**POPI and Smart Devices recommendations**

As part of your overall POPI Act compliance risk assessment in order to comply with Condition 7 (Security Safeguards, Section 19) you need to identify the risks associated with using smart devices in your organisation. Follow these recommendations as part of your overall risk management approach.

# Guard your phone or tablet or tablet, and set PINs and passwords

## Treat your phone or tablet as carefully as you would your bank cards. Take care when using your phone or tablet in public, and don’t let it out of your possession. Thieves can quickly rack up huge bills on stolen phone or tablets, and you may be liable for all charges run up on your phone or tablet before you have reported it lost or stolen to your provider.

## To help prevent this happening, protect your phone or tablet against unauthorised use by setting up a PIN, swipe pattern or password for your home screen. You can usually do this through the Settings feature on your phone or tablet.

# Take precautions in case your phone or tablet is lost or stolen

## Make a record of your phone or tablet’s IMEI number, as well as the make and model and serial number. The IMEI is a unique 15-digit serial number which you will need to give to your mobile operator to have your phone or tablet blocked. You can check your IMEI number by keying \*#06# into your handset or by looking behind your phone battery.

## Consider making your phone or tablet less useful to potential thieves by barring calls to international numbers and premium rate lines, if you never use them.

## Some mobile insurance policies, or any other policies that may cover the mobile phone or tablet, could provide limited cover for unauthorised use. So it is worth checking the terms and conditions of your existing policy, and when considering a new policy.

# Don’t override your smartphone or tablet’s security settings

## It is not advisable to attempt to ‘crack’, ‘jailbreak’ or ‘root’ your smartphone or tablet. This is a process people use to remove restrictions placed on their device’s operating system by the phone or tablet manufacturer.

## Doing so carries considerable risks: it compromises the security of your device, and may leave you more vulnerable to malicious software. It is also likely to invalidate your manufacturer’s warranty.

# Back up and secure your data

## Many smartphones or tablets come with a software package to back up your data to a personal computer, so that you don’t lose it if your phone or tablet goes astray. Check for information on how to do this in the phone or tablet’s manual.

## There are also some third-party applications (‘apps’) that can do this for you, creating a copy of information such as contacts, photographs and other data.

# Install apps from trusted sources

## Apps are the easiest way for someone to hack into your phone or tablet. Sometimes hackers will take a popular paid-for app, add their own illegitimate elements and then offer it for free on ‘bulletin boards’, ‘peer-to-peer’ networks or through fake online stores.

## Once the rogue app has been downloaded to your phone or tablet, the hacker can potentially take control of the handset, incur charges via premium SMS without your permission, make calls, send and intercept SMS and voicemail messages, browse and download online content. You may not be aware anything is wrong until it’s too late.

## So avoid apps from unauthorised sources, such as ‘bulletin boards’ or ‘peer-to-peer’ networks. Instead, download your apps from official stores, such as the Apple App Store, BlackBerry World or Google Play – and exercise care: for example, research the app and check reviews.

# Use antivirus software

## It’s not just rogue apps which pose a threat to your smartphone or tablet. Viruses and spyware can also be downloaded from websites, or by connecting your device to an infected computer.

## Some phone or tablets may be more vulnerable than others, but you can check for antivirus software in a reputable app store such as Google Play.

## Also, before connecting your device to a computer, ensure it has the latest antivirus/antispyware and firewall installed and running.

# Use software to find or erase your phone or tablet if it goes missing

## Consider installing a reputable security app that enables you to track your phone or tablet’s location if it goes missing, or to wipe data from the phone or tablet remotely if you’re not able to recover the handset.

## Some manufacturers provide such an app themselves: for example, Apple’s Find My iPhone or tablet, BlackBerry Protect, the Android Device Manager or Windows Find My Phone or tablet. Third-party apps are also available to perform a similar function.

# Clear your phone or tablet before you dispense with it

## If you decide to donate, resell or recycle your smartphone or tablet, remember to erase any data on it first.

## Remove and erase any media cards and perform a full or ‘factory’ reset by going into the Settings menu.

# Accept updates and patches

## Occasionally, your smartphone or tablet manufacturer may send you a message proposing an update to your operating system – the software that runs your device. App developers may also propose updates to their app.

## It is advisable to accept these updates as they become available. As well as typically offering new features and improving your phone or tablet’s performance, they can also fix security vulnerabilities.

Source: Adapted from “Safer smartphones - a guide to keeping your device secure, ICO, October 2013”