Acceptable Use Policy

Policy owner IT Services **Approval date and body** **UMT Approved 2 Feb 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. As part of our continued commitment to equality, diversity and inclusion, we strive to create an inclusive environment in which all members of our community should expect to be able to thrive, be respected and have a real opportunity to participate in and contribute to University activities so that they can achieve their fullest potential.

Users are expected to ensure usage of University IT Resources is carried out in an acceptable, safe, respectful and legally compliant manner.

The purpose of this Policy is to provide all those who use the University's IT Resources with clear guidance on the acceptable, safe, respectful and legal way in which they can use the University's IT Resources.

This Policy is designed to ensure that the University can offer the widest possible range of IT systems and network resources to UCD's community in a way that is compliant with data security and data protection and is not intended to limit use of the University's information services.

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 regardless of whether the device was purchased by the University or is personally owned.
- **IT Resources** consist of all University IT systems, network resources, University owned devices and the institutional data they contain regardless of whether the system is provided directly by a University unit or 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 staff, students, or other users of UCD's IT Resources including third party users, whether they are physically located on campus or accessing IT Resources remotely regardless of geographic location.

4. Principles

The University is committed to maintaining data privacy. However, the University reserves the right to maintain audit and activity logs and to monitor the use of its IT Resources for the following purposes:

- Investigating and enforcing University Policies, Codes of Conduct and Statutes.
- Maintaining the availability and performance of the University's IT Resources.
- Detecting, preventing, and investigating IT security-related incidents.
- Responding to legal or compliance requests from UCD Legal, Audit, HR or Registry.
- Complying with any legal and statutory obligations applicable to the University

Although schools and units may have developed their own policies at a local level, those policies cannot diminish the acceptable usage expectations as set out below.

5. Roles and Responsibilities

There is an obligation for all users of UCD's IT Resources or who have been issued an IT account to:

- Comply with this policy and all other relevant policies and procedures that apply to their role in the University. Please review UCD's Governance Document Library for a full list of University Policies.
- Report all breaches of this Policy to the IT Helpdesk by emailing ithelpdesk@ucd.ie or call 01-716 2700.

The Acceptable Use policy is included in employee contracts, presented in university systems including InfoHub and SISWeb and included in university communications such as student and staff eZines. A link to the policy is also incorporated into the footer of www.ucd.ie and most UCD-branded websites. Any user of IT Resources is deemed to have made themselves aware of this policy.

6. Acceptable Use

While it is impossible to address every possible situation, good judgement should always be applied when using University IT Resources and which should be used in a responsible and respectful manner. The following highlight areas for attention:

Legal and Policy Requirements

You shall use IT Resources in accordance with Irish law and University policies and procedures including the Universities Policies on Dignity and Respect, Equality, Diversity and Inclusion, Sexual Misconduct, Research Integrity and Student Code of Conduct.

IT Accounts and Access Rights

You may be provided with University IT accounts and passwords or other credentials to permit access to the University's IT Resources as outlined in IT Services IT Account and Service Access Procedure. Please be aware that UCD retains ownership of all IT accounts, data, and services for all IT accounts issued by UCD. Users are responsible for all activities and information accessible through their University IT accounts, including any additional IT accounts such as sponsored or visitor accounts which have been requested or renewed by an individual. You must ensure that in so far as practicable, that all use of IT accounts for which you are responsible conform to the University's policies regarding use and behaviour so that your use of UCD's IT Resources does not expose the University, its students, employees and other stakeholders to unnecessary risks.

IT accounts must be protected in line with UCD's Password Protection Policy and any unauthorised access or use of an IT account must be reported immediately to IT Services.

Use of IT Resources

You shall recognise that IT Resources are provided primarily for University related business including to support teaching, learning, research & enterprise, professional and administrative activities and you must behave reasonably in your use of University IT Resources. You must not undertake or facilitate any activity that could jeopardise in any way, the security (confidentiality and integrity), availability and performance of UCD's IT Resources, or compromise their utility or availability to other users. There is a page dedicated to Unacceptable Online Behaviour on the IT Services website for further information.

Please be aware that the University uses various technical measures to safeguard the stability and performance of the University's IT Resources, to help protect the University's information and IT Resources from cyber threats, and to enforce University policies. Technical measures include malware protection measures, IT Account protection measures, network intrusion detection and prevention controls, network stability services, application security controls, etc. These measures may be enhanced, or new controls or procedures introduced as necessary to help ensure the stability and performance of the University's network and to protect the University's IT Resources and Information against new or emerging cyber security threats.

Malware and Device Security

It is the device owner's responsibility to ensure that all Devices that have access to University IT Resources or process or store Personal or Confidential University Information are protected in line with IT Services Device Protection requirements.

You must take reasonable care to ensure that you do not transmit viruses or other malicious software to other users or Devices. If you suspect that University information, IT Resources, IT accounts or Devices have been abused or otherwise compromised, for example by a virus, ransomware, trojan, hacked, etc. you must notify IT Services immediately by emailing ithelpdesk@ucd.ie or calling 01-7162700. You must also take reasonable steps to ensure that the impacted system is removed from the University networks and other IT Resources.

Servers and other network connected devices must be configured, maintained and secured in line with IT Services device security requirements. Registration details for all network registered devices must be kept up to date and renewed in line with IT Services network registration requirements.

Licencing of software

All software installed and used on the University's computer systems, including stand-alone computers, must be appropriately licensed. Where University site licenses permit off-campus use and/or personal use, you must adhere to the terms and conditions of such licenses. IT Services offers a Software Downloads service that provides staff and students access to a library of software applications and utilities which UCD has licensed.

