

Information Technology Acceptable Use Policy

ADM-ITU 111

Contents

Purpose	3
Organisational Scope	3
Provision	3
Responsibility of Users Use	3
Personal Use	4
Prohibited Activities	4
Authorisation for Use	5
User Security	5
User Awareness	6
Examples of Unacceptable Use	6
Monitoring and Restricting Usage	7
Legislation	8

Purpose

The purpose of this document is to specify the NCIUL policy on the acceptable use of its IT Resources and the sanctions for non-compliance. The policy addresses the need to protect NCIUL and its Data, balanced with the need to support the needs of the students, staff, alumni and associates.

IT Services provides support to students, staff and related third party professionals wishing to make use of NCIUL's IT Resources. Where possible, NCIUL will strive to provide academic freedom however; there are certain obligations that must be adhered to, as detailed in this policy.

Organisational Scope

This policy is a institution wide policy and applies to all Users as defined above.

Provision

IT Services are provided to Users primarily for institutional purposes, i.e. to support teaching, learning, research and professional & administrative activities. In addition, occasional and limited personal use of the facilities by staff and students is allowed. The use of IT Resources should be kept to a minimum and should not obstruct, delay or in any way impede the completion of NCIUL related activities.

Staff should utilise NCIUL provided email accounts as the primary mechanism for email communication within NCIUL and when representing NCIUL about external email communication.

Responsibility of Users Use

Access to NCIUL's IT Services is a right granted to NCIUL Users and NCIUL expects that all Users will act responsibly in accordance with relevant laws, and obligations including, but not restricted to :- licensing, copyright, harassment and libel. Any User utilising IT Resources is deemed to have accepted this Policy and is bound by it.

Should Users be in any doubt as to what constitutes acceptable use, they should seek further advice and guidance from their Line Manager, Programme Leader, Senior Tutor or the IT Service Desk.

Every User must recognise and accept responsibility for the integrity of NCIUL owned IT Resources. Furthermore, all Users of NCIUL owned IT Resources must respect other Users; Control measures are in place to ensure the integrity of NCIUL owned IT Resources therefore; it is the responsibility of all Users to recognise, accept and adhere to these measures.

Users must ensure that NCIUL IT Resources and IT accounts such as email accounts are to be used only for the activities for which they are assigned. Users must also agree not to waste or abuse IT Resources (for example unnecessary excessive printing), interfere with others' use of, or cause harm to others using NCIUL IT Resources.

All Users, including System Administrators, must guard against any activity which disrupts or threatens the viability of NCIUL systems and resources, including those on networks to which NCIUL's systems are connected.

Personal Use

All Users should ensure personal use is reasonable and ensure personal use does not contravene the primary purpose of NCIUL; interfere with, conflict with or take priority over the performance of NCIUL duties, waste resources, deny or impair the service to other users or have a negative impact on NCIUL or other users and when using social media.

Prohibited Activities

Users should NOT knowingly or deliberately receive access, create, change, store, download, upload, share, use or transmit:

- a) any illegal, obscene or indecent images, data or other material, or any data capable of being resolved into such material (other than in the course of properly supervised, lawful and authorised research);
- b) any infected material or Malware whether designed specifically or not, to be destructive to the correct functioning of computer systems, software, networks, data storage and others' data, or attempt to circumvent any precautions taken or prescribed to prevent such damage.

If users do receive or suspect they have received Malware they must immediately cease all use of IT Resources and inform IT Services.

Access to IT Resources using someone else's user name and password is strictly prohibited and is subject to the appropriate disciplinary measures.

In support of NCIUL's Prevent Duty, Users should not knowingly use IT Resources to draw people into terrorism, which includes not just violent extremism but also non-violent extremism, which can create an atmosphere conducive to terrorism and can popularise views, which terrorists may exploit. Users must not access extremist materials unless authorised to do so as part of academic research.

Removal of NCIUL IT Resources from the organisation's premises without prior authorisation is forbidden. If IT Resources are removed from NCIUL's premises, all reasonable actions should be taken to safeguard the resource and protect from theft, loss or damage.

Authorisation for Use

Users wishing to access NCIUL IT Resources must have proper authorisation from the IT department.

Only authorised users are permitted to use IT Resources. Each User is issued with a valid username and password as appropriate. The username and password must be kept confidential and not be shared with anyone else under any circumstances.

NCIUL IT Resources are not to be used for commercial purposes or non-institution related activities without written authorisation from NCIUL.

Unauthorised use of NCIUL IT Resources, intentional corruption or misuse of resources will be regarded as direct violations of NCIUL's standards for conduct as outlined in NCIUL's Code of Conduct.

