UCD Information Technology Services Acceptable Use Policy

To safeguard individuals and to ensure the integrity and reliability of information services, UCD has a number of Use Policies. These are designed to ensure that the University can offer the widest possible range of services to its community. The Policies are not intended to limit use of the University's information services.

Nothing that follows in this document attempts to limit academic freedom as set out in the Universities Act (1997) as follows:
"A member of the academic staff of a university shall have the freedom, within the law, …. to question and test received wisdom, to put forward new ideas and to state controversial or unpopular opinions and shall not be disadvantaged, or subject to less favourable treatment by the university, for the exercise of that freedom."

Your privacy

The University is committed to maintaining your privacy. You should be aware that records are kept of usage and could be made available in accordance with the relevant UCD policies and external legal or regulatory requirements.

Usage limits

In general, the computer resources of the University may not be used for:

- Illegal acts
- Activities in breach of University policies
- Personal commercial activity unless specifically authorised.

Only staff of the University, registered students or other approved users may make use of the University's information services that are not available to the general public. Unauthorised use may lead to internal disciplinary action or investigation by external authorities.

Terms & conditions

The following highlight a number of areas that you must pay particular attention to:

Irish law

Your access to the University's information systems and services is subject to Irish law. Users are required to familiarise themselves with Irish law in all areas that apply to their role in the University.

University policies

The University defines policies in relevant areas to which all users are subject. You are required to be familiar with and comply with UCD policy in all areas that apply to your role in the University.

Access rights

You may be provided with accounts and passwords or other credentials to permit access to the University's information services. You must take reasonable precautions to prevent unauthorised use of such accounts. In addition, you must ensure, in so far as practicable, that information systems and data for which you are responsible are not used for unauthorised purposes.

Advice and practical help is available to help safeguard data, systems and computer equipment.

Use of the UCD network

You must behave reasonably in your use of University resources. You must not undertake or facilitate any activity that could jeopardise in any way, the integrity, reliability and performance of these resources, or compromise their utility or availability to other UCD users. Any devices connected to the UCD network must comply with the requirements of UCD IT Services. Wilful damage (or attempted damage) to Information resources or services will result in disciplinary action, which may include prosecution under appropriate legislation. Likewise deliberately wasteful use of resources and time could lead to a withdrawal of services or severe disciplinary action.

Security and viruses

You must take reasonable care to ensure that you do not transmit viruses or other malicious computer code to other users. The University provides guidelines and practical help to all users to protect their computers. If you suspect that UCD data, systems or services have been abused or otherwise compromised, for example by a virus, you must notify IT Services immediately. You must also take reasonable steps to ensure that the impacted system is isolated from networks and other systems.

Indecency, libel and privacy

It is not acceptable to view, download, transmit or store any offensive, indecent images or material. Nor is it acceptable to attempt to access any systems, data or records for which you are not authorised.
You may not use the University's information services to publish or transmit anything that is libellous or defamatory or is damaging to another computer system. Neither may you deliberately misrepresent your views as those of the University or any other person or organisation. Such action will be regarded as a serious disciplinary matter.

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.

Data & data protection

Data and information are 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 confidentially 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 as may be amended). You must also be aware that the Freedom of the Information Act (1997-2003 as may be amended) applies to records held in any format.

Penalties & agreement

A failure to abide by this Policy may result in being denied access to services as well as other proceedings.

This Policy on Information Technology Services Acceptable Use Policy supersedes all previous policies on acceptable information services use and will be amended from time to time as required. Any user of University information services is deemed to have made themselves aware of these policies.

User Policy

IT Service accounts are issued to three broad categories of user in UCD, namely: Staff, Students and limited service users. Each group has distinct service requirements, defined by their overall relationship with UCD. For all accounts, the person or entity issued with the account is responsible for all assets, data and activity conducted or used via the account.

- **Student Accounts** are issued exclusively on their registration status with the University, and for the periods for which they have a valid registration status. Access to services is defined for systems and services based on the requirement to participate effectively in the University's study programmes and is contingent on compliance with University policy, regulations and external regulatory compliance. University Graduates retain access to their student accounts with a reduced set of services.
- **Staff Accounts** are issued to members of UCD staff who hold a position of employment with the University as their primary role in the organisation.[1] Staff accounts provide a baseline for information services and service provision within the University. All members of staff following normal retirement retain staff accounts and access to a reduced set of services.
- **Limited Service Accounts** are issued to defined categories of individuals, devices and organisations based on a requirement approved by UCD's Chief Technology Officer. Each account type must have a service profile approved by the respective service owners, and may only be issued for a limited period of time or to accommodate a specified purpose.

UCD IT Service accounts are issued to people or organisations arising from a requirement to access information systems, networks and services. Possession of an IT Services account does not entitle a user to assert that they are acting for or on behalf of the University.

Account ownership

UCD retains ownership of all accounts, data and services arising from accounts issued by UCD. Users are responsible for all activity and data in their accounts and are required to conform to the University's policies regarding use and behaviour. Individual users must not share their access or credentials with any other person, entity or service. Users must follow IT Services and service owner advice and procedures to protect and manage their access to services and data.

Where access to staff or limited service accounts is shared or delegated arising from a UCD operational requirement that cannot otherwise be accommodated, the person or organisation issued with the account remains responsible for all activity on the account. Service owners may separately define more restrictive policy criteria on the use of shared accounts.

