artificial intelligence, and the importance of reporting concerns.

Staff will receive appropriate training and updates so that they understand current online harms, know how to identify and respond to concerns and can support pupils in using technology safely and responsibly.

7. Artificial Intelligence and Emerging Technologies

The Trust recognises that artificial intelligence and other emerging technologies may support teaching, learning, administration, and operational efficiency. Their use must nevertheless be lawful, secure, developmentally appropriate, and consistent with the Trust's safeguarding and educational responsibilities.

Only approved systems may be used for Trust purposes. Before a new system or material use is introduced, the Trust will consider safeguarding, data protection, information security, equality, accessibility, accuracy, bias, intellectual property, age appropriateness, and the need for human oversight. A Data Protection Impact Assessment or other risk assessment will be completed where required.

Staff must not enter identifiable pupil information, safeguarding information, health information, confidential employment information, credentials, or other restricted information into an unapproved or publicly available AI service.

AI-generated output must be checked by an appropriately competent person before it is relied upon, recorded, or communicated. Artificial intelligence may support professional judgement but must not replace safeguarding responsibilities, fair decision-making, or meaningful human oversight. Pupils will be taught to use AI responsibly and in accordance with expectations concerning academic integrity.

8. Use of the Internet

The internet is an important educational resource and supports learning, research, communication, and professional development. Access is provided for legitimate educational and operational purposes and is subject to Trust policies, academy rules, and appropriate supervision.

Users are expected to access suitable material, respect intellectual property rights, and avoid activity that may compromise safeguarding, information security, the learning environment, or the reputation of the Trust. Access may be restricted where misuse occurs, and concerns may be addressed under the relevant behaviour, safeguarding, disciplinary, or acceptable use procedure.

Pupils will be taught that online material may be inaccurate, misleading, manipulated or generated by artificial intelligence. They will be supported to assess sources, distinguish evidence from opinion, and verify information before accepting or sharing it.

9. Electronic Communications

Electronic communication systems support the day-to-day operation of the Trust and provide important channels for learning, collaboration, and communication. Users must communicate lawfully, professionally, and respectfully when using email, messaging services, and other digital platforms.

Personal data and confidential information must be shared only through approved methods and in accordance with the Trust's Data Protection Policy and information security arrangements. Users must take care when selecting recipients, opening links or attachments and responding to unexpected requests for information.

Suspicious emails, phishing attempts, account compromise, scams, or other cyber security concerns must be reported immediately through the Trust's established reporting arrangements.

10. Social Media and Online Platforms

The Trust recognises that social media and online communication platforms form part of everyday life and can support communication, creativity, and participation. They may also create safeguarding, privacy, behavioural and reputational risks.

Pupils will be supported to use social media and online services safely, including through appropriate privacy settings, careful sharing of personal information, respectful communication and an understanding of the permanence and potential reach of online activity.

Staff must maintain appropriate professional boundaries and comply with the Trust's Social Media Policy and Staff Code of Conduct. They must not use personal accounts or informal channels in a way that compromises safeguarding, confidentiality, neutrality, professional standards, or the reputation of the Trust.

Where social media activity gives rise to a safeguarding concern, harmful behaviour or potential illegality, the Trust will take proportionate action under the relevant safeguarding, behaviour, disciplinary, or incident response arrangements.

11. Filtering and Monitoring

The Trust will maintain appropriate filtering and monitoring arrangements to support a safe digital and online environment. Filtering is used to reduce access to illegal, inappropriate, or potentially harmful content. Monitoring is used to help identify activity that may indicate a safeguarding concern, misuse, or security risk.

The Trust Board and senior leadership will seek assurance that arrangements are appropriate. Relevant responsibilities will be allocated to senior leaders; Designated Safeguarding Leads and ICT staff or providers. Filtering and monitoring will reflect the age and needs of pupils, including pupils with special educational needs and disabilities, while avoiding unreasonable interference with teaching and learning.

The effectiveness of filtering and monitoring arrangements will be checked and reviewed regularly and at least annually at Trust or academy level as appropriate. Material changes, recurring concerns, and significant incidents will prompt an earlier review.

Monitoring information will be accessed only by authorised individuals for legitimate safeguarding, security, or operational purposes. Alerts and concerns will be reviewed and escalated in accordance with defined procedures. The Trust recognises that no technical control can remove all risk, so filtering and monitoring will be supported by education, supervision, and staff vigilance.

12. Remote Learning and Video Conferencing

Where remote learning or video conferencing is used, the Trust will use approved platforms configured with appropriate security, privacy, and access controls. Staff will maintain the same standards of safeguarding, professionalism and confidentiality that apply to in-person activity.

Recordings will only be made where there is a defined and authorised purpose. Participants will be given appropriate information, access will be restricted, the recording will be stored on an approved system, and a suitable retention period will be applied.

Pupils and other participants must not record, copy, distribute or publish remote learning sessions without authorisation. Access links, credentials, and meeting information must not be shared with unauthorised individuals.

13. Images, Video and Audio Recordings

The Trust may create and use photographs, video, and audio recordings for educational, safeguarding, administrative, communication and promotional purposes. Their use will be managed in accordance with the Data Protection Policy, relevant privacy notices, safeguarding requirements, and any applicable consent arrangements.

