



Digital Resources

Acceptable Usage Policy

Purpose.....	2
Scope.....	2
Definitions	2
Policy Statement	2
General	2
Licensing and Copyright	3
Legal Context and Consequences.....	3
Artificial Intelligence (AI) Systems	4
Access to DCU Data & Monitoring Digital Resources	4
Roles and Responsibilities.....	5
Sanctions and Reporting Breaches	5
Related Documentation	5
Contact.....	6
Policy Review.....	6
Version Control	6

Purpose

The purpose of this policy is to define the University's policy on acceptable and unacceptable usage of its digital resources.

Scope

This policy applies to all:

- Units of the University, both academic and professional, including its subsidiary campus companies and its research centres (all hereinafter collectively referred to as the 'University' or 'DCU');
- Staff and students of the University who use its digital resources; &
- External parties (e.g. agents, contractors, visitors, etc.) operating within a DCU campus and/or acting on behalf of DCU.

For the purposes of this policy, staff, students, and external parties as described above are collectively referred to as 'users.'

Definitions

Digital Resources	This is defined as all Information and Communications Technology (ICT) that supports the normal business activities of the University.
--------------------------	--

Policy Statement

General

1. The University provides digital resources to users to support its educational, research and administrative activities (i.e. its business purposes).
2. DCU provided digital resources are not to be used for any illegal or unethical purposes.
3. DCU provided digital resources are provided solely for DCU business purposes.
4. Reasonable storage quotas will apply on all systems and users must keep within the allocated quota.
5. Users are individually authorised to access the University's digital resources in line with the [Digital Identity Retention Policy](#). Accounts are created as needed for users on relevant systems and networks. Each user is responsible for the content, usage, and all activities conducted under their account. Account passwords must not be shared with others. Users must not compromise the integrity, performance, or

- reliability of the University's digital resources. Users must not attempt to bypass security controls, hack into systems, or interfere with their intended operation.
6. Users must participate in cybersecurity awareness training when offered by the University and must take appropriate precautions to protect the University's digital resources from malicious activity.
 7. Users must not interfere with, or attempt to access or copy or share, any data which is not explicitly required as part of their role and must comply with DCU's [Digital Access Control Policy](#), [Personal Data Retention Policy](#) and [Data Privacy Policy](#).
 8. Users must not impersonate others or send messages that falsely appear to originate from someone or somewhere else.
 9. Digital resources must not be used to access, store, create, display, or transmit any illegal, offensive, obscene, or indecent material, except for properly supervised and lawful research purposes with appropriate ethical approval.
 10. Users must not deliberately waste or unfairly monopolize digital resources.
 11. Users must not engage in any activity using University digital resources that could bring the University into disrepute.

Licensing and Copyright

1. Users of University digital resources should be aware that copyright law applies to all materials accessed or published on the Internet. Unless explicitly stated otherwise, online content should be assumed to be copyrighted.
2. Users must ensure their online activities do not violate intellectual property rights, including copyright.
3. Uploading copyrighted material (e.g., images, videos, music, software) to University digital resources is prohibited without prior permission from the copyright owner.
4. Users must adhere to all licensing agreements entered into by the University and avoid infringing on software or documentation copyrights. Illegally acquiring, copying, using, or distributing software is prohibited.

Legal Context and Consequences

1. Users must comply with all applicable laws governing the use of computing resources, including those related to AI systems, copyright, privacy, and data protection.
2. Breaching copyright laws may lead to legal proceedings, financial penalties, or, in some cases, criminal prosecution. The University disclaims all liability for such violations.
3. Accessing or modifying data, including programs, without authorisation is a criminal offence under the Criminal Damage Act 1991. Convictions under this Act may result in fines, imprisonment, or compensation payments to affected parties. In certain cases, parents or guardians may also be held financially responsible.
4. Users are responsible for ensuring their actions comply with all relevant legislation.

