Use of IT Facilities Policy
Effective from 26/10/2016

---

1. Purpose
The University provides IT facilities for use by students and staff for the purpose of their studies and/or employment.

2. What is covered by the policy?
This policy applies to all use of University-provided IT facilities, including, but not limited to, University-managed hardware, software, and network resources. This includes computers, mobile devices, cloud storage, collaboration platforms (e.g., Office 365, Teams), internet access, data storage systems, licensed software, and personal devices connected to the University network.

3. Who does the policy apply to?
This policy applies to all staff (including emeritus staff) and registered students of the University and to visitors to the University who are authorised to use the facilities.

4. Roles and responsibilities
- **Director of IT -** Responsible for overseeing IT policy implementation and ensuring alignment with University strategy.
- **Heads of Department/Units -** Promote policy awareness within their departments and escalate concerns to IT Services.
- **Users (Staff, Students, Visitors) -** Responsible for familiarising themselves with this policy and their use of IT facilities is compliant.
- **Student Services and People Services -** Responsible for any investigations and subsequent action taken to address non-compliance.

5. Policy
- **a.** Each user of University computing systems is personally assigned a login name and email address. It is the user's responsibility to keep their login credentials secure, and their password must not be shared with any other person.
- **b.** Users must not use the resources in such a way that the work of other users, the integrity of the computing equipment or any stored programs or data may be jeopardised.
- **c.** At its sole discretion, the University normally permits personal use of these facilities subject to the terms of this policy. Such personal use must not:
  - Incur significant cost, nor consume significant amounts of time.
  - Interfere with the legitimate use of the facilities by others.
  - Infringe any law, nor any other University policy or rules.
- **d.** Use of social media should be in line with corporate guidelines. See Social Media Policy within People Services Policies.
- **e.** Newcastle University takes its responsibility under the Counter-Terrorism and Security Act 2015 extremely seriously. You must not deliberately create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist, except where required for academic purposes and for which prior ethical approval has been obtained.
- **f.** Other than as provided in law:
  - The University accepts no responsibility for the malfunctioning of any equipment or software, nor failure in security or integrity of any stored program or data.
  - No claim shall be made against the University, its employees or agents in respect of any loss alleged to have been caused whether by defect in the resources or by act or neglect of the University, its employees or agents.

6. Related regulations, statutes, and policies
This policy is supplemental to the general practice and regulations of the University.

7. Procedure to implement the policy
- **a.** The University monitors and logs usage of its IT facilities (including email and voicemail) for the purposes of:
  - Efficient operation and management of those facilities;
  - Ensuring compliance with its statutory obligations; and
  - Ensuring that the rules and policies governing use are adhered to.

b. The University will comply with lawful requests for information from law enforcement and government agencies for the purposes of detecting, investigating or preventing crime, and ensuring national security.

c. This policy is supported by the University's Statement of Internet Use published within People Services Policies.

8. Monitoring and reporting on compliance

What will be monitored?	Frequency	Method	Who by	Reported to
Use of IT Services as per **Section 7**	Ongoing	As appropriate (Breach dependent)	NUIT	Line Management (as appropriate)

9. Failure to comply

a. Failure to abide by this policy may result in suspension of login facilities, without warning.

b. A breach of this policy may be investigated under the appropriate University disciplinary policy and procedures.

c. Where an alleged offence has occurred under relevant law, it will be reported to the appropriate authority. Breach of any applicable law will be regarded as a breach of this policy.

Document control information		
Does this replace another policy? **No**		
Approval		
Approved by: Executive Board	**Date:** 24/06/2025	
Effective from: 26/10/2016		
Review due: 12/06/2029		
Responsibilities		
Executive sponsor: Nick Collins		
Policy owner: Director of IT, NUIT		
Person(s) responsible for compliance: All Heads of Department/Units		
Consultation		
Version	**Body consulted**	**Date**
v1.2	Uplifted to new template – Governance and Operations Manager and Head of IT Business Management	12/06/2025
v1.1	Approved by Staff Committee	23/01/2017
v1.0	Approved by Digital Campus Steering Group	26/10/2016
Equality Impact Assessment: YES~~/NO~~		
Initial assessment by: Lisa Renney	**Date:** 20/06/2025	
Key changes made as a result of Equality Impact Assessment: TBC		
Document location		
https://newcastle.sharepoint.com/docs/Information%20Data%20and%20IT%20Policies/Forms/Policies.aspx		