



MULTI ACADEMY TRUST

Trust Online Safety Policy

Date published: September 2026

Date of next review: September 2027

1. Introduction

Inspiring Learners Multi Academy Trust recognises that digital technologies play a significant role in education, communication, safeguarding and everyday life. The Trust is committed to promoting the safe, responsible and positive use of technology whilst protecting pupils, staff and the wider school community from potential online harms.

The Trust recognises that digital technologies provide significant opportunities for learning, creativity, collaboration, accessibility and communication. However, the Trust also acknowledges that online technologies present safeguarding, wellbeing, security and privacy risks which must be appropriately managed.

Online safety is recognised as a safeguarding responsibility and forms an integral part of the Trust's wider commitment to safeguarding and promoting the welfare of pupils.

2. Scope

This policy applies across Inspiring Learners Multi Academy Trust and all member schools.

The policy applies to all members of the Trust community, including:

- Pupils
- Staff
- Volunteers
- Trustees
- Governors
- Contractors
- Parents and carers
- Visitors
- Community users authorised to access Trust systems

This policy applies to the use of digital technologies and online services both within and outside Trust premises where such use affects members of the Trust community or relates to Trust business.

3. Online Safety as a Safeguarding Responsibility

The Trust recognises that online safety is a safeguarding responsibility and that effective online safeguarding requires a whole-Trust approach.

All staff have a responsibility to promote safe and responsible technology use, educate pupils about online risks and opportunities, and report concerns in accordance with safeguarding procedures.

The Trust recognises that online risks do not affect all pupils equally. Some pupils may be more vulnerable to online harms due to their:

- Age
- Special Educational Needs and Disabilities (SEND)
- Communication needs
- Mental health needs
- Safeguarding concerns
- Family circumstances
- Previous experiences

The Trust will take a proportionate and individualised approach to supporting pupils who may be at increased risk online and, where appropriate, will work in partnership with families and external agencies to promote safe, responsible and positive use of technology.

4. Roles and Responsibilities

Trustees and Governors

Trustees are responsible for approving this policy and monitoring its effectiveness.

The Trust Board and Local Governing Bodies will receive appropriate assurance regarding:

- online safety arrangements
- filtering and monitoring systems
- online safety incidents and trends
- staff training and awareness
- emerging technologies and associated risks

The Safeguarding Trustee and Safeguarding Governor will maintain regular contact with relevant safeguarding, digital and online safety leaders and report to the appropriate governance body.

Headteachers and Senior Leaders

Headteachers and senior leaders are responsible for ensuring that:

- online safety is embedded within safeguarding practice
- staff understand their responsibilities
- appropriate procedures are in place to manage incidents
- online safety leaders receive suitable training and support
- staff and pupils receive appropriate guidance regarding artificial intelligence and emerging technologies

Designated Safeguarding Lead

The Designated Safeguarding Lead (DSL) will maintain an awareness of online safety risks and ensure that online safety concerns are managed in accordance with safeguarding procedures.

This includes awareness of:

- grooming and exploitation
- online abuse
- cyberbullying
- deepfakes and AI-generated imagery
- AI-enabled abuse and harassment
- misinformation and manipulation
- sharing of personal data

They will also maintain records of online safety incidents.

Online Safety Lead

The Online Safety Lead will:

- lead the development and review of online safety arrangements
- promote good practice across the school and support the implementation of Trust online safety expectations
- provide guidance where needed
- monitor developments in online safety, artificial intelligence and emerging technologies
- report regularly to senior leaders and governors

Technical Staff

Technical staff are responsible for ensuring that:

- technical infrastructure remains secure
- appropriate filtering and monitoring systems are maintained
- monitoring arrangements are regularly reviewed
- access to Trust systems is appropriately managed
- security incidents are reported and addressed

Teaching and Support Staff

Staff are responsible for:

- following the Staff Acceptable Use Policy
- maintaining awareness of online safety risks
- following Trust policies and procedures
- reporting concerns appropriately
- embedding online safety within teaching and learning
- promoting safe, responsible and ethical use of technology, including artificial intelligence
- remaining vigilant to emerging risks associated with AI-generated content and online technologies

Pupils

Pupils are expected to:

- follow the Pupil Acceptable Use Policy
- act safely and responsibly online
- report concerns appropriately
- understand the risks and opportunities associated with digital technologies
- develop an awareness of artificial intelligence, bias, misinformation and ethical technology use

Parents and Carers

The Trust recognises the important role of parents and carers in supporting children to use technology safely and responsibly.

Parents and carers are encouraged to work in partnership with schools and support online safety messages at home.

