Acceptable Use Policy

1. INTRODUCTION

Whilst the University of Northampton (UON) expects its employees and staff to comply with this Policy, it does not confer contractual rights or form part of any contract of employment. The Policy may be amended by the University or replaced at any time following appropriate consultation and negotiation with recognised trade unions. Breach of this Policy may be addressed via the University's Disciplinary Policy and Procedure, and Code of Conduct Policy.

This Policy will be reviewed by the IT Services and Human Resources departments on an annual basis, with amendments being made on a 3-year basis unless in response to major changes in future legislation and/or case law.

2. OWNERSHIP

The IT Services and Human Resources departments own and manage this Policy on behalf of The University.

3. ORGANISATIONAL SCOPE

This is a University Policy that applies to all employees, students, and contractors of the UON, and any applicable 3rd parties working on behalf of the UON. This also includes any wholly owned subsidiaries, unless an alternative applicable Policy exists. Those in scope will be referred to as 'Users' for the purpose of this document.

4. POLICY STATEMENT

UON IT Resources are provided to Users primarily to support: learning, teaching, research, and professional and administrative activities. The UON seeks to ensure that the IT Resources provided to Users meet legal and social requirements, and are therefore used safely, lawfully and fairly. This Policy applies to all IT Resource usage on UON premises, partnership sites and off premises.

When using UON IT Resources and/or connecting to the UON network off premises, secure and approved remote access protocols and systems must be in place to secure remote working and reduce the risks of remote access (Cloudflare).

Limited personal use of IT Resources by Users, when kept to a minimum, is permitted during breaks and before and after working hours. This usage should not obstruct, delay or in any way impede the completion of UON related activities. This usage is subject to the JANET Acceptable Use Policy and the JANET Security Policy published by JANET (UK) here.

It is the responsibility of all Users of UON IT Resources to read, understand and comply with this Policy and any additional Policies related to their activities, including those relevant to information security.

5. DEFINITIONS

JANET
A high-speed network for the UK research and education community.

IT Resources
All assets that connects to the UON network, and/or contains, accesses, stores, and/or processes UON data. This includes, but is not limited to: desktop computers, laptops, smartphones, tablets, servers, printers, data and voice networks, networked devices, software, applications, electronically-stored data, portable data storage devices, hardcopies, third party networking services, telephone handsets, and video conferencing systems.

Data
Includes but is not limited to any information accessed, stored, and/or processed on/by IT Resources, stored either digitally or hardcopy, in formats including, but not limited to: text, graphics, images, sound, and video.

General Data Protection Regulation (GDPR)

A regulation in EU law on data protection and privacy for all individuals within the EU and EEA.

Authentication
A process that confirms a user's identity.

Encryption
Encryption is the process of converting data to an unrecognisable or "encrypted" form. It is commonly used to protect sensitive data so that only authorised parties can decrypt/view it. This includes files and storage devices, as well as data transferred over wireless networks and the internet.

Anti-Virus
Software designed to detect and remove viruses/malware from a device/network.

System Administrator
Those who manage the computer systems in an organisation.

Web Filtering
Content-filtering software used to filter content delivered over the internet. This determines what content will be available on a machine or network.

Virus/Malware
Software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system or network.

Obscene or indecent content
Inappropriate content that may be offensive and does not conform with generally accepted standards of behaviour, especially in relation to sexual matters. This includes but is not limited to: adult content (pornography), indecent images of children, fights or terrorism related content.

Sensitive Data

There are three main types of sensitive data, including but not limited to: **personal** (this is data from which an individual/individuals are personally identifiable. It includes names, contact details (phone, address, email), initials, financial information. It can include any identifier of an individual, e.g. a job title can be personal data if it alongside other information that would allow someone to identify the individual), **special category** (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, generic data, biometric data, or data concerning health, a person's sex life, or a person's sexual orientation) and **confidential** (information which is confidential to the University for example for business reasons. This can include meeting papers and minutes, proposals for discussion, research and intellectual property, financial information like individual bank details or details of contracts. If you are unsure about the confidentiality of data, check with your line manager or the person/team which originated the data). This data must be protected from unauthorised access to safeguard its privacy and the security of individuals and the organisation.