Data Privacy, Data Protection and Freedom of Information

Personal or Confidential University information is stored on the University's systems. If you have access to or are responsible for such data, you must ensure that the integrity, accessibility, accuracy, and confidentiality of such data are maintained. If you keep personal data on others you must comply with the provisions of the Data Protection Acts (1988, 2003 & 2018 - General Data Protection Regulations, as may be amended). This includes considerations regarding limiting disclosure of personal data to only those individuals that have a professional reason to access them, or to not keeping personal data any longer than permitted.

You must also be aware that the Freedom of the Information Act (2014 as may be amended) applies to records held in any format on University systems. Records and information held may need to be disclosed on foot of Freedom of Information requests (under Freedom of Information legislation) or Data Subject Access Requests (under Data Protection legislation) received by the University.

Please review UCD's Data Protection website for further details on UCD's Data Protection, and the Freedom of Information website for Freedom of Information obligations.

The University is committed to maintaining your privacy and only monitors or accesses IT Resources usage and activity for the reasons outlined in the Principles section above.

7. Unacceptable Use of IT Resources

Unacceptable use of IT Resources includes behaviour that is threatening, harassing, bullying, defamatory, libellous, illegal, offensive, discriminatory on the grounds of race, disability, gender, gender identity, age, sexual orientation, religion, civil status, family status, membership of the travelling community, socio-economic status, involves theft or fraud including creating , downloading, viewing, storing, sending, transmitting or causing the transmission of any material or images that are abusive, obscene, derogatory, pornographic, or otherwise indecent or illegal.

Further, unacceptable behaviour includes IT activities using IT Resources that will:

a) intentionally or recklessly use the name of the University in such a way that either by content or expression brings the University into disrepute including online activity that deliberately misrepresents your views as those of the University

b) incite hatred

c) advocate or promote any unlawful act

d) be likely to defame, defraud or deceive another person or organisation

e) cause harm, offence, harassment, sexual harassment, bullying, discrimination, victimisation, needless anxiety or persistent nuisance to others

f) corrupt, destroy or disrupt other users' data or deny and disrupt services to other users, for example: unnecessary or trivial messages, chain, junk mail or unsolicited bulk or marketing email (spam)

g) plagiarise or infringe the copyright, licence terms, trademark or proprietary rights of another person or organisation

h) conflict with an individual's obligations, contractual or otherwise to the University leading to personal financial gain or competing with the University in business

i) agree to terms, enter into contractual commitments or make representations by email on behalf of the University, unless authorised and appropriate to do so.

Security, Performance and Availability of IT Resources

Unacceptable behaviour also includes but is not limited to any activity that impacts the performance, availability, and security (confidentiality and Integrity) of the University's IT Resources or information such as spreading malware, hacking, network tracking (spying), high volume network attacks or scans, using another individuals IT Account without permission, impersonating another individual, spamming or sending unsolicited emails, interfering with University IT equipment or simulating University network equipment.

Intellectual Property Rights and Commercial Activity

You must not use IT Resources to infringe the copyright, patent, or intellectual property rights of any individual or the University by either downloading or distributing unlicensed or copyrighted software or materials. Use of IT Resources for personal commercial activity unless specifically authorised is unacceptable.

Confidential University Information

You must not use any IT Resources to disclose any Confidential University Information without consent of the University.

Examples of Unacceptable Behaviour

Examples of unacceptable online behaviour are available on the IT Services unacceptable user behaviour webpage.

8. Breaches of Policy

Unacceptable use of University IT Resources or IT Accounts can have a significant impact on the availability, performance, and security of the University's IT Resources and Information. Breaches of this policy can also have legal, financial, and reputational consequences for the University, including, but not limited to, fines.

Breach of this Policy may result in disciplinary action under the University's policies and procedures including the Disciplinary Statute and the Student Code of Conduct as well as referral to the An Garda Síochána or other regulatory body. The University shall carry out such investigations as required arising out of any breach or suspected breach of the Policy.

Furthermore breach of this Policy or where an IT security incident is suspected may result in content being taken down, disconnection of systems and/or devices, being denied access to University IT Resources including the withdrawal of network privileges, the suspension of an IT account or the loss of system privileges.

9. Related documents

- UCD Data Protection Policy
- IT Security Policies and Procedures
- Data Protection Policy
- Password Protection Policy
- Device Protection Policy
- University College Dublin, Statute 28, Disciplinary Statute
- Student Code of Conduct
- Equality, Diversity and Inclusion Policy
- Employment Equalities Acts 1998-2015
- Universities Act (1997)

10. Version history

Name	Version	Date	Reason for change
Library and Information Technology Board	V1.0	18/11/2013	First published version of the policy
Paul Kennedy	Draft	09/09/2020	Redrafted, including ITLG feedback, IT CCB feedback
Brídín Walsh	Draft	22/10/2020	Updated draft with initial feedback from the UMT GDPR & Data Group
Brídín Walsh	Draft	05/11/2020	Updated draft with final feedback from the UMT GDPR & Data Group meeting on 04/11/20
Brídín Walsh	Draft	12/11/2020	Updated following review meeting UCD Legal, Student Engagement and HR Employee Relations
Brídín Walsh	Draft	18/11/2020	Updated to incorporate some minor textual changes following review by IT Communications Officer
Brídín Walsh	Draft	03/12/2020	Updated to address the comments from the Equality Impact Assessment (EIA), feedback from the UMT IT Strategy Group and feedback from UCD Legal
Brídín Walsh	Draft	10/12/2020	Updated to incorporate final updates from UCD Legal relating to confidentiality and FOI
Brídín Walsh	Draft	22/12/2020	Submitted for approval by UMT
Brídín Walsh	Draft	27/01/2021	Section 7 reviewed with UCD Legal and proposed changes agreed at the UMT GDPR & Data Group meeting on 27th Jan.
Brídín Walsh	V2.0	02/02/2021	Approved by UMT