Statement of Internet Use

1. **Introduction**
   This statement sets out the University's position on the use of Internet facilities by colleagues.

2. **Scope**
   - **2.1.** The document applies to all colleagues, including visiting, honorary and guest colleagues of the UK, NuMed Singapore and Malaysia campuses,
   - **2.2.** The University provides many facilities for use by colleagues during their employment. One of the facilities provided gives access to the Internet (including, but not limited to, web browser and e-mail packages,). This document covers all access to the Internet by colleagues, in any way and at any time, when University facilities, equipment or connections are involved, including access from outside University premises.

3. **Standards**
   - **3.1.** These facilities are provided for use by colleagues in connection with their employment by the University. At its sole discretion, the University normally permits colleagues to use the facilities for personal use subject to the following conditions:
     - **3.1.1.** Such use does not incur significant cost, nor consume significant amounts of work time;
     - **3.1.2.** Such use does not interfere with the legitimate use of the facilities by others;
     - **3.1.3.** Such use does not infringe any legislation, nor any other University policy or rules;
     - **3.1.4.** Colleagues accept that the University monitors usage of its facilities to an extent necessary for the efficient operation and management of those facilities, to ensure compliance with its statutory obligations, and to ensure that the rules and policies governing use are adhered to.
   - **3.2.** This discretion is exercised jointly by the Line Managers/Heads of Academic and Service units and by the University IT Service (NUIT) and may be withdrawn if any of the above conditions are violated. Serious or repeated violation will lead to disciplinary proceedings being initiated, and may lead to disciplinary action under the terms of the relevant disciplinary procedure. Non-employees who are found to be in breach of these conditions may have their access to the facilities withdrawn. Other actions, including withdrawal of their permission to work in the University may also be taken when there has been a serious or repeated breach.
   - **3.3.** Relevant legislation includes:
     - **3.3.1.** The Computer Misuse Act 1990, particularly in attempting to secure unauthorised access to or affecting the reliability of computers or information they hold;
     - **3.3.2.** The Data Protection Act 1998, particularly in relation to holding, disclosing or transmitting personal data;
     - **3.3.3.** The Criminal Justice and Immigration Act 2008, particularly in relation to extreme pornographic images;
     - **3.3.4.** The Protection of Children Act 1978, as amended by the Criminal Justice and Public Order Acts 1994, particularly in relation to indecent images of a child;
     - **3.3.5.** The Terrorism Act 2006, particularly in relation to the encouragement of terrorism and dissemination of terrorist publications;
     - **3.3.6.** The Communications Act 2003, particularly in relation to the transmission of grossly obscene or offensive messages and messages designed to cause annoyance, inconvenience or needless anxiety. Also regarding fraudulent use of a telecommunications system;
     - **3.3.7.** The Regulation of Investigatory Powers Act 2000, particularly in intercepting or disclosing messages except in the cause of duty;
     - **3.3.8.** The Copyright, Designs and Patents Act 1988, particularly in copying programmes or data, publishing works of art or performances of music and/or video images;

3.3.9. The Sex Discrimination Act 1975, Race Relations Act 1997 and Race Relations (Amendment) Act 2000, in relation to publishing or receiving material, which is discriminatory or encourages unlawful discrimination;

3.3.10. The Protection from Harassment Act 1997, in relation to unlawful harassment, including the use of electronic media such as e-mail;

3.3.11. The Fraud Act 2006, particularly in relation to fraud by false representation. This includes submitting false statements in any form to any computer system or device designed to receive or respond to communications;

3.3.12. Laws of Defamation, in relation to any statement, comment or innuendo about another individual or organisation, which cannot be justified.

3.4. Relevant University policies include those on Equal Opportunities, Dignity at Work, Sexual, and Racial Harassment. Arising from these policies, it is not acceptable for colleagues to create, access, download, retain, distribute or disseminate any images, text, materials or software which:

3.4.1. Are or might be considered to be indecent or obscene;

3.4.2. Are or might be offensive or abusive in that its content is or may be considered to be a personal attack, rude or personally critical or demeaning, sexist, racist or personally harassing or which could bring the University into disrepute.

