Ron Dearing

UTC

E-Safety

Policy

Document Title	Ron Dearing UTC E-Safety Policy
Version number:	2.0
Date of issue	05/01/2026
Date to be revised	Annually
Status	Final

Introduction

Ron Dearing UTC is committed to keeping all members of the school community safe and secure when using technology. This includes:

- Preventing access to harmful or unsuitable material (violence, hate speech, sexual content, extremism, bullying).
- Preventing exposure to misinformation, disinformation, conspiracy theories, and harmful AI-generated content (e.g. deepfakes).
- Embedding safe, ethical and responsible use of Artificial Intelligence.
- Promoting responsible digital citizenship in school and beyond.
- Protecting data and systems from cyber threats.

This policy complements the Safeguarding Policy, Data Protection Policy, Anti-Bullying Policy, and Staff Code of Conduct.

Aims

The school aims:

- Safeguard students and staff when using technology in school or remotely.
- Promote safe and responsible use of the internet, AI tools, esports, and mobile devices.
- Comply with KCSIE 2025, UK GDPR 2018, DfE Filtering & Monitoring Standards, and DfE Cyber Security Standards.
- Provide clear systems for reporting, responding to, and reviewing online safety incidents as per our safeguarding policy.

Leadership & Governance

- The online safety lead at Ron Dearing UTC is Zaeem Basit. Zaeem Basit is a member of Senior Leadership Team and leads Digital & Online Safety.
- Online Safety Group meets termly.
- Policy published on school website and shared with staff, students, and parents.
- Parents and carers will be regularly informed about online safety updates through newsletters, workshops, and National Online Safety resources.

End-to-End E-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT and AI use by all.
- Termly review of filtering effectiveness and logs, annual SLT oversight.
- Annual risk assessment against DfE Cyber Security Standards.
- Secure network design and access management, including BYOD.
- Students are taught how to use AI tools responsibly, recognising issues of bias, misinformation, and privacy.

Information Systems Security

- Multi-Factor Authentication (MFA) is enforced on all administrator accounts and any system accessed remotely or containing sensitive data.
- Strong password requirements are enforced for all users, including minimum length, complexity, and automatic lockout after repeated failed attempts.
- Access rights are restricted to the minimum necessary for each role, with immediate removal or adjustment of accounts when staff join, move roles, or leave.
- Secure backups in place in line with the DfE 3-2-1 guidance.
- A documented cyber incident response plan and business continuity plan are in place and reviewed annually, including procedures for reporting breaches.
- Email security controls in place and staff/students are provided training on phishing & safe use of technology.
- Network infrastructure is segmented to separate staff, student, administrative and BYOD environments, reducing the impact of potential cyber incidents.

Use of Email & Communication

- School email for educational/professional use only.
- All staff and students are expected to handle information securely and will be instructed not to disclose any personal or confidential data except through approved and protected systems, in line with UK GDPR and RDUTC Personal Data Policy.

- Staff must avoid using students full names in email communications to minimise the disclosure of personal information and to reduce safeguarding and data-protection risks
- Staff Training will be provided and includes risks of phishing, social engineering, and AI-generated emails/deepfakes.
- Everyone using RDUTC IT Systems is encouraged to escalate suspicious or offensive emails to IT.

Social Media & LinkedIn

- The UTC will place emphasis on safe and responsible use of social media.
- Staff prohibited from contacting students via personal social media and training provided annually. Social media include TikTok, Instagram, Snapchat, livestreaming, gaming chats.
- LinkedIn provides professional networking opportunities for staff/students. It is therefore important that staff/students recognise a public facing account linked to Ron Dearing UTC and any subsequent posts or comments made on the platform do represent Ron Dearing UTC as an employer/UTC. Therefore, any post/comments made must not bring the reputation of Ron Dearing UTC into disrepute either directly or indirectly through likes, comments or shares.
- Staff & Students in Year 12/13 or ex-students can “connect via LinkedIn” however must not use the LinkedIn Messaging function to communicate. If a student sends a Direct Message via LinkedIn to a member of staff, the member of staff should report this following our normal Safeguarding procedures.
- Staff must NOT send direct messages to students or ex-students at any time.
- Staff are not permitted to “connect” with students in years 10 or 11 and if they receive a connection request must report it following our normal safeguarding policy.

Filtering & Monitoring

At RDUTC we are Filtering compliant with DfE Standards and in line with our Safeguarding Policy.

- Monitoring system alerts DSL and key personnel for safeguarding keywords (CSA, self-harm, extremism).

- Keywords alerts are in line with our safeguarding policy and monitored for staff and students.

Software Approval

- Any new technology (AI tools, software, hardware, wearables, esports, IoT) risk-assessed before use.
- Staff will be expected to fill in the software/hardware approval form which will be used to assess the risk.
- Any new software/hardware request will be in line with our Software/Hardware Approval Process.

Esports

- We consider E-Sports as educational and competitive.
- Esports suites will be subject to monitoring.
- Esports Code of Conduct signed by students and parents.
- Esports Groups will be small to ensure active observation of the suite by the teacher.
- No unauthorised streaming, recording or game chat.
- Esports procedures to follow the E-Sports Code of Conduct.

Bring Your Own Device (BYOD)

- Filtering/monitoring applied when you connect to Guest / School Wi-Fi.
- Acceptable Use Policy apply to Guest Wi-Fi.
- Segmented VLANs in place to protect school systems.

Reporting & Responding

- Online Concerns & Online Bullying to be reported in line with our safeguarding policy.
- Students and staff can report online safety concerns through the school's reporting system or directly to a trusted adult, DSL, or Online Safety Lead

Acceptable Use Policy

- Updated 2025 for staff and students.
- Staff AUPs cover professional AI use and personal online conduct.
- Student AUPs cover AI, gaming, streaming, and social media.
- Parent AUPs confirm support for school e-safety expectations.

Monitoring & Evaluation

- Policy reviewed annually.
- Dashboard of incidents, training, filtering/monitoring audits maintained.
- The E-Safety Policy is available on the school website and will be revisited with staff and students annually as part of online safety training