Provisioning: Access to services

As far as possible, service access provisioning and control shall be automated for all account types. With this as a key objective, service access for accounts is broadly defined in IT Services for staff and students, and includes personal email and storage; access to the University's campus and extended networks, and access to information systems and services in a manner consistent with their role. Changes to access may be requested by individual users or information owners, and must be approved and implemented by the information owner.

For Limited service accounts, baseline access does not include access to any systems or services. A separate schedule of limited account service profiles is maintained by IT Services.

Removal of service access

IT Services may withdraw service access from any user arising from a suspected breach of University policy; or where a security incident is suspected, or in the event of an authorised request from University or external regulatory authority. In this event, the user shall be notified via available mechanisms, which may include notification to their Unit, Sponsor, School or programme administration.

[1] Postgraduates and other students with paid roles do not have a primary role as staff. Staff registered on a course of study have a separate identity and role as students.

Withdrawal of access shall be for a period of time to be determined by IT Services as necessary to assess or remediate any incident, and return of service access may be contingent on the completion of a University disciplinary or external regulatory process. Service may be permanently withdrawn by IT Services arising from such process.

Ordinary removal of access

Authorised access to all accounts ceases from the expiry date of the underlying relationship with the University.

For Students, the expiry date is the end date for the last term for which they have a valid registration status. For students on a continuing course, account access is continued through to the start of the next term, subject to their continued registration status. For graduating students, access is continued up to the issue of final exam results on their course, after which services are reduced to those available to graduates.

For Staff, the expiry date is their final date of employment, or the commencement of a period of long term absence from the University (e.g. career break). Staff who retire retain access to a reduced set of services.

For limited service accounts, the expiry date or sponsored duration is as stipulated in the service plan for the account type.

For staff and students, a discretionary grace period may be provided for expiring accounts to facilitate UCD operational requirements. For sponsored accounts, there is no grace period.

Networks and Systems Policy

Registered users are entitled to use the University's network and information services for their academic requirements. Use of the University's network and information services requires the agreement of the user to comply with UCD regulations and agreement of the user to respect the rights and privacy of all other users. Registered users automatically agree to these regulations when they apply for:

- An IT Services account
- Device registration for access to the UCD network

Users of unregistered networks are deemed to have made themselves aware of the UCD Information Technology Services Acceptable Use Policy and infringement of this Policy will give rise to sanctions and penalties as laid down in the staff and student disciplinary procedures.

Network Zones Introduction

UCD IT Services provide a number of different networks for staff and student use. These are as follows:

Network	Description	Registration Required
CPA (Cabled Private Access)	Staff network	Yes
COA (Cabled Open Access)	Student network	Yes
WaveLAN / UCD Wireless	Open access Wi-Fi network	No
Eduroam wireless	Authenticated Wi-Fi network	Yes
NPN (non-person network)	Pervasive computing	Yes

Desktop or laptops equipment connecting to the cabled networks must be registered with IT Services.

Network Access Procedures

Staff and students are entitled to connect personal computers, mobile phones and tablets to the University network. In some cases there is a requirement that these personal devices are registered in line with the registration procedures laid down by IT Services.

Networks Management

In order to ensure the provision of acceptable levels of service to the UCD Community, the UCD network is managed and maintained by IT Services. Network equipment, wireless equipment or software which simulates network equipment (e.g. bridging) may not be connected or installed without explicit written agreement from IT Services. Unauthorised equipment will be disconnected from the UCD network.

Wireless networks can only be setup with prior authorisation and agreement. UCD IT Services has local authority for the installation and operations of all wireless equipment. Wireless networks operating outside of this remit will be removed from the UCD network.

Configuration

All personal computing devices must be configured to obtain an IP address automatically allocated by IT Services. Users must configure their devices to use DHCP method and should not under any circumstances use fixed or hardcoded IP addresses. IT Services do not allocate a specific address to client equipment.

Server Equipment

All server equipment must be registered by the UCD staff owner with IT Services, and renewed on a periodic basis. Administrators of servers must ensure they are fully aware of security requirements, and manage their equipment accordingly. Servers, which present significant risk, found to be the source of an incident, or compromise performance may be removed from the network. Security and risk management for servers is the responsibility of their registered owners.

IT Services provide software, service advice and support to users in maintaining a secure environment. Specific provision is made for servers in Colleges, Schools or belonging to individual staff users.

Servers are allocated a fixed IP address and DNS name. Server registration must be renewed on an annual basis or as otherwise requested by IT Services.

The staff member is responsible for securing the equipment, ensuring that use complies with this Policy, and that the server does not impact on general or network performance.

Internet access to servers is provided on a per protocol\application basis. Server owners are required to request their services be made available externally according to processes defined by IT Services. Remote access to servers for administration is available via the UCD IT Services remote access services.

End User Equipment

IT Services licences and provides security and virus protection software for all staff and students, including automated updates. Virus protection and update services must be installed on all equipment connected to UCD network. Security advice and support is available on our web site for personal devices. All equipment should have an up to date operating system and relevant software patches installed. All equipment and accounts must be protected by a secure password. It is the responsibility of staff and students to ensure that their equipment is secure. Equipment which is not secure or which has been compromised will be removed from the network. IT Services routinely scan the network and equipment to ensure adequate security and performance.

Pervasive Computing and other devices

IT Services operate and manage specialist networks for pervasive computing devices, which require network services. Access to these networks is managed by IT Services and all devices that wish to use these networks must be registered. Unauthorised equipment will be disconnected from the UCD network.