The content of any e-mail messages sent must be lawful, and not include defamatory or libelous statements. Care should be taken to ensure that it is clear whether the views expressed are those of the University, or whether the author is representing his/her personal views, where this could have implications for the University.

Severe breaches of this policy, for example by downloading material of a pornographic or unlawful nature, may be treated as gross misconduct, which could lead to summary dismissal and could result in criminal proceedings. In the event of any uncertainty, or where colleagues may be working with material covered by the above descriptions, they are advised to consult with either their Head of Academic/Service Unit or relevant People Services Manager.

3.5. Colleagues are also advised that use of these facilities is also governed by the Rules of Use issued by NUIT and by the Computer Users Agreement, also issued by NUIT. Use of the Joint Academic Network (JANET) is also governed by the JANET Acceptable Use Policies. In addition, NUIT issue a range of guidance notes, which provide helpful advice on responsible use of IT facilities.

3.6. The University monitors usage of its Internet facilities to an extent necessary for the efficient operation and management of those facilities, to ensure compliance with its statutory obligations, and to ensure that these rules and other policies governing use are adhered to. Such monitoring will normally concern data volumes and traffic; content will only be monitored where a breach of the above policies is suspected (e.g. excessive or inappropriate personal use).

3.7. Colleagues are reminded that the University provides e-mail services for business purposes and that personal use is at the discretion of the University. The University reserves its right to be able to monitor all e-mails to the extent required by or permitted by law to enable it to fulfil its operational, legal and contractual obligations to ensure operational, legal and contractual and policy compliance and/or to safeguard health and safety. Colleagues should also bear in mind that their colleagues may need to monitor for work purposes, business related emails received during their absence.

3.7.1. Colleagues may wish to grant a work colleague delegate access to their e-mails in the interests of business continuity and efficiency. This is an additional means of ensuring that business related communications could be processed during periods of staff absence.

3.7.2. Since delegate access enables all e-mails within the delegated mailbox to be read, it is to be emphasised that delegate access should only be used to access business related e-mails. E-mails which in their unopened state appear not to relate to the business of the University, e.g. e-mails that are marked 'personal' in the header,

should not be accessed unless there are convincing grounds on which to believe they are in fact business related.

3.7.3. Colleagues who misuse their delegate access, which may include accessing e-mails, which are clearly personal, could face criminal or civil and/or disciplinary action.

3.7.4. Colleagues who wish to keep personal e-mails and folders private can help avoid any accidental access by clearly labelling such items as "personal" in relevant folder names and e-mail subject lines. Alternatively, colleagues may wish to use a personal e-mail account on an externally hosted mail service such as Gmail, Hotmail, etc.

3.7.5. Colleagues are not required to grant delegate access and there are circumstances where it may not be appropriate. However, in this situation, where there is no delegate access to a colleague mailbox, and the colleague is absent from work, the system controller may grant a written authorisation to a Head of Academic or Service Unit to access that mailbox if access is required for a specific business purpose. As with delegate access, an authorisation only allows access to business related e-mails. Colleagues who misuse an authorisation, which may include accessing e-mails, which are clearly personal, could face criminal or civil and/or disciplinary action.

3.8. It should also be remembered that e-mail should not be regarded as a confidential medium of communication; care should therefore be taken regarding the content of e-mails, and its use generally as a means of exchanging private or confidential information.

4. Related policies and regulations

- *See*: Use of IT Facilities Policy within Information, Data & IT Policies - All Documents.
- Regulation of Investigatory Powers Act 2000 ("RIPA")
- Newcastle University has given authority to the Director of IT to act as the person with the right to control the operation and use of all telecommunications systems and services provided by Newcastle University ("system controller"). Where delegate access in **3.7.1.** relies on the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 to provide for lawful interception of a communication, that conduct has the implied consent of the system controller.

Document control information		
Approved by: Executive Board	**Date:** 24/06/2025	**Version**: v1.1
Review due: June 2029		
Document owner: Director of IT		
Document location: https://newcastle.sharepoint.com/docs/HR%20Policies/Forms/Policies.aspx		
Consultation		
Version	**Consulted and amendments**	**Date**
1.1	Uplifted into new template – Governance and Operations team.	August 2024
1.0	Staff Committee - Approved	November 2005
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		