University College Cork

Guidelines for Smartphone Users

Version 1

Guidelines for smartphone users in the university community regarding their use and the user's responsibilities under the university's IT security policy, data policy and AUP

Document Location

http://www.ucc.ie/en/it-policies/guidelines

Revision History

Date of this revision: 02/08/2013	Date of next review: 2/08/2014

Version Number/Revision Number	Revision Date	Summary of Changes

Consultation History

Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes

Approval

This document requires the following approvals:

Name	Title	Date

Guidelines for Smartphone Users

Mobile devices are becoming increasingly computer-like. Smartphones can store and process information and connect to network services. If you use your smartphone in conjunction with your University activities, please be aware of your responsibilities under the University's IT security Policy, Data Policy and Acceptable Use Policy.

Most popular smartphones use cut-down versions of "traditional" computer operating systems. As a consequence, they have similar functionality and risks. To protect your device and the University you should observe the following usage guidelines.

DO take regular backups of your phone and keep them in a safe location.

DO keep your phone software and applications up to date.

DO disable services such as Bluetooth, NFC or WiFi when they are not in use.

DO use password protection and a power on/timeout lock on your device.

DO put a physical label on it so as to maximise the chance of its return when lost.

DO enable "remote wipe" features for use if the phone is lost or stolen.

DO ensure that information is adequately removed before passing on or disposing of a device.

DO exercise caution when browsing the web or reading e-mail. (This applies all the more in your personal time when you may be more vulnerable to "social engineering".)

DO protect your credentials, credit card details and other significant information while they are in transit.

DO consider antivirus precautions. (AV software often has, however, limited availability and effectiveness on these platforms.)

DO consider the use of encryption to protect phone memory contents and that of removable memory. (The effectiveness (and availability) of encryption varies considerably from device to device.)

DO remember that the file systems on memory cards may not be well protected from Apps.

DO review the Guidelines for Portable Devices in conjunction with this.

DO check your bill for anomalies.

DO record your IMEI (International Mobile Equipment Identity) number.

and

DON'T download applications from untrusted sources.

DON'T "jailbreak", "root" or "unlock" your phone to install an application.

DON’T grant applications additional powers without careful consideration.

DON’T rush to install the “latest app” – even trusted applications can have malware.

DON’T follow unsolicited links on social media, SMS, or e-mail.

DON’T load UCC data onto the device without taking into account the permission of the data owner and the appropriate UCC policies.

DON’T connect to arbitrary WiFi hotspots. Connect only to those you are expecting to find and use them only for non-confidential activities.

DON'T use public kiosks to charge your phone via USB.