5. The Four Cs of Online Risk

The Trust recognises that online harms may be categorised using the Four Cs framework identified within Keeping Children Safe in Education.

Content Risks: Content risks arise when users are exposed to harmful, inappropriate or misleading material online.

Examples include:

- Extremist, hateful or discriminatory content
- Misinformation and disinformation
- AI-generated content and deepfakes
- Harmful online communities
- Content promoting self-harm, eating disorders or unhealthy body image
- Misogynistic, extremist or harmful influencer content
- Manipulative advertising
- Nudification apps
- Image abuse
- Algorithm-driven echo chambers
- Age-restricted content

Contact Risks: Contact risks occur through interaction with others online.

Examples include:

- Grooming
- Coercion and manipulation
- Child criminal exploitation
- Child sexual exploitation
- Harmful communication
- Unsafe interaction with AI systems and chatbots
- Requests for personal information
- Pressure to move conversations to private platforms

Conduct Risks: Conduct risks relate to behaviour online.

Examples include:

- Cyberbullying
- Harassment
- Exclusion
- Sharing harmful content
- Creation or distribution of manipulated images
- AI-generated abuse materials
- Inappropriate comments or posts
- Failure to understand the permanence of digital communication

Commerce Risks: Commerce risks involve financial harm or exploitation.

Examples include:

- Scams
- Fraud
- Phishing
- Gambling
- Loot boxes
- In-app purchases
- Financial exploitation

The Trust recognises that online harms may overlap multiple categories and that effective online safety requires a proactive and preventative approach.

6. Online Safety Education

Online safety education is an essential part of the Trust's safeguarding provision.

6.1 Pupils

The Trust is committed to providing a progressive, age-appropriate programme of online safety education which develops pupils' knowledge, understanding and resilience.

Online safety education will be delivered through:

- Computing
- PSHE
- Assemblies
- Pastoral activities

- Cross-curricular learning opportunities

Planning will be informed by:

- DfE Teaching Online Safety in Schools guidance
- Education for a Connected World Framework
- Project Evolve and other recognised resources

Pupils will be taught about:

- Online risks and opportunities
- Digital wellbeing
- Critical thinking
- Safe use of search engines
- Misinformation and disinformation
- Algorithms and online influence
- Advertising and persuasive design
- Privacy and personal data
- Reporting concerns
- Artificial intelligence and emerging technologies

The Trust recognises that some pupils may require additional support and interventions to help them understand and manage online risks effectively.

Particular consideration will be given to pupils with SEND and neurodivergent pupils who may be more vulnerable to manipulation, coercion, misinformation or online exploitation.

6.2 Staff

The Trust recognises that staff play a vital role in promoting online safety and safeguarding pupils from online harms.

All staff will receive appropriate online safety training and updates to ensure that they remain aware of current and emerging risks, relevant legislation and Trust procedures.

This will include:

- Online safety as part of staff induction
- Annual safeguarding updates relating to online safety
- Annual online safety training
- Updates regarding emerging technologies and trends.
- Awareness of artificial intelligence and AI-related safeguarding risks.
- Guidance relating to filtering and monitoring arrangements.
- Cyber security awareness and good practice.

Staff will be encouraged to share good practice, seek support when required and engage with professional learning opportunities that support the development of their online safety knowledge and skills.

The Online Safety Lead and other designated staff will attend specialised training and provide advice, guidance and support to colleagues where appropriate.

6.3 Parents and Carers

The Trust recognises that parents and carers play a crucial role in helping pupils develop safe, responsible and positive online behaviours.

Schools will work in partnership with parents and carers to promote online safety and increase awareness of current and emerging online risks.

The Trust may support parents and carers through:

- Newsletters and written communications.
- Parent information sessions and workshops.
- Information available through school websites and communication platforms.
- Signposting to trusted online safety resources.
- Awareness campaigns and national events such as Safer Internet Day.
- Updates relating to emerging technologies, social media trends and artificial intelligence.

The Trust encourages parents and carers to work collaboratively with schools in supporting safe and responsible technology use both at home and in school.

6.4 Governors and Trustees

Governors and trustees have an important role in ensuring that appropriate online safety arrangements are in place across the Trust.

To support this responsibility, governors and trustees will be provided with opportunities to develop their online safety awareness and understanding.

This may include:

- Trust-provided safeguarding and online safety training
- external professional development opportunities
- briefings relating to changes in legislation and guidance
- updates regarding emerging technologies and online trends
- information relating to filtering and monitoring arrangements

Training will support governors and trustees in providing effective challenge, support and strategic oversight.