Single Sign On

Single Sign On (SSO) is an authentication process which allows Users to provide their username and password once to a trusted service and to have their identity securely and consistently provided to other applications, without having to log in more than once.

6. KEY PRINCIPLES

6.1. Acceptable Behaviour

- When using UON IT Resources, Users must not:
  - Attempt to authenticate using another User's or organisation's credentials.
  - Knowingly receive, access, create, change, store, download, upload, share, use or transmit: any illegal, obscene, or indecent content. This includes any data capable of being resolved into such material (other than while material is being properly supervised, is lawful or for authorised research).
  - Knowingly attempt to access, delete, modify, or disclose information belonging to another User without their permission.

- Share sensitive data externally outside the UON, without the authorisation of their line manager. Advice and guidance can be provided by the Data Protection team.
- Cause needless offence to others including posting of inappropriate comments about other Users outside of genuine scholarly criticism and debate.
- Use IT Resources for criminal activities.
- Deliberately or intentionally receive, access, create, change, store, download, upload, share, use, transmit, or otherwise facilitate any terrorist related or extremist material, or any data capable of being resolved into such material as per the University's Prevent Duty under s26(1) of the Counter Terrorism and Security Act 2015, as specified by guidance issued under s29(1) of the Act. Anyone witnessing such material should report it to their line manager/deputy head.
- Take UON IT Resources off premises without prior authorisation. If authorised, all reasonable actions should be taken to safeguard the resource and protect it from theft, loss, or damage.
- Take UON IT Resources overseas without prior authorisation from management.
- Send spam/phishing (unsolicited/malicious email), forge/spoof email addresses, or use UON mailing lists other than for legitimate purposes related to UON or Trade Union activities.
- Deliberately or recklessly consume excessive IT Resources such as processing power, bandwidth, or storage.
- Knowingly undertake any activity which jeopardises the confidentiality, integrity, or availability of IT Resources and data including sensitive data.
- Knowingly undertake any unauthorised penetration testing, vulnerability scanning or monitoring and/or interception of network traffic.
- Seek to gain unauthorised access to restricted areas of the network.
- Setup their own unauthorised Wi-Fi access points on UON premises.
- Use Bluetooth connectivity to send or receive information.
- Participate in 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.

- Knowingly undertake any unauthorised activities which compromise a physical IT Resource, including but not limited to theft, damage, access, or replacement of components/hardware such as storage drives, processors, or memory.
- Attempt to disrupt or circumvent IT security measures.
- In association with the UON Code of Conduct Policy, participate in activities deemed inappropriate for the UON to be associated with and/or are detrimental to the UON's reputation.
- Use internet-based email services (e.g., Hotmail) for UON business purposes.
- Create or build applications for use within a department or business area without being subject to review and approval by IT Services.
- Misuse Administrator/Privileged access to UON IT Resources, including participating in any unauthorised activities.

6.2. Safeguarding of Information

- A User may be held responsible for any serious breach of acceptable use carried out using a connection authenticated with their username, this includes actions taken by others.
- All Users are expected to:
  - Be mindful of and safeguard the UON's reputation.
  - Be aware of the permanent record and electronic footprint they make on the internet using social media.
  - Comply with UON Policies, particularly protecting sensitive data or material protected by copyright law or GDPR/Data Protection Act.
  - Have appropriate authorisation and technical protection before sending or transmitting UON sensitive data externally.
  - Comply with all relevant copyright legislation, licences and agreements for software and electronic information resources when accessing and connecting to UON IT Resources.
  - Be aware of the appropriate procedures for handling UON sensitive data.
  - Only print sensitive data when necessary and authorised.
  - Securely store sensitive hardcopy documents on premises when not in their immediate possession, and not take such documents off premises without authorisation.

