



IT Acceptable Usage Agreement

2025-2026

Introduction

Students at UTC Reading are expected to use digital technology responsibly, safely, and in line with the expectations of the school. This agreement applies to all devices, including but not limited to:

- Laptops
- Tablets
- Mobile phones
- Smart devices (e.g., smartwatches)
- Any personal or school-owned device used on site or connected to the UTC network

All students must adhere to this Acceptable Usage Agreement to ensure a safe, secure, and productive learning environment.

Use of Devices for Learning

The use of digital devices at UTC Reading provides opportunities for students to enhance their learning, access resources, and develop digital literacy. Students are expected to:

- Use devices for educational purposes during lessons and Independent Learning Time
- Access the UTC Wi-Fi network only, which is filtered and monitored for safeguarding
- Ensure their device is charged and ready for use each day
- Back up all schoolwork using Microsoft OneDrive
- Maintain their device in good working order

Technical issues or forgotten devices do not remove the student's responsibility to complete work.



Filtering, Monitoring, and Searching

To comply with safeguarding legislation and ensure safe use of technology:

- All devices connected to the UTC network are subject to internet filtering and monitoring
- Staff may monitor usage to ensure devices are being used appropriately
- The UTC reserves the right to search and confiscate any device if there is reasonable suspicion of misuse, safeguarding concerns, or a breach of this agreement
- Confiscated devices may be held overnight or longer if required for investigation
- Serious breaches may be reported to the police or external safeguarding agencies

Students are responsible for ensuring their device is secure and used appropriately at all times.

Lost, Damaged, or Stolen Devices (Personal or School-Owned)

- Any lost, damaged, or stolen device must be reported to the IT Support Team or a member of staff immediately
- If a device is stolen, this must be reported to the police within 24 hours and a crime reference number provided to the school
- Students are responsible for the care of their personal devices and accessories
- The UTC is not responsible for personal devices brought onto school site including laptops used for learning purposes
- The UTC is not responsible for loss of personal data stored on any device

Mobile Phones, Hotspots, and Personal Connectivity

- Students must use the UTC Wi-Fi for internet access on all devices
- Personal hotspots must be switched off on site
- Students must not connect any device to a mobile hotspot while on school premises
- Breaches will result in warnings, followed by confiscation of the mobile phone and parental contact if the behaviour continues



Prohibited Uses of Any Device

The following activities are strictly prohibited on any device used on UTC premises or connected to the UTC network:

1. Accessing Inappropriate Content

Including but not limited to:

- Pornographic, obscene, or sexually explicit material
- Violent, extremist, or hateful content
- Threatening, abusive, or discriminatory material

2. Illegal Activities

Any activity prohibited by law, including:

- Hacking or attempting unauthorised access
- Downloading or sharing copyrighted material illegally
- Possession or distribution of illegal content

3. Misuse of Images, Video, or Audio

- Taking photos, videos, or recordings without permission
- Creating or sharing content intended to embarrass, bully, or harm others
- Any use of cameras in toilets, changing rooms, or other private areas (treated as a serious safeguarding violation)
- Students must delete any images or videos if requested by staff or if individuals do not consent to appear in them

4. Misuse of Accounts or Passwords

- Attempting to access another user's account, files, or data
- Sharing passwords or using someone else's login credentials



5. Malicious or Unsafe Behaviour

- Attempting to damage, disable, or disrupt devices, software, or the school network
- Installing unauthorised software or applications
- Bypassing or attempting to bypass filtering or monitoring systems

6. Inappropriate Media or Content Storage

Including:

- Pornographic material
- Drug, alcohol, or gang-related imagery
- Offensive or discriminatory content

7. Non-Educational Use During Lessons

- Streaming non-educational videos
- Playing games without educational value
- Using social media or messaging apps

Security and Maintenance

Students must:

- Keep antivirus software up to date
- Install system updates regularly
- Ensure devices connected to the UTC network are identifiable by name and MAC address
- Prioritise academic storage over personal files



Consequences of Breaching the Agreement

Breaches may result in:

- Confiscation of devices
- Removal of content
- Loss of network or device privileges
- Disciplinary action
- Parental involvement
- Referral to police or external safeguarding agencies where required

Completion of schoolwork remains the student's responsibility regardless of disciplinary action.

Date of agreement creation – September 2026

Date of agreement review – March 2026 (to include messaging apps and social media in lessons)

Date of next Review August 2026 in preparation for new academic year