

 **Protecting Mobile Devices**

 Updated September 2021

Version 2.0

**Compiled with reference to the** [National Cyber Security Centre](https://www.ncsc.gov.uk/collection/small-business-guide/keeping-your-smartphones-and-tablets-safe)

**Contents**

[**1.** **Keep devices locked** 3](#_Toc83198113)

[**2.** **Password / Biometric Protection** 3](#_Toc83198114)

[**3.** **Encrypt your Device** 3](#_Toc83198115)

[**4.** **Update the Operating System** 4](#_Toc83198116)

[**5.** **Lost Devices** 4](#_Toc83198117)

[**6.** **Keep your Apps Updated** 4](#_Toc83198118)

[**7.** **Don’t Connect to Unknown Wi-Fi Hotspots.** 5](#_Toc83198119)

[**8.** **Beware of Downloads** 5](#_Toc83198120)

[**9.** **Install Anti-Virus Software** 5](#_Toc83198121)

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.

## **Keep devices locked**

If you don’t lock your device, you are immediately losing a key layer of security. Enable automatic lock to enhance the security on all mobile devices. Choosing the shortest amount of time between when you last used your device and it locking will give you the best protection, and save your battery power by reducing the screen brightness.

## **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.

Cyber Essentials requires 8-character passwords, even for mobile devices used to connect to school systems, including reading emails.

## **Encrypt your Device**

Devices offer device encryption when you set them up for the first time. Encrypted data is stored in an unreadable form so it can’t be understood. Encrypting the device provides better security for the data it holds.

For iOS devices: Go to the settings menu and then click on ‘Touch ID & Passcode’. It will prompt you to enter your lock screen code. Then scroll to the bottom of the page where it should say ‘Data Protection is enabled’.

To encrypt an Android: Go to ‘Security’ and choose ‘Encrypt Phone’.

Encryption can take an hour or more, so fully charge it or plug it in and DO NOT interrupt the process.

## **Update the Operating System**

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

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.

To check if your device OS is up to date, go to ‘about device’ or ‘general’ and click ‘system updates’ or ‘software update’.

## **Lost Devices**

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 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
* 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 4G/5G mobile network, which will have built-in security.

This means you can also use 'tethering' (where your other devices such as laptops share your 4G/5G 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.

## **Beware of Downloads**

When you are downloading apps, be sure to download them from the official app stores and check the reviews. Criminals can mimic trusted apps to trick users into installing. Check the number of reviews and if an app asks you to download another app to function, stop the install.

Rogue apps don’t have robust security and may attempt to steal device information and spy on user activity while running in the background.

## **Install Anti-Virus Software**

Tablets and smartphones can hold all your important data and personal information. Mobile devices are just as likely to suffer from viruses and other malware and anti-virus software should be installed if it isn’t already available ‘out of the box’. Remember to keep it updated and to review any logs/alerts regularly.