Rise
Flourish & Succeed

Rise Multi Academy Trust: Online Safety Policy 2025

Rise
Flourish & Succeed

Date of Policy: 3rd September 2025

Approved by the Trust Board: 3rd September 2025

Signed:

Introduction

The Rise Multi Academy Trust Online Safety Policy is designed to protect all members of the school community in relation to digital technology use, both inside and outside the classroom. The policy aligns with statutory guidance including Keeping Children Safe in Education (KCSIE 2025), Teaching Online Safety in Schools guidance, and the UKCIS Education for a Connected World framework. It integrates online safety with our safeguarding and child protection practices.

This policy builds on national guidance and our local needs. The school uses dynamic risk assessment to adapt to new challenges such as emerging technologies (e.g., AI) and trends seen among pupils and families.

Aims

This policy aims to:

- Set clear expectations for safe, responsible and respectful online behaviour.
- Ensure staff, pupils, parents and carers understand their roles in maintaining online safety.
- Provide guidelines on appropriate use of digital technologies, including AI.
- Promote digital literacy, resilience and awareness of online risks (4Cs: Content, Contact, Conduct, Commerce).
- Establish procedures for handling incidents, reporting and escalation.

Scope

This policy applies to all members of the Rise Multi Academy Trust community – staff, governors, volunteers, contractors, pupils, parents, and visitors – who have access to or use the school's technology, networks, systems, or data. It also covers personal devices brought into school.

Roles and Responsibilities

- The **Designated Safeguarding Lead (DSL)** has overall responsibility for online safety, including filtering and monitoring.

- **Deputy DSLs, curriculum leads (e.g., PSHE, Computing), the network manager, and the senior leadership team** all play roles in maintaining and reviewing online safety measures.

- **All staff** must follow the Acceptable Use Policy (AUP), report concerns promptly and and act as role models for safe digital behaviour.

- **Pupils** are expected to follow the SMART online safety rules, report unsafe content, and use digital technologies responsibly.

- **Parents and carers** are encouraged to engage with online safety training and guidance provided by the school.

Teaching and Learning

The internet is a vital tool for learning, research, and communication. We teach pupils to use it responsibly by ensuring they:

- Use the internet responsibly and understand acceptable/unacceptable behaviours.
- Know how to evaluate online content for accuracy and reliability.
- Report unpleasant or unsafe content immediately.
- Recognise issues related to copyright, intellectual property, and AI-generated content.
- Are aware of the potential dangers as well as opportunities online (following the 4Cs model: Content, Contact, Conduct, Commerce).

Online safety education is embedded across the curriculum, including Computing, PSHE, and other subjects where appropriate.

Internet Access and Use

- Internet access in school is designed for safe pupil use, with age-appropriate filtering and supervision.
- Children must not have unsupervised access to the internet. For younger pupils, searches and online resources are pre-checked by staff.
- All usernames and passwords must remain private and secure.
- Use of the school's internet for personal financial gain, gambling, or offensive material is strictly prohibited.
- Staff and pupils are expected to use polite and professional language in all communications.

Filtering and Monitoring

- The school works with AIT and other technical providers to ensure robust filtering and monitoring systems.
- All online activity is monitored and recorded in the ICT violations register, reviewed regularly by the DSL and senior leadership.
- Inappropriate content or attempts to bypass filters must be reported immediately.
- Staff and pupils are informed that all activity may be logged and reviewed for safety purposes.

Publishing Pupils' Images and Work

- No pupil's photo, video or work will be published without written parental consent.
- Surnames will not be published alongside images.
- We take care to ensure images are appropriate, respect privacy, and are used only for school-approved purposes.
- The school website is maintained with oversight from senior leaders to ensure content is accurate and complies with safeguarding, copyright, and data protection regulations.

Email and Communication Systems

- Pupils and staff must not reveal personal information (their own or others') via email or online messaging.
- Incoming emails are treated with caution, and suspicious attachments or links are not opened.
- Email to external bodies is usually sent from official staff accounts.

Managing Emerging Technologies (incl. AI)

- New technologies (e.g., AI tools, video conferencing, cloud-based platforms) are assessed for educational benefit and risk before implementation.
- Pupils are educated about AI ethics, reliability, and risks such as plagiarism or deepfake content.
- Use of AI for cheating or inappropriate purposes is prohibited and addressed under the Behaviour Policy.
- Mobile phones and smartwatches are not permitted unless explicitly authorised (e.g., for medical or safety reasons) and must be stored securely during school hours.

Social Media

- The school's social media channels are managed by designated staff.
- Pupils are educated on the dangers of sharing personal data online.
- Inappropriate online behaviour by pupils or parents will be addressed under the Behaviour Policy or reported to authorities if necessary.

Handling Online Safety Incidents

- Online safety concerns are treated as safeguarding matters and dealt with in line with the Safeguarding and Child Protection Policy.
- All incidents are reported to the DSL and logged.
- Serious breaches may result in withdrawal of access, disciplinary measures, or referral to external agencies (e.g., Police, CEOP).
- Staff concerns about other staff misuse must be reported to the Headteacher or, if appropriate, the Chair of Governors.

Home Learning

- Online home learning (e.g., Microsoft Teams) follows government guidelines and the same standards of online behaviour as in school.
- Pupils and parents must adhere to the AUP during remote learning sessions.

Parental Engagement

- Parents are informed of online safety policies and are encouraged to use the National Online Safety resources provided by the school.
- Consent for internet and image use is obtained at enrolment and renewed as needed.

Policy Links

This policy should be read alongside:

- Safeguarding and Child Protection Policy
- Acceptable Use Policy (AUP)
- Social Media Guide
- Data Protection Policy
- Behaviour Policy
- AI Guidance