University of Nottingham
UK | CHINA | MALAYSIA

IT Acceptable Use Policy	
PO-IT/Rev01	16/6/2025

IT Acceptable Use Policy

1 Introductory Purpose & Background

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 all other relevant policies and regulations.

2 Scope

This policy applies to all users of the University of Nottingham Malaysia’s IT facilities, whether accessed on campus or remotely. The policy applies regardless of the device used and includes both academic and non-academic activities.

3 Definitions

IT facilities include hardware, software, data, network access, cloud services, third-party services, online platforms, and IT credentials, all of which are provided to support authorised users in their academic activities and to support the operations of the University.

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

IT Services (ITS) is responsible for maintaining the security, functionality, and accessibility of all IT facilities, and for providing guidance and support to users.

4 Policy

4.1 Key principles

All users must ensure their actions do not compromise the integrity, confidentiality, or availability of the IT facilities. Compliance to this policy is compulsory to ensure responsible use and to maintain the security and integrity of the University's digital environment.

4.2 Rules and Behaviours

Users must not commit an offence whilst using the IT facilities. 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
- bullying or harassment
- 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).

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 any 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 and/or Intranet portal 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 security awareness training (staff only)
- report any security incidents to the IT Service Desk
- keep communal IT work areas tidy and litter free (e.g., in computer rooms, learning spaces, 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 licenses must be made available on request
- use of licensed services must comply with the license conditions. If an application is installed on a device, the user is accountable for ensuring that the application is kept up to date

With respect to data protection and privacy, users must:

- comply with the University's Personal Data Protection and Privacy Policy when accessing or using the IT facilities. This includes handling personal and sensitive information responsibly, ensuring data is collected, stored, and shared in accordance with applicable laws and internal guidelines
- maintain confidentiality, report any data breaches promptly, and take reasonable steps to protect the privacy of individuals and the integrity of our systems

4.3 Monitoring and Authorised Access

In cases where there is suspicion and/or reports of criminal activity, gross misconduct, or acts that warrant investigation, the relevant University authorities may conduct further investigations, which may include the examination or seizure of any University-owned computer, appliance, or media related to the suspected offence.

Examination may include opening and reading emails, files, data stores or any forensic materials deemed relevant to the investigation. The University may disclose information to the Police or other authorities in the case of suspected criminal or relevant activity.

Access to a user's email, files or data stores 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 their location for the purposes of managing devices, monitoring building occupancy and other University business requirements.

4.4 The consequences of non-compliance.

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 IT 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

4.5 How compliance with the policy will be measured.

Compliance with this policy will be measured through a combination of regular audits, system monitoring, and periodic reviews. Automated monitoring tools will track user activity, system configurations, and security event logs to identify deviations from policy standards. Additionally, employees will be required to complete security awareness training and demonstrate understanding through assessments.

4.6 Provisions for monitoring and reporting related to the policy.

To enhance the detection of unauthorised access, suspicious activity, and policy violations, the University has the capability to perform 24/7 monitoring and threat detection. All security incidents are investigated and responded to in accordance with the University's incident response procedures. The University will implement continuous improvements to effectively manage these risks.

5 Review

This policy will be reviewed every 2 years to account for changes in the University's technology environment, regulatory requirements, or threat landscape and approved by the IT & Digital Committee.

6 Communication

Official communications to staff and students are sent to University email accounts or published on the Intranet portal. Staff and students should check their emails and the portal regularly to keep informed.

Key contact details:

- Our dedicated IT Service Desk is available to help with all your IT needs
- Our IT Service Desk PLUS booth can answer your IT questions
- Our IT Status Page

7 Document Change History

Policy name	IT Acceptable Use Policy
Reference number	PO-IT/Rev01
Policy category	Tier 1
Subject	This policy covers the rules and required behaviours for using University provided IT facilities.
Approving authority	IT & Digital Committee
Accountable person	Director of IT
Responsible Team	IT Services
First approved	29/09/2022
Last review date	16/06/2025
Next review date	16/06/2027
Application	University of Nottingham Malaysia
Related documents	UNM Personal Data Protection and Privacy Policy
Related regulations	Personal Data Protection Act 2010