6.5 Wider Community

The Trust recognises the value of working with the wider community to promote safe, responsible and positive use of technology.

Where appropriate, schools may:

- Provide information and guidance to grandparents and other family members.
- Share expertise with other educational settings.
- Support community organisations, childcare providers and youth groups.
- Participate in local and national online safety initiatives.

The Trust is committed to contributing positively to the wider online safety community and supporting the development of digitally safe and informed communities.

7. Online Safety and the Use of Technology in Early Years

In line with the Early Years Foundation Stage (EYFS) Statutory Framework (September 2026), our schools ensure that any use of screens or digital technology in the Early Years is purposeful, age-appropriate and supports children's learning and development. Technology is used to enhance, not replace, high-quality interactions, communication, active play and real-world experiences.

The statutory framework requires providers to have regard to the Department for Education's guidance on children's screen use in early years settings, which advises that screen time for children aged two to five should be limited to **no more than one hour per day, with less being preferable**.

Staff carefully consider children's developmental needs when using technology and actively promote safe, healthy and balanced digital habits. We work closely with families to support children's wellbeing and ensure that digital experiences are appropriate, supervised and contribute positively to learning and development.

8. Artificial Intelligence and Emerging Technologies

The Trust recognises that artificial intelligence and emerging technologies will form an increasingly significant part of pupils' futures.

AI technologies may support:

- Learning
- Accessibility
- Creativity
- Personalisation
- Administrative efficiency

The Trust also recognises the unique risks associated with AI technologies, including:

- Deepfakes
- AI-generated intimate imagery
- Impersonation
- Misinformation
- Harmful chatbot interactions
- Emotional dependence on AI systems
- Bias and discrimination
- Privacy concerns
- Academic integrity concerns

The Trust acknowledges that AI technologies continue to evolve rapidly and that new risks may emerge. Online safety arrangements will be reviewed regularly to ensure that the Trust remains responsive to developments in AI and other emerging technologies.

The use of AI technologies is further governed through the Trust's Artificial Intelligence Policy.

9. Filtering and Monitoring

The Trust will maintain appropriate filtering and monitoring systems to support safeguarding and reduce exposure to harmful content.

All Trust-owned devices that access online services will be subject to filtering and monitoring arrangements.

The Trust will ensure:

- Appropriate filtering levels are applied.
- Monitoring arrangements are proportionate and effective.
- Logs are reviewed regularly.
- Clear procedures exist for reporting concerns.
- Appropriate access arrangements are in place for staff, volunteers and other authorised users.

The effectiveness of filtering and monitoring arrangements will be reviewed at least annually by the designated senior leader responsible for filtering and monitoring, with support from the Designated Safeguarding Lead and technical staff in accordance with The DfE Filtering and Monitoring Standards.

10. Mobile Devices and Network Access

The Trust recognises that mobile and internet-enabled devices form an important part of modern life and learning.

The use of such devices within Trust settings will be managed in accordance with Trust policies and school procedures.

School-owned devices will remain subject to Trust filtering, monitoring and safeguarding arrangements.

Access to Trust networks and systems will be restricted to authorised users and approved devices.

11. Communication and Online Presence

Images and Videos

The Trust recognises that photographs and videos form an important part of school life and celebration.

The Trust will:

- obtain and record appropriate consent
- review permissions regularly
- ensure images are appropriate
- protect pupil identities
- avoid publishing unnecessary personal information

Parents and carers may take photographs at school events, where permitted, but should respect the privacy of others and avoid publishing images of other pupils online without permission.

Social Media

The Trust will ensure that official social media accounts are authorised and appropriately managed.

Staff must use social media in accordance with the Trust Social Media Policy.

Pupils will not routinely be provided with access to social media platforms for educational purposes unless appropriate safeguards are in place.

Where concerns arise regarding a pupil's use of social media, appropriate safeguarding action will be considered.

Digital Communications

Pupils may be provided with age-appropriate email and communication tools to support learning.

Staff must communicate with pupils and parents only through approved Trust systems and in a professional manner.

12. Data Protection and Information Security

The Trust recognises that online safety, cyber security and data protection are closely linked.

