Mobile technology is now an essential part of teaching and learning, with more of our data being stored on tablets, smartphones and laptops. These devices are now as powerful as traditional static computers and so portable that they are more at risk than 'desktop' equipment.

**Keep devices locked**

You must avoid leaving mobile network devices in unlocked or unattended locations. If you don’t lock your device, you are immediately losing a key layer of security.

Your IT Support should have enable automatic lock to enhance the security on all mobile devices.

**Password / Biometric Protection**

Use a PIN or password, which is not related to other common personal identifiers, such as your birth date. Many devices include fingerprint/face recognition to lock your device but this may not be enabled. If possible, switch this on to prevent others from accessing it.

**Encrypt your Device**

Encrypting devices provides better security for the data it holds. e.g. BitLocker for Windows which is free and built-in.

**Update the Operating System**

Operating system updates don’t just improve the user experience, but also cover protection from newly discovered threats and reported bugs.

When flaws are discovered, the manufacturer will normally fix them and send the fix out as a patch or part of an update. Updates should be applied automatically, but sometimes you may be prompted to manually install an update, which must be done at the earliest convenient opportunity.

You must avoid or replace unpatched or unsupported hardware or software, including operating systems. These devices are the most popular targets for successful cyber-attacks.

**Keep your Apps Updated**

All installed applications and software should also be updated regularly with patches from the software developers. These updates will not only add new features, but they will also patch any security holes that have been discovered.

Hackers rely on you to ignore those ‘annoying’ update notifications so they can get in before the update is made – so don't give them the chance.

**Use Caution when connecting to WiFi Hotspots.**

When you use public Wi-Fi hotspots e.g. coffee shop, there is no way to easily find out who controls the hotspot, or to prove that it belongs to who you think it does. If you connect to these hotspots, somebody else could access your private login details or what you're working on whilst connected.

Always assume a public Wi-Fi network isn’t secure – have a think if logging in and sending sensitive information can just wait a while until you get home or get back to work when it could be more secure to do so.​

**Beware of Downloads**

Your school is likely to control the software or apps that can be installed on your school devices. If it’s your personal device and you control what apps and software you install, it’s best to only use official app stores (like Google Play or Apple App Store).​ You should avoid downloading third party apps from unknown websites or vendors as these may not have been scanned for virus or malware.

Many web browsers alert you before you visit a scammy website or download malicious programs. Don’t ignore those warnings.

**Anti-Virus Software**

An antivirus product is a program designed to detect and remove viruses and other kinds of malicious software.

Antivirus software is often included for free within device operating systems. If you make sure that this built-in antivirus is switched on, you'll instantly be safer.