Device Protection Policy

Policy owner IT Services **Approval date and body** **UMT Approved 2 February 2021**

1. Purpose

Our University community is made up of a wide range of people with diverse backgrounds and circumstances, which we value and regard as a great asset. Our continued commitment to an inclusive and respectful University environment includes a responsibility to protect personal data and to protect individuals from discrimination on the grounds of race, disability, gender, gender identity, age, sexual orientation, religion, civil status, family status, membership of the travelling community or socio-economic status resulting from unauthorised access to their personal data.

The purpose of this policy is to safeguard Personal Data and Confidential University Information from being exposed to threats through the use of unprotected and unsecured devices. This policy seeks to reduce the risk of an information security related incident from a device being lost, stolen, used or exploited in such a way to take unauthorised advantage of Personal Data or Confidential University Information.

2. Definitions

- **Devices** include, but are not limited to laptop computers, desktop computers, registered servers, tablet devices, smartphones, internet connected devices that are commonly referred to as "IOT" or "Internet of Things" and external storage devices.
- **University Issued Device** means any device that has been purchased, is owned or leased by the University.
- **Personally Owned Device** means any device that is held personally by an individual in a private capacity. Personally owned devices are commonly referred to as "BYOD" or "Bring Your Own Device".
- **University IT Systems** consists of any University supported IT system whether it is provided directly by a University unit or is managed by a third party on behalf of the University.
- **Personal Data** consists of any information concerning or relating to a living person who is either identified or identifiable. An individual could be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (such as an IP address) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.
- **Confidential University Information** consists of information which if disclosed, deleted, altered or made publicly available could cause damage or distress to individuals, damage commercial or

financial interests of the University and its connected companies, or result in the loss of intellectual property of the University or those connected to it.

3. Scope

This policy applies to all devices which access University IT Systems or access and store Personal Data or Confidential University Information, regardless of whether the device is university issued or personally owned, and regardless of geographic location of the device.

4. Principles

The principle of this policy is that all devices which are used to access University IT Systems or access and store Personal Data or Confidential University Information are appropriately protected, regardless of whether the device is University Issued or Personally Owned.

5. Roles and Responsibilities

It is a requirement of each individual user to ensure that all devices they use to access University IT systems or access and store Personal Data or Confidential University Information comply with the following minimum-security requirements:

- Device is protected with a strong passcode (e.g. pin, password, biometric authentication, etc.), which automatically locks the device after a maximum of 3 minutes of inactivity.
- Device has up to date anti-virus software with on-access scanning enabled.
- All software including the operating system and all applications must be running a supported version with up to date patches applied where available.
- Any Devices (including external storage devices) that permanently or temporarily stores Personal Data or Confidential University Information must be encrypted and the decryption key stored securely in order to prevent unauthorised access to information if the device is lost or stolen.
- It is strongly recommended that Personal Data or Confidential University Information that is stored on or accessed via a UCD central repository is not saved to any device as a local duplicate copy. Any Personal Data or Confidential University Information temporarily saved to a device must be safely erased immediately when it is no longer required.
- Before disposing of a device all University data stored on the device must be deleted in an irreversible manner by using a certified deletion programme or reset to manufacturers' original default settings.
- All traces of University data must be removed from any personally owned devices when leaving the employment of UCD.
- Review IT Services device security guidelines for the latest security requirements.

Lost or Stolen Devices

In the event of loss or theft of any device which is used to access University IT systems or access and store Personal Data or Confidential University information, the user must act promptly to minimise the risk of a compromise to University information and immediately:

- Change all University passwords and remotely wipe the device if this feature is supported by the device. Please contact the IT Services helpdesk (ithelpdesk@ucd.ie) if you require technical assistance.
- If the device contained Personal Data, the incident must be reported to the Data Protection Office (gdpr@ucd.ie)
- If the device contained Confidential University Information, the incident must be notified to a member of the UMT, directly or via your Head of School/Unit
- Report any lost or stolen University owned device to UCD's Safety, Insurance, Operational Risk & Compliance Office (sirc@ucd.ie)
- Report any on campus theft to UCD Estates (estates@ucd.ie).
- Report any theft to An Garda Síochána or local police service, depending on the geographic location of the device.

Breaches of compliance

A failure to abide by this policy may result in being denied access to University IT Resources including the withdrawal of network privileges, the suspension of an IT account, the loss of system privileges and/or disciplinary action.

Loss of Personal Data or Confidential University Information can have a significant legal, financial and reputational consequence for the University, including fines. Under GDPR regulations, anyone with access to Personal Data must take appropriate technical and organisational security measures to protect this information. If you believe that Personal Data or Confidential University Information has been put at risk due to a device being lost, stolen or exploited, you must report the incident to the University Data Protection Officer immediately by emailing gdpr@ucd.ie

6. Related Documents

- Acceptable Use Policy
- Data Protection Policy
- Password Protection Policy
- IT Services Device Security Guidelines
- Equality, Diversity & Inclusion Policy

7. Version History

Name	Version	Date	Reason for change
Paul Kennedy	Draft	01/07/2020	Draft for review
Paul Kennedy	Draft	17/08/2020	Updated draft for ITLG Review
Paul Kennedy	Draft	17/09/2020	Updated with feedback from ITLG and IT CCB
Paul Kennedy	Draft	22/09/2020	Updated with final updates from IT, for review by the UMT GDPR & Data Group
Brídín Walsh	Draft	22/10/2020	Updated with initial feedback from the UMT GDPR & Data Group
Brídin Walsh	Draft	05/11/2020	Updated draft with final feedback from the UMT GDPR & Data Group meeting on 04/11/20
Brídin Walsh	Draft	03/12/2020	Updated to address the comments from the Equality Impact Assessment (EIA) and feedback from the UMT IT Strategy Group
Brídín Walsh	Draft	10/12/2020	Updated to incorporate final updates from UCD Legal relating to confidentiality
Brídín Walsh	Draft	22/12/2020	Submitted for approval by UMT
Brídín Walsh	Draft	27/01/2021	Section 5 updated - reviewed with the IT Leadership Group, rewording was agreed at the UMT GDPR & Data Group meeting on 27th Jan.
Brídín Walsh	Version 1.0	02/02/2021	Approved by UMT