The purpose and lawful basis will be identified before identifiable material is used. Safeguarding risks will be considered before publication, and unnecessary identifying information will not be published alongside images or recordings.

Where consent is relied upon, the Trust will distinguish between different optional uses where appropriate. Withdrawal will apply to future use and will not make earlier lawful processing unlawful or necessarily enable material already distributed, archived, or independently republished to be retrieved.

14. Information Security

The Trust is committed to protecting its systems, networks, devices, and information. Appropriate technical and organisational measures will be implemented in a manner proportionate to the risks presented.

Measures may include secure authentication, multi-factor authentication, role-based access, anti-malware protection, filtering and monitoring, encryption, secure configuration, software updates, logging, resilient backups, and recovery arrangements. Access will be altered or removed promptly when responsibilities change or a user leaves.

All users share responsibility for information security. Passwords and authentication methods must be protected, approved systems must be used, and actual or suspected compromise, loss or misuse must be reported immediately.

15. Personal Devices

The use of personal devices by pupils and staff will be managed through Trust requirements and academy rules. Permission to use a personal device does not permit unrestricted access to Trust information or systems.

Where personal devices are allowed, users must ensure that their use does not create safeguarding, behaviour, privacy, or security risks. Devices must not be used for unauthorised recording or to bypass filtering, monitoring, supervision, or other controls.

Personal data must not be stored on or accessed through a personal device unless the arrangement has been expressly approved and the required security measures are in place.

16. Cyberbullying

The Trust does not tolerate cyberbullying or any form of online abuse. Cyberbullying may occur through social media, messaging services, websites, gaming environments, shared documents or other digital services, and its impact may continue beyond the school day.

Reports will be taken seriously and considered under the Trust's safeguarding, behaviour, and anti-bullying arrangements. The response will take account of the impact on those involved, any wider safeguarding risk, the need to preserve evidence and whether external advice or referral is required.

Appropriate support will be provided to affected pupils. Where conduct may constitute a criminal offence or place a child at risk of significant harm, the Trust may refer the matter to the Police, Children's Social Care, or another appropriate agency.

17. Personal Data and Privacy

The Trust processes personal data as part of its educational, safeguarding, employment, and administrative functions. Personal data will be collected, used, stored, shared, retained, and disposed of in accordance with the Data Protection Policy, Records Management and Retention Schedules Policy and applicable privacy notices.

Users must protect personal information and must not access or disclose information without authority. An actual or suspected personal data breach must be reported immediately under the Trust's breach reporting arrangements.

Monitoring of Trust systems will be necessary, proportionate, and transparent. Access to monitoring information will be limited to authorised individuals, and records will be retained only for as long as required for the relevant safeguarding, security, investigation, or legal purpose.

18. Incident Reporting and Response

Online safety incidents may include cyberbullying, harmful content, online abuse, exploitation, misuse of technology, unauthorised access, malicious software, account compromise, inappropriate communication, unlawful activity, or any other online behaviour presenting a safeguarding or security risk.

Incidents will be recorded, assessed, and managed according to their nature and seriousness. Safeguarding staff, senior leaders, ICT personnel, information governance staff, and other relevant professionals will work together where necessary. The response may include containment, preservation of evidence, support for affected individuals, restrictions on access, disciplinary or behaviour action and referral to an external agency.

Where an incident involves personal data, the Data Protection Policy and Personal Data Breach Procedure will also apply. Where it raises a safeguarding concern, the Safeguarding and Child Protection Policy will apply. Lessons identified from incidents will be used to improve controls, education, and staff awareness.

19. Reporting Concerns

Any online safety concern, inappropriate online behaviour, suspected safeguarding risk or cyber security incident must be reported without delay. Concerns may be reported to a teacher, line manager, senior leader, Designated Safeguarding Lead, Principal, ICT lead, or another appropriate member of staff.

The Trust will take concerns seriously and will respond in a child-centred, proportionate, and timely manner. Where a concern relates to the conduct of a member of staff, the Trust's procedure for managing safeguarding concerns or allegations about adults will be followed.

Where appropriate, the Trust may seek advice or make a referral to Children's Social Care, the Police, Prevent partners, the Local Authority, the Information Commissioner's Office, the National Cyber Security Centre, or another relevant organisation.

20. Communication, Monitoring and Review

This policy will be made available to staff, trustees and governors and will be communicated to pupils and parents in an age-appropriate and accessible way. Acceptable use expectations, reporting routes and the fact that Trust network and internet use may be monitored will be explained to users.

Implementation will be monitored through safeguarding review, staff training, online safety education, incident reporting, filtering, and monitoring reviews, cyber security activity, audit, and other appropriate assurance processes.

The Trust Board will receive suitable assurance about online safety arrangements. This policy will be reviewed annually and sooner where legislation, statutory guidance, technology, organisational arrangements, or safeguarding risks materially change.

21. Related Policies

This policy should be read alongside the following Trust policies and procedures:

- Safeguarding and Child Protection Policy
- Data Protection Policy
- Records Management and Retention Schedules Policy
- ICT Acceptable Use Policy
- Social Media Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Surveillance and CCTV Policy
- Information Security and Cyber Incident procedures
- Relevant privacy notices and acceptable use agreements.