Such violations may be dealt with by NCIUL's disciplinary processes, as appropriate. In some cases, such violations may also be considered a civil or criminal offense and will be dealt with accordingly.

User Security

Users should make all reasonable efforts to send data that is Malware free and not open email attachments or click on links sent by unsolicited or untrusted sources. Users should ensure any personally owned computer used to access NCIUL IT Resources have regularly updated operating systems & anti-Malware programs thereby protecting NCIUL network as much as possible from accidental or premeditated infection and hacking attempts and attacks. If Users have personal equipment and are unsure about the level of protection on their device should visit the IT Service Desk.

All Users are responsible for all activity that takes place under their usernames and must not allow anyone else to access the IT facilities using their usernames and passwords.

All NCIUL Systems Owners must ensure that their information systems and supporting infrastructure comply with IT Services Policy and current legislation.

Personal IT equipment must not be connect directly i.e. cabled/Ethernet to the NCIUL network, and only use of Wi-Fi is permitted for access.

User Awareness

All Users are expected to;

- Be mindful of, and safeguard NCIUL's reputation.
- Be aware of the permanent record and electronic footprint a user makes on the internet with social media.
- Follow all relevant laws and regulations, including those relating to copyright, extremism, libel and data protection (including the GDPR).

All users are expected to;

- Comply with NCIUL Policies, particularly protecting sensitive or confidential information or material protected by copyright law or the Data protection Act.
- Have appropriate authorisation and technical protection before sending or transmitting NCIUL confidential information external to NCIUL network.
- Comply with all relevant copyright legislation, licences and agreements for software and electronic information resources when accessing and connecting to NCIUL IT Resources.

All staff are expected to;

- Utilise good information security and management practices for the storage, access, retention and deletion of NCIUL Data.

Examples of Unacceptable Use

The points below are provided as examples of unacceptable use, but should not be considered an exhaustive list. Should a User need to perform a task or role which they believe may be considered as 'unacceptable use', they should consult with and seek approval from IT Services before commencing any such activity.

- All illegal activities, including theft, computer hacking, Malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services. These also include activities that contravene data protection regulations.

- All activities that may negatively affect the long-term success of NCIUL. These include sharing sensitive information outside NCIUL, such as research and development information and customer lists.
- All activities for personal benefit only that would have a negative impact on the day-to-day functioning of NCIUL. These include activities that slow down the computer network e.g. streaming video, playing networked video games (except within student halls).
- All activities which may cause offence to other users, such as those related to the protected characteristics under the Equality Act 2010 – specifically, in relation to sex, sexual orientation, race, age, gender or gender reassignment, marriage or civil partnership, pregnancy or maternity, religion or belief, and disability.
- All activities deemed inappropriate for NCIUL to be associated with and/or are detrimental to NCIUL's reputation.
- Circumventing the IT security systems and protocols, that NCIUL has put in place.

Monitoring and Restricting Usage

NCIUL reserves the right to limit, restrict, or extend IT Resource privileges, and access to its information resources.

NCIUL also reserves the right to deploy software and systems that monitor, block or record network activity for productivity and/or investigational purposes.

There will be circumstances under which NCIUL may have a legitimate need to read private computer data, including e-mail records or to monitor electronic transmissions. These circumstances include:

- Compliance with legal obligations in judicial proceedings.
- Requests from law enforcement authorities.
- IT system administration and maintenance.
- Investigation of suspected violations of NCIUL policy.
- Subject Access Requests or requests under the Data Protection Act
- Freedom of Information requests

Access privileges may be revoked or other sanctions imposed by the IT Services or HR for violations of this policy and the supporting processes, as deemed appropriate.

Legislation

Applicable legislation includes those listed below. This list is not exhaustive and may be subject to change in accordance with changes in legislation.

[Human Rights Act 1998](#)

[Equality Act 2010](#)

[Computer Misuse Act 1990](#)

[Copyright Designs and Patents Act 1988](#)

[Data Protection Act 1998](#)

[GDPR \(14 April 2016. Enforcement date: 25 May 2018\)](#)

[Defamation Act 2013](#)

[Telecommunications Act 1984 & Communications Act 2003 \(subject to updates\)](#)

[Freedom of Information Act 2000 \(subject to updates\)](#)

[Anti-terrorism, Crime and Security Act 2001](#)

[Counter Terrorism and Security Act 2015](#)

Document owner:	IT Services
Created:	03/2017
Last reviewed:	03/2019
Responsibility for review:	IT Services Equality and Diversity Committee
Date of next review:	09/2019
Related documents:	
Approved by:	IT Services April 2017
Equality impact Assessment undertaken:	04/2017
Version	V2.3 Logo Change