



We CARE

Welcoming all Community Achievement Respect Encouragement

---

# Protecting Mobile Devices

(Compiled with reference to National Cyber Security Centre)

Version 1.0

---

<b>Last Reviewed</b>	12.07.2021
<b>Reviewed By</b>	FGB
<b>Minute Number</b>	
<b>Next Review Date</b>	July 2022

## **Protecting Mobile Devices**

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

### **Switch on Password / Biometric Protection**

Use a pin or code which is not related to other common personal identifiers, such as your birth date. Many devices include fingerprint recognition to lock your device but may not be enabled. If possible, switch this on to prevent the average criminal from accessing your phone.

### **Encrypt your Phone / Tablet**

Many phones and tablets offer device encryption when you set them up for the first time. Encrypting the device provides better security for the data it holds.

### **Make sure lost devices can be tracked, locked or wiped.**

Staff are more likely to have their tablets or phones stolen (or lose them) when they are away from the office or home. Free web-based tools can:

- track the location of a device
- remotely lock access to the device (to prevent anyone else using it)
- remotely erase the data stored on the device
- retrieve a backup of data stored on the device

### **Keep your Device Updated**

All manufacturers (for example Windows, Android, iOS) release regular updates that contain critical security updates to keep the device protected. This process is quick, easy, and free; devices should be set to automatically update, where possible.

Make sure your staff know how important these updates are, and explain how to do it, if necessary.

### **Keep your Apps Updated**

All installed applications 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. Make sure staff know when updates are ready, how to install them, and that it's important to do so straight away.

## **Don't Connect to Unknown Wi-Fi Hotspots.**

When you use public Wi-Fi hotspots (for example in hotels or coffee shops), 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:

- what you're working on whilst connected
- obtain private login details that many apps and web services maintain whilst you're logged on

The simplest precaution is not to connect to the Internet using unknown hotspots, and instead use your mobile 3G or 4G mobile network, which will have built-in security.

This means you can also use 'tethering' (where your other devices such as laptops share your 3G/4G connection), or a wireless 'dongle' provided by your mobile network.

You can also use Virtual Private Networks (VPNs), a technique that encrypts your data before it is sent across the Internet. If you're using third party VPNs, you'll need the technical ability to configure it yourself, and should only use VPNs provided by reputable service providers.