IT Acceptable Usage Agreement

As you will be aware, a laptop is an essential piece of equipment for every student at UTC Reading. There are two ways in which students are able to access a laptop to complete their studies at the UTC. The first would be for the students to Bring Their Own Device (BYOD), and the second would be to join the UTC Reading E-Learning Scheme. The E-Learning Scheme gives every student access to a school laptop for their use both at home and at school to ensure that they can make the most of the time available for learning. Whether you bring your own device or use a device on the E-Learning scheme, all students must adhere to the IT Acceptable Usage Agreement.

The use of the laptop in a one to one environment provides an opportunity to enhance each student's overall learning experience. Utilising the laptop at UTC Reading (UTC) gives students the access to learn anywhere, anytime - at the UTC or at home. This one to one personalised learning also narrows the digital divide between students and promotes responsible use of today's ever changing technologies.

To ensure all users are protected from inappropriate content all devices accessing the UTC Wi-Fi will be subject to the UTC filtering policies.

In order to comply with local legislation, the UTC reserves the right to search and confiscate a student's laptop to ensure compliance, in line with the Acceptable Usage Agreement. Students in breach of the Acceptable Usage Agreement may be subject to, but not limited to; disciplinary action, overnight confiscation, removal of content or referral to external agencies where required by law. In the event of any disciplinary action, completion of all work remains the responsibility of the student.

The UTC is not responsible for the financial loss of any personal files that are deleted.

Safeguarding and Maintaining as an Academic Tool

- All students will have access to the Office 365 suite of applications. This set of applications are to be used by staff and students for completion of work and communication.
- Students are expected to check and interact with their school emails on a daily basis.
- If a laptop is left at home or is not charged, the student remains responsible for completing all work as if they had use of their laptop.
- Work should always be backed up, such as being stored in Office 365/OneDrive and not on the laptop or other portable storage.
- Items deleted from the laptop cannot be 'undeleted', so use of One Drive is essential.
- Malfunctions or technical issues are not acceptable excuses for failing to complete work, unless no other means of completion exist.
- Where storage space is limited, academic content takes precedence over personal files and apps.
- The whereabouts of the laptop should be known at all times. It is a student's responsibility to keep their laptop safe and secure.

- Laptops belonging to other students are not to be tampered with in any manner.
- If a laptop is found unattended, the nearest member of staff should be made aware of it.

Lost, Damaged, or Stolen Laptop (for eLearning Scheme Devices only)

- If the laptop is lost, stolen, or damaged, a member of the IT support team must be notified immediately.
- If a laptop is stolen you must report this to the police within 24 hours and they will issue a crime reference number; you must then present this immediately to the IT support team as it is required for insurance purposes.
- Without a crime reference number, UTC Reading is unable to claim for replacement of the laptop.
- Costs incurred for laptops that are damaged and not covered by standard insurance or warranty will be charged to the student/parent.
- It is the responsibility of the student to ensure the laptop and accessories are looked after. Any lost or damaged accessories must be replaced by the student.
- No more than 2 insurance claims will be allowed during any 2-year period.

Monitoring

To comply with local legislation and safeguarding policies, all computer usage is subject to routine monitoring by staff. The IT Support Team will periodically monitor laptop wireless activity.

All devices (including BYOD) will be monitored using classroom management software. This software allows staff to ensure that devices are being used appropriately and safely during lessons and Independent Learning Time. This requires the installation of client software on BYOD devices and school laptops, which is required in order for laptop users to access the Wi-Fi network. This software will only be used during the UTC normal working hours and cannot monitor any activity outside of the school network. The software will not access cameras or microphones. The monitoring software will be running on student laptops and BYOD devices during normal school hours. If a student is not at school for any reason i.e. sickness, then the monitoring software will still be monitoring their online activities by default.

All devices must be known to the school network. School laptops will be allocated to the students using a device name and MAC address. BYOD device names and MAC addresses are also required so that monitoring can happen on the school network. Therefore students are required to bring their own device to IT support so that the appropriate software can be installed for monitoring purposes and the laptop name and MAC address can be noted down. If the monitoring software is uninstalled on the BYOD devices and/or the device name or MAC address change, then this will be in breach of the Acceptable Use Policy and the laptop will not be able to be brought in to school until the device is back to the school security standard.

All BYOD devices must have up-to-date antivirus software installed and running and Windows Updates must be applied to keep the security of the laptop to the required

level. Laptops on the E-Learning scheme will have their security managed automatically and are not required to change any of the settings.

Students on the E-Learning Scheme are not allowed to change the laptop configuration in any way, wipe the hard drive or replace any software on the laptop. All software required for teaching and learning purposes will be installed on the school laptops whereas BYOD devices will just have access to Office 365 applications. If students require additional software to what is offered, they can request the installation of software and this will be considered by the IT team for its educational appropriateness.

Prohibited Uses Include:

- Accessing Inappropriate Materials - All material on the laptop must adhere to the UTC IT Acceptable Usage Agreement. Students are not allowed to send, access, upload, download, or distribute material that is offensive, threatening, pornographic, obscene, or sexually explicit.
- Illegal Activities – Activities prohibited by law.
- Commercial or financial gain – including the UTC email and internet services for BYOD users.
- Violating Copyrights - Students are only allowed to have music and applications in compliance with copyright laws and applicable licenses.
- Use of any applications/software not authorised by the UTC for use on the UTC systems.
- Photography - Students must use good judgement when using the camera. The student agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to take photos or videos of those not wishing to appear in that media, and nor will it be used to embarrass anyone, student or staff, in any way. Any use of camera in toilets or changing rooms, regardless of intent, will be treated as a serious violation. Photos and videos created on site must be deleted should those appearing in the created media object.
- Misuse of Passwords, Codes or other Unauthorised Access: Any user caught trying to gain access to another user’s accounts, files or data, or the school network, will be subject to disciplinary action.
- Malicious Use/Vandalism - Any attempt to destroy or deface hardware, software or data, or otherwise compromise the security of the UTC systems.
- Display of Inappropriate media - This includes the presence of pornographic materials, inappropriate language, alcohol, drug or gang related symbols or pictures and will result in disciplinary actions.
- Streaming of videos (including music videos) which do not have any educational content.
- Playing online games which do not have any educational benefit.
- Storing of any confidential data on any school device unless the storage facility is fully encrypted.