Artificial Intelligence (AI) Systems

1. The use of any AI systems (as defined in the EU AI act) by users must adhere to the EU AI Act.
2. In particular, users must be aware of the EU AI Act's definition and treatment of 'high risk' and 'unacceptable risk' AI systems. The use of such systems is not permitted by DCU users.
3. Users are fully responsible to ensure that their use of AI systems does not compromise the security, privacy, or integrity of the University's data, systems, or intellectual property.
4. Users are fully responsible for their sharing or publishing of content generated by AI systems. AI systems regularly produce inaccurate, biased or copyright material in their outputs.
5. When using AI systems, staff and students must adhere to all relevant University policies, guidance and statements, including but not limited to the [DCU Position Statement on the use of Artificial Intelligence tools](#), the [Academic Integrity Policy](#), [Data Privacy Policy](#), and [Research Integrity Policy](#).
6. DCU data of any kind must not be entered into any AI system outside the control of the University.

Access to DCU Data & Monitoring Digital Resources

1. The DCU Data Classification Policy and any relevant Record of Processing Activities (ROPA) must be adhered to when collecting, storing, retrieving, consulting, disclosing/sharing, erasing, or destroying DCU data using digital resources.
2. The University reserves the right to monitor the use of its digital resources.
3. The University may access any systems, files, records, or logs connected to a users DCU digital identity, without their consent, in the following circumstances:
 - i. When required by, and consistent with, law.
 - ii. When there is a substantiated reason to believe that violations of law, or of University policies or Codes of Conduct, have taken place.
 - iii. Under time-dependent or critical operational circumstances, such as circumstances where access is needed to comply with legislation or failure to act could expose the University to unacceptable risk or seriously hamper the ability of the University to function.
 - iv. Access under these conditions must be authorised by the Chief Operations Officer (COO), in advance and in writing, or exceptionally by such other University Officer as the President may nominate, with the President being formally notified in every instance.
 - v. Normally, reasonable steps shall be taken to inform the affected individual by the requester of the actions taken and the reasons for them. There may be exceptional circumstances when this is not possible or appropriate, in which case the requester should inform the COO about the nature of these circumstances.

Roles and Responsibilities

1. Users have a responsibility to be aware of this policy.
2. Heads of Schools and Units play a key role in promoting awareness of this policy and supporting its application within their departments.
3. The Chief Operating Officer has a role in the approval of access to a user's data as outlined in this policy.
4. The Director of Digital Technology Solutions has the overall delegated responsibility for coordinating the day-to-day operation of this policy.

Sanctions and Reporting Breaches

The University expects all users to adhere to this policy to ensure a safe, secure, and respectful digital environment for everyone.

Where there are concerns about a potential breach of this policy, the University will review the matter in line with its existing regulations and disciplinary procedures. Any action taken will be proportionate and conducted with fairness and due process. This may include (but is not limited to):

- a) Engaging the University's staff disciplinary procedures as outlined in Statute No. 5 of 2010: *'Suspension and Dismissal of Employees'*
- b) Engaging the University's student disciplinary process in accordance with the *Student Code of Conduct and Discipline*

The University reserves the right to report breaches to An Garda Síochána where it believes a criminal offence may have been committed.

Breaches of this policy may be reported to:

1. The Director of Digital Technology Solutions
2. The Vice President for People, Equality, Diversity and Inclusion (for staff)
3. The Vice President for Academic Affairs/Registrar (for students)
4. The Chief Operations Officer

Related Documentation

This policy should be read in conjunction with the following:

1. Academic Integrity Policy
2. Code of Conduct for members of the Governing Authority
3. Data Classification Policy

4. Data Privacy Policy
5. Data Retention Policy
6. Digital Access Control Policy
7. Digital Systems & Cloud Services Policy
8. Digital Identity Retention Policy
9. Employee Code of Conduct
10. Intellectual Property Policy
11. Network Connectivity Policy
12. Password Policy
13. Position Statement on the use of Artificial Intelligence tools
14. Research Integrity Policy
15. Student Code of Conduct & Discipline


Contact

Further queries or clarifications on any aspect of this policy can be sought from the Director of Digital Technology Solutions.

Policy Review

A review of this policy will be carried out every three years at a minimum.

Version Control

Document Name	Digital Resources Acceptable Usage Policy		 Ollscoil Chathair Bhaile Átha Cliath Dublin City University
Unit Owner	Director of Digital Technology Solutions		
Version Reference	Original Version - 1.0	Reviewed Version	
Approved by	Executive	N/a	
Effective Date	April 15 th 2025	N/a	

End.