



Digital Technology, IT and Online Safety Policy

Policy Owner:	Chief Operating Officer
Approved by:	Executive Team
Last reviewed:	July 2026
Next review due by:	July 2029

Due to the evolving nature of The CAM Academy Trust, procedures behind this policy will be reviewed and amended accordingly to reflect changes.

At the heart of our work lie the six core principles of The CAM Academy Trust. These drive everything that we do.



EXCELLENCE

We insist on the very best. This means setting out a clear entitlement to excellence for all our young people. For us, excellence comes from the highest standards of curriculum, teaching and pupil support. We adopt a mindset that keeps us striving for better.



COMPREHENSIVE EDUCATION

We are proud to educate pupils of all abilities, backgrounds and needs. Inclusive schools are vibrant communities, that are richer for their diversity. We value fairness and social equity.



BROAD EDUCATION

Our pupil entitlement offers more than just academic success. A broad education develops confidence, creativity and character. The wider experiences and opportunities offered in our schools mean that our pupils have more choice and agency.



COMMUNITY

We prioritise our civic duty. Our schools are at the heart of their local communities. We draw on the best that our local area has to offer and work with community leaders to help our schools thrive.



PARTNERSHIP

Together we achieve more than we can alone. We deeply value the partnerships we have with our families. CAM plays an active role in our communities, our region and the wider education system. We share and build connections to help make the system better.



INTERNATIONAL

We think beyond borders; we value diversity. We prepare pupils to thrive in a global society, promoting cultural understanding and awareness of the wider world.

Everyone has a role in online safety. Safeguarding is everyone's responsibility, and every member of the Trust community is expected to contribute to a culture in which technology is used safely, responsibly, ethically and in a manner that promotes the welfare, dignity and rights of all.

1. Purpose

The CAM Academy Trust recognises that digital technology is fundamental to education, communication and the effective operation of our academies. Technology provides significant opportunities to enhance learning, improve accessibility and strengthen collaboration, whilst also presenting safeguarding, security and operational risks.

The Trust is committed to ensuring that all members of our community can access technology safely, responsibly and securely.

Online safety is an integral element of safeguarding and promoting the welfare of children. The Trust adopts a child-centred approach and recognises that technology is a significant component in many safeguarding and wellbeing issues.

This policy establishes the Trust's strategic approach to IT, cyber security and online safety and should be read alongside the Trust Child Protection and Safeguarding Policy, Data Protection Policy, Information Security Policy, Behaviour Policy and Artificial Intelligence Policy.

2. Scope

This policy applies to:

- Trustees
- Members
- Local Advisory Boards
- Employees
- Agency staff
- Volunteers
- Contractors
- Pupils
- Visitors
- Third party providers

It applies whenever Trust systems, networks, devices, cloud services or digital platforms are used, whether on Trust premises or remotely.

3. Legislative framework

This policy has regard to:

- Keeping Children Safe in Education
- Department for Education Filtering and Monitoring Standards
- Working Together to Safeguard Children
- Data Protection Act 2018 and UK GDPR

- Prevent Duty
- Computer Misuse Act
- Education Act 2002
- UK Safer Internet Centre guidance
- National Cyber Security Centre guidance

4. Principles

The Trust will:

- safeguard children and vulnerable adults online
- provide secure and resilient IT systems
- promote responsible digital citizenship
- encourage positive and inclusive use of technology
- protect personal information
- provide age-appropriate online safety education
- respond effectively to safeguarding and cyber incidents
- continuously review filtering and monitoring arrangements

5. Governance and responsibilities

Trust Board

The Trust Board has strategic responsibility for:

- assurance of statutory compliance
- oversight of online safety and cyber security
- receiving annual reports regarding filtering, monitoring and significant incidents
- ensuring sufficient resources are available

Chief Executive Officer

The CEO is responsible for ensuring Trust-wide implementation of this policy.

Trust Executive Team

Responsible for operational delivery, risk management and ensuring consistent implementation across all staff.

