Acceptable Use Policy

Author: Helen Crotty

Version	Updated:	Reviewers:
1.1 – Final Draft	7.12.2021	1. DTS Peer Review 2. DTS Senior Leadership Team 3. Head of Information Compliance 4. Gartner Analyst 5. CISO 6. Legal Services 7. HR Leadership Team 8. Director of Registry and Academic Affairs 9. Director of Communications & Advocacy
1.2 Final Version	24.02.2022	IMSSC approved subject to the addition of a link to the Policy on Eternal Work (added to section 3, para 1).
1.2 Final Version	25.03.2022	IMSSC approved.

University of Nottingham
UK | CHINA | MALAYSIA

1. Overview

This policy covers the rules and required behaviours for using University provided IT Facilities. The policy outlines monitoring of usage and infringements.

The requirements of this policy are in addition to the expectations set in the University Information Security Policy, the University Regulations and the University Social Media Policy for Students and Staff. Staff should also be aware of the guidance supporting Hybrid Working.

All computing use must comply with relevant legislation (see Appendix).

2. Definitions

IT facilities includes hardware, software, data, network access, cloud services, third-party services, online services, and IT credentials.

Users are staff, students, and any other authorised person e.g., associate, contractors, visitors.

The format of university email addresses is:

- Undergraduate and Postgraduate Taught students: username@nottingham.ac.uk
- Postgraduate Researchers and Staff: firstname.lastname@nottingham.ac.uk
- Associates: firstname.lastname@nottingham.ac.uk addresses available upon request.

3. Rules and Behaviours

Computing facilities are provided to support authorised users in the pursuit of their academic activities in line with the Policy on External Work and to support the running of the University. Following the outlined rules and behaviours helps to protect the network and keep the University online.

Users must not commit an offence whilst using University systems. This includes but is not limited to:

- downloading illegal material (e.g., audio, video, illicit content etc.)
- breaching copyright (e.g., using books, music, film, images etc. without appropriate permission or licence)
- hacking
- accessing/replicating pornography
- sending spam e-mail (e.g., unsolicited bulk email etc).
- defamation (e.g., making false statements that would cause harm)
- misuse of private information (e.g., disclosure of personal information to cause harm)
- inciting hatred (such as sending messages to groups that encourage biased views).

The University will not tolerate any form of bullying or harassment by our students or staff, including cyber bullying. The University expects that all staff and students follow the principles set out in Dignity at Nottingham Policy.

Further, users must not:

- let anyone else use their logon or attempt to logon as anyone else
- lend their University Card to anyone
- leave a workstation or PC logged in and unattended
- damage University computer equipment
- interfere with systems or any other user software housed on the University computer systems, e.g., by introducing viruses, denial of service, overloading attacks
- use or attempt to use any networked service accessed from the University for unauthorised purposes
- install unlicensed software on University computer equipment (e.g., Freeware titles are often for 'personal use only' and not permitted to be used on University owned systems).

Users must remember to:

- set a strong password
- always log off when leaving a computer
- take their memory stick or any other removable media with them when they leave
- ensure that personal data is saved and backed up (save often), using university provided cloud storage where possible
- check their emails regularly to keep informed
- plan for and return any loaned IT equipment by the due date
- return any University owned equipment upon leaving employment or study
- check responsibilities before connecting to the internet in Halls of Residence
- attend annual security awareness training
- report any security incidents including:
    - Clicking on a phishing email
    - Accidentally sharing personal data
    - Identifying a control weakness
- keep communal IT work areas tidy and litter free (e.g., in computer rooms, libraries etc.).

Users should note that:

- they are responsible for their personal belongings at all times
- they are responsible for taking due care of any IT equipment they have loaned from the University and for returning the equipment in good working order

- university provided cloud storage should be used where possible to save and share your documents
- removable media, including USB's, connected to any PC or workstation must comply with the University's Information Security policies
- the JANET network is subject to the JANET Acceptable Use Policy
- all software used on University IT equipment must be appropriately licensed, and proof of such licences must be made available on request
- use of licensed services must comply with the license conditions. In particular, use of software/datasets licensed through CHEST must comply with the eduserv agreements and the associated User Acknowledgement of Third Party Rights Form
- If an application is installed on a device, the user is accountable for ensuring that the application is kept up to date
- All stored data (emails, chat, documents etc) could be subject to Freedom of Information and / or Subject Access Requests where the data is personal in nature. For further information see the Information Compliance pages on the website.

Additional Rules When Accessing Sensitive Data

Examples of 'Sensitive Data' include payment/card details, personal information (addresses, date of birth etc), financial data, research data.

When accessing this data, you must:

- follow the rules and guidelines provided by your department
- not send the data to your personal device
- not duplicate any of the data without permission
- ensure that devices are encrypted
- follow the Data Handling Policy and Data Protection Policy.

4. Monitoring and Authorised Access

Communications may be monitored by DTS staff for the business purposes of the University as permitted by UK legislation. The legislation allows the interception of network traffic without consent for purposes such as:

- recording evidence of transactions

- ensuring regulatory compliance
- detecting crime or unauthorised use
- ensuring the efficient operation of university communications systems

Communications could be released to requestors if considered in the public interest under the Freedom of Information Act (2000).

Access to a user's email, files or datastores related to the University's activities may also be granted to a line manager or authorised alternate if the user is unavailable for their normal duties for a period and the materials are necessary for the efficient operation of the University.

University and device ID's may be monitored to track location whilst on campus for the purposes of managing building occupancy and other University business requirements.

5. Infringement

Infringement of the policy may result in disciplinary action under the relevant provisions for staff and students. Disciplinary action may take the form of, but is not limited to:

- withdrawal of computing facilities
- the giving of a formal disciplinary sanction ranging from Oral Warning to Dismissal
- the imposition of a fine (students only)
- the suspension or expulsion of the relevant staff or student

More information can be found on the Staff Disciplinary and Student Regulation webpages.

6. Keeping Informed and Key Contacts

Official communications to staff and students are sent to university email accounts. Staff and students should check their emails regularly to keep informed.

The DTS Services web pages hold further information and help guides to support and optimise your use of the University IT Facilities.

Key contact details:

- Our dedicated IT Service Desk is available to help with all your IT needs
- Our Smart Bars can answer your IT questions
- Your local Campus IT Support Team are available to help

Our IT Status Page

University of Nottingham
UK | CHINA | MALAYSIA

Appendix

All computing use must comply with relevant legislation, which includes but is not limited to:

- Data Protection Act (2018) and UK GDPR 2020
- Human Rights Act (1998)
- Copyright, Designs and Patents Act (1988)
- Computer Misuse Act (1990)
- Privacy and Electronic Communications (EC Directive) Regulations (2003)
- Freedom of Information Act (2000)
- Counter-Terrorism and Security Act (2015).