Policy on Use of IT Facilities

1. Scope, Governance and Infringement

1.1 The University provides IT facilities for use by students and staff for the purpose of their studies and/or employment. 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. Failure to abide by this policy may result in suspension of login facilities, without warning.

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

1.3 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.

1.4 This policy is supplemental to the general practice and regulations of the University.

2. Key principles

2.1 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.

2.2 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.

2.3 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:

1) Incur significant cost, nor consume significant amounts of time.
2) Interfere with the legitimate use of the facilities by others.
3) Infringe any law, nor any other University policy or rules.

2.4 Use of social media should be in line with corporate guidelines: http://www.ncl.ac.uk/info/socialmedia/guidelines/

2.5 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.

2.6 Other than as provided in law:

1) 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.
2) 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.

3. Monitoring

3.1 The University monitors and logs usage of its IT facilities (including email and voicemail) for the purposes of:

1) Efficient operation and management of those facilities;
2) Ensuring compliance with its statutory obligations; and
3) Ensuring that the rules and policies governing use are adhered to.

3.2 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.

Policy Owner: Peter Dinsdale, Information Security Officer (Compliance), NUIT
Approved by: Digital Campus Steering Group on 26 October 2016
Approved by: Staff Committee on 23 January 2017
Review date: NUIT policies are currently under review, to be revised 2022/23.