Trust IT Team

Responsible for:

- cyber security
- network resilience
- identity and access management
- secure infrastructure
- filtering and monitoring systems
- technical investigations

- business continuity
- Providing technical advice to school leaders and DSLs

Trust Safeguarding Lead and school level Designated Safeguarding Leads (DSLs)

Responsible for:

- online safeguarding strategy
- oversight of filtering and monitoring alerts
- responding to online safeguarding concerns
- staff guidance and training
- analysing incident trends
- ensuring safeguarding procedures are followed

Principals

Responsible for:

- Effective implementation of this policy within their school
- promoting a culture of safe technology use
- ensuring staff receive appropriate training
- ensuring online safety education is delivered
- working with safeguarding and IT teams to manage risks

6. Responsibilities of the Trust community

6.1 All Employees

All employees have a responsibility to contribute to a culture of safe, responsible and professional use of technology. Technology and automated systems support safeguarding but do not replace professional curiosity or professional judgement.

Employees will:

- recognise that online safety is an integral part of safeguarding
- comply with this policy and the Trust Acceptable Use Agreement
- maintain appropriate professional boundaries in all digital communications
- protect confidential and personal information
- report safeguarding concerns, cyber security incidents or suspected misuse immediately
- model positive digital behaviours for pupils
- participate in mandatory online safety, safeguarding and cyber security training
- use Trust technology and digital services responsibly and lawfully.
- Employees should understand that safeguarding responsibilities extend to online behaviours and activities both within and outside the workplace where these may affect pupils, colleagues or the reputation of the Trust.

6.2 Teaching staff

Teaching staff have an additional responsibility to promote safe and responsible technology use through the curriculum and wider academy life.

Teaching staff will:

- embed online safety education into learning where appropriate
- support pupils in developing digital literacy and critical thinking skills
- supervise the use of digital technologies appropriately
- reinforce Trust expectations regarding acceptable use
- respond appropriately to online safety concerns and report them in accordance with safeguarding procedures.

6.3 Support staff

Support staff are often trusted adults for pupils and play an important role in safeguarding.

Support staff will:

- remain vigilant to online safety concerns
- report concerns immediately
- follow Trust procedures for the use of digital technologies
- support pupils in using technology safely where appropriate.

6.4 Pupils

Pupils are expected to become safe, responsible and respectful digital citizens.

Pupils will:

- comply with the Trust Pupil Acceptable Use Agreement
- use Trust technology appropriately
- respect the rights, privacy and dignity of others
- protect their passwords and personal information
- report anything online that makes them feel unsafe, uncomfortable or concerned
- understand that misuse of technology may result in disciplinary action.

6.5 Parents and Carers

The Trust recognises that parents and carers play a vital role in supporting children to use technology safely.

Parents and carers are encouraged to:

- support the Trust's online safety messages at home
- encourage safe and responsible use of digital technology
- monitor age-appropriate access to online services
- work in partnership with academies when concerns arise
- familiarise themselves with Trust Acceptable Use expectations.

6.6 Visitors, volunteers and contractors

All visitors, volunteers and contractors using Trust systems or devices must:

- comply with Trust policies and acceptable use requirements
- protect confidential information
- report safeguarding or cyber security concerns immediately
- use Trust technology only for authorised purposes.

The Trust encourages a positive reporting culture in which staff and pupils feel confident to raise concerns about online safety, cyber security or technology misuse without fear of blame or reprisal. Early reporting enables effective safeguarding and supports continuous improvement.

7. Online Safety

The Trust recognises four categories of online risk.

Content

Exposure to harmful, illegal or inappropriate material including:

- extremism
- pornography
- hate content
- self-harm material
- misinformation
- AI-generated content such as deep fakes

Contact

Risks arising from interaction with others including:

- grooming
- exploitation
- radicalisation
- sextortion
- Coercion

Conduct

Risks arising from online behaviour including:

- cyberbullying
- harassment
- sharing images
- impersonation
- deepfakes
- misuse of AI

Commerce

Financial and commercial risks including:

- Scams
- ransomware
- phishing
- gambling
- fraud
- subscription traps

8. Filtering and monitoring

The Trust operates age-appropriate filtering and monitoring across its managed networks and devices. The Trust uses Netsweeper to support compliance with Department for Education Filtering and Monitoring Standards.