The Trust will:

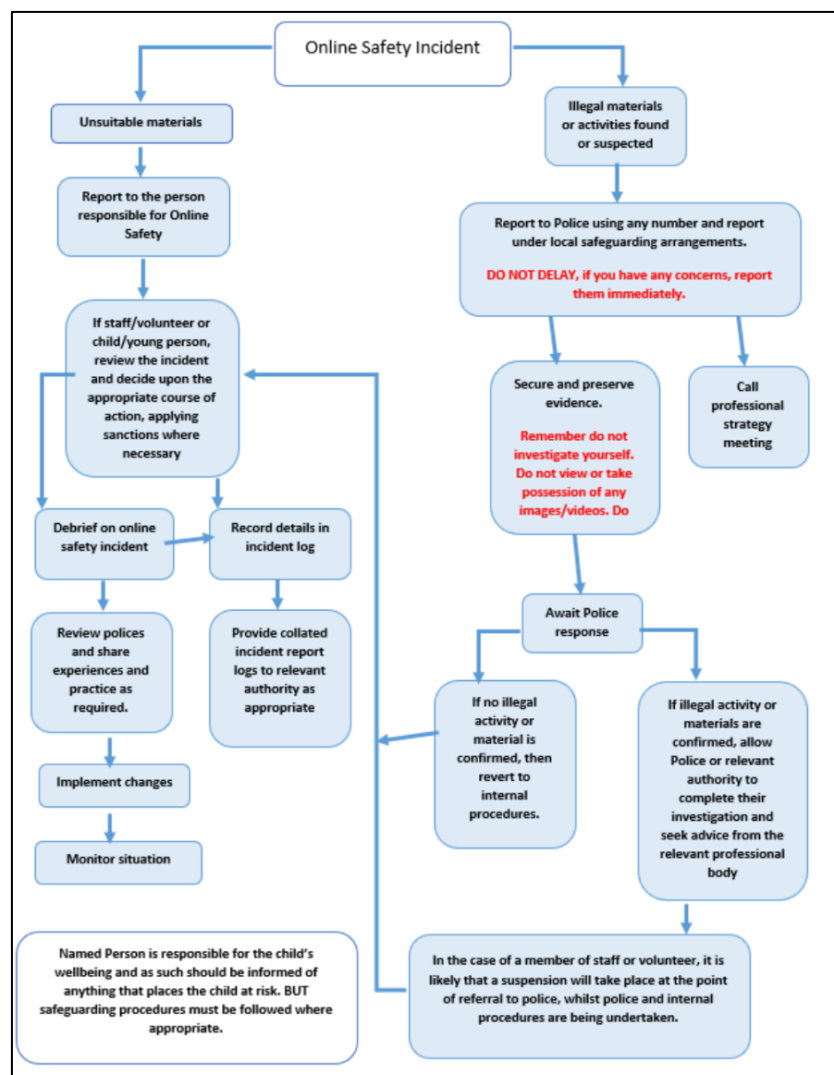
- maintain appropriate technical and organisational security measures
- promote the safe handling of personal information
- provide staff with appropriate training
- respond appropriately to data breaches
- consider data protection implications when implementing new technologies

The Trust recognises that cyber security forms an important part of safeguarding, operational resilience and information governance.

Appropriate procedures will be maintained for granting, reviewing and removing access to Trust systems. Access may be provided to prospective employees before their official start date where this is necessary to prepare for their role and has been appropriately authorised.

Detailed arrangements are contained within the Trust's Data Protection Policy and Trust Information Security Policy and associated procedures.

13. Responding to Online Safety Incidents



The Trust expects all members of the community to act as responsible users of technology. However, incidents may occur through misuse, misunderstanding or deliberate actions. Online safety concerns should be reported without delay and managed in accordance with safeguarding procedures.

Investigations will be conducted fairly, proportionately and in accordance with relevant legislation and Trust procedures.

Where appropriate, concerns may result in:

- Internal disciplinary action
- Safeguarding intervention
- Involvement of external agencies
- Police involvement

The Trust recognises that online safety incidents frequently occur outside school hours and beyond school premises.

Where such incidents affect the safety, wellbeing or education of pupils, or impact the wider school community, appropriate action may be taken.

Online incidents occurring outside school will be managed in conjunction with:

- Safeguarding procedures
- Behaviour procedures
- Anti-Bullying procedures
- Relevant legislation

Parents and carers will be involved where appropriate.

14. Monitoring and Review

The Trust will monitor the effectiveness of this policy through:

- Incident monitoring
- Filtering and monitoring reviews
- Staff feedback
- Pupil voice activities
- Parent and carer feedback
- Governance oversight

This policy will be reviewed regularly and at least annually to ensure that it remains effective and reflects current legislation, guidance and emerging risks.

15. Associated Policies and Procedures

- Trust Child Protection and Safeguarding Policy
- Trust Acceptable Use Policy (Staff and Pupil)
- School Behaviour Policy
- School Kindness and Anti-Bullying Policy
- Trust Staff Code of Conduct
- Trust Data Protection Policy
- Trust Social Media Policy
- Trust Artificial Intelligence Policy