PORTABLE DIGITAL DEVICES GUIDE

# INTRODUCTION

To maintain the security on portable digital devices (like mobile phones, tablets, laptops and smartphones) it is important that all staff are aware of the security threats and the precautions recommended to reduce the risk of these threats.

# SECURITY AWARENESS

The use of portable digital devices within is becoming more prevalent. Technology has advanced the features of portable devices providing more functionality with access to the Internet, higher quantity of data storage, applications and greater connectivity options. As the technology advances the risk of a security incident also increases.

The security threats and the recommended precautions you should take to mitigate the risk of a security incident are outlined in this guide. If you have any questions about the following recommendations please refer to .

## LOSS OR THEFT

Due to their small size, portable digital devices have a propensity to become lost or misplaced. They are also an easy target for theft.

 It is recommended that portable digital devices should not be:

* Left in an unattended vehicle even for a short period of time where the device can be easily seen;
* Left in a vehicle overnight;
* Positioned such that it is easily visible from a publically accessible window;
* Your portable digital device should be locked when not in use (ask if you are unsure how to lock your portable digital device);
* To minimise the impact of a portable digital device being lost or stolen it is recommended that restricted or confidential information is not stored on the device;
* If your portable digital device is lost or stolen contact immediately as they may be able to, dependent upon the device, lock or disable the portable digital device remotely.

## DISPOSAL

When your portable digital device is no longer required it is important that the device is returned to for appropriate disposal.

Portable digital devices that are no longer required will be cleared of information using the built-in software. This is important as data often resides on portable digital devices and without re-setting the device through the approved process information can be easily restored. will follow the approved disposal process for these devices to ensure data is removed permanently.

## UNAUTHORISED ACCESS

Access to a portable digital device and its contents may be gained by forging or guessing authentication credentials (e.g. a PIN or password) or bypassing the authentication mechanism.

We recommend:

* Do not change your security settings to remove the start-up and screen saver password\PIN prompt that has been set by . Having a start-up PIN is a requirement of asset management protocols;
* Do not share your PIN or password with anyone else.

## MALWARE

A threat for mobile phones, tablets, laptops and smart phones that interact with communications networks is the infection of malware. Malware can be spread through:

* Internet connections and downloading of infected files (like games, utilities).
* Messaging services delivering infected files through attached electronic email, instant messages or Multimedia Messages.
* Bluetooth communications connecting a portable digital device to another and infecting this device with malware.

For these delivery methods the user of the portable digital device usually has to give consent for the malware to install and execute. It is recommended that you:

* Do not change the communications options that have been installed on the portable digital device, this includes amending the services or adding new services. For example Bluetooth and Infrared are disabled to comply with asset management protocols.
* When using the Internet follow Acceptable Use Policy.
* Do not accept any requests to share information or install additional utilities; if unsure contact .

## SPAM

Unwanted text messages, emails and voice messages from advertisers can appear on portable digital devices. Besides the inconvenience of removing items, charges may appear for inbound messages or costs applied to download attachments. Messages may also persuade users to call or send messages to chargeable service numbers. If a spam message is received we recommend you delete it and do not follow any Internet links.