Filtering and monitoring arrangements will:

- block illegal content
- reduce access to harmful material
- identify safeguarding concerns
- support investigation of incidents
- provide appropriate access for educational purposes

Filtering and monitoring arrangements will be reviewed at least annually and whenever significant changes, incidents occur or when DfE guidance changes. Any safeguarding concerns identified through filtering or monitoring will be managed in accordance with the Trust Child Protection Safeguarding Policy.

Reviews will consider:

- effectiveness
- overblocking
- underblocking
- accessibility
- educational impact

9. Cyber Security

The Trust will maintain proportionate cyber security measures including:

- multi-factor authentication
- secure password standards
- endpoint protection
- encryption
- regular patching
- secure backups
- vulnerability management

- incident response planning
- conditional access

All users have a responsibility to protect Trust systems and report suspected security incidents immediately.

10. Digital professional conduct

All staff are expected to model safe, responsible and professional online behaviour.

Staff must:

- use Trust systems appropriately
- maintain professional boundaries
- protect confidential information
- report safeguarding concerns immediately
- use approved communication channels
- comply with Trust Acceptable Use Agreements

11. Digital education

Schools will provide age-appropriate education that develops pupils':

- digital literacy
- media literacy
- critical thinking
- online resilience
- understanding of misinformation
- understanding of AI technologies
- cyber awareness
- responsible digital citizenship

12. Personal data

All processing of personal data will comply with UK GDPR and the Trust Data Protection policy. Personal information must only be stored on approved Trust systems and must never be shared or stored using unauthorised services.

13. Mobile devices and remote working

Trust devices and approved personal devices must be used securely.

Users must:

- protect devices with passwords or biometrics
- report loss immediately
- use secure networks where possible
- avoid storing confidential information locally
- follow Trust remote working guidance

14. Social Media

Staff must maintain appropriate professional boundaries. Official Trust social media accounts will only be managed by authorised staff.

Personal social media activity must not undermine professional responsibilities or the reputation of the Trust. This is set out within the Trust Child Protection Safeguarding Policy and Staff Code of Conduct.

15. Artificial Intelligence (AI)

The Trust recognises that Artificial Intelligence forms part of the digital landscape. The use of AI technologies must comply with this policy, the Trust Artificial Intelligence Policy and all safeguarding, data protection and information security requirements.

16. Incident Management

Online safety, safeguarding and cyber security incidents must be reported immediately. Safeguarding incidents will be managed in accordance with the Trust Child Protection Safeguarding Policy. Cyber security incidents will be managed through Trust IT incident response procedures.

Classifications of these are:

- Safeguarding incidents - Managed through the Child Protection and Safeguarding Policy.
- Cyber security incidents - Managed through Trust IT incident response procedures.
- Data breaches - Managed through the Data Protection Policy.
- Behaviour incidents - Managed through Behaviour and Relationships policies.

17. Training

All staff will receive regular training appropriate to their role covering:

- online safety
- cyber security
- phishing
- safeguarding
- digital professionalism
- filtering and monitoring
- artificial intelligence awareness

18. Monitoring and review

The Trust will undertake annual reviews of:

- filtering effectiveness
- monitoring arrangements
- safeguarding trends
- cyber incidents

- staff training compliance
- emerging technologies and risks

The Trust Board will receive appropriate assurance that this policy remains effective and compliant with statutory guidance.

This policy will be reviewed every three years, or sooner if there are any legislative changes. At each review the policy will be approved by the Executive Team.

This policy should be read and used in conjunction with the Trust Child Protection & Safeguarding Policy, IT Acceptable Use Agreement, AI Policy and Data Protection Policy.