- Where possible the '.pdf' (Portable Document Format – Adobe Reader compatible) format should be used, to protect the integrity of documents attached to emails.
- Utilise good information security and management practices for the storage, access, retention, and deletion of UON Data.

6.3. Password Policy

- As part of our GDPR compliance, we are required to ensure we have appropriate safeguards in place. The following Password Policy ensures a consistent and secure approach for the use of passwords for User authentication, prior to access to UON systems and data.
- User passwords must follow the following minimum requirements:
  - Minimum password length of 8 characters.
  - Contain a combination of 3 of the following components:
    - At least one lowercase alpha character.
    - At least one uppercase alpha character.
    - At least one numeric character.
    - At least one special character.
  - Minimum password history of 15 passwords.
  - Minimum password age of 1 day.
  - Maximum 10 allowed failed logins attempts.
  - Minimum account lockout duration of 15 minutes.
  - A form of Multi Factor Authentication (MFA) in place.
- It is recommended that Users use the "three random words" technique to ensure they are using a strong, unique, and rememberable password.
- Initial passwords set by systems/IT Services shall be first-time use only and force a password change.
- If a UON endpoint has been left idle for 10 minutes, Users will be required to re-authenticate to access the device.
- The following are practises that weaken the strength of passwords and should be avoided:
  - The password is a single word found in a dictionary (English or otherwise).
  - The password is a commonly used or personal word such as:
    - Names of family, pets, friends, co-workers, hobbies, etc.

        - Computer terms such as device names, websites, companies, hardware, software.
        - The words "University of Northampton", or any derivation such as site or building names.
        - Birthdays or other personal identifying information such as addresses and phone numbers.
        - Word or number patterns (such as qwerty or 12345).
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
    - Using the same password for UON accounts as for other UON or non-UON accounts (e.g., personal account, forum logons etc.) unless single sign on is available.
    - Sharing passwords with anyone else or writing them down.
    - Communicated the password for a document within the same email communication as the attached document. Passwords should be communicated via an alternative method of communication, such as a password manager, text message, instant messaging or at the very least, a separate, delayed email communication.
- Users using UON endpoints can reset their password by: Click [Ctrl]+[Alt] +[Del] and select 'Change password'.
- Users using their own device can reset their password via: https://user.northampton.ac.uk/sspr/private/login.
- If a User suspects their account or password has been compromised, they should report the incident to the IT Service Desk via www.northampton.ac.uk/help or calling 01604 893 333 (Ext. 3333) and change their password immediately.
- IT Services reserves the right to require a User to reset their password in the event of an account/password compromise alert being triggered against that User's account.
- The effective Password Policy against an account may vary dependant on the User's role or the account's level of privilege access.

6.4. Data Backups

- Users are responsible for ensuring that any information they create or modify as part of their role, is stored in a UON managed system where it will be

automatically backed up; or, if working with information outside UON managed systems, Users are responsible for ensuring that appropriate backup controls are in place.

- Users must ensure that:
  - Information they are working with is saved into the UON storage locations which have appropriate back-ups in place, for example One Drive, SharePoint, UON network storage and UON shared network storage.
  - If information cannot be saved to the UON managed storage for example, when unable to connect to UON systems/network, Users must ensure their information is saved locally on their device and transfer to UON systems as soon as possible.
  - They refrain from using removable media where possible. If it is essential to use it, according to the classification of information contained, Users should consider encrypting the device.
  - They do not leave back-up media in devices after back-ups have completed.
  - They do not keep back-up data in the same physical location as the original data.
  - They do not use cloud storage solutions not provided by UON IT Services (such as Google Drive or DropBox) for UON data.

6.5. Remote Access

- To connect to certain UON IT Resources remotely, for example U4BW, Users must ensure that Cloudflare WARP is configured as 'connected' on their UON device.
- When accessing UON IT Resources from a public/insecure network, Users must note that:
  - Public and Hotel wireless/hot spots are not to be trusted even if they state that they are secure.
  - If connecting to UON systems, sit with your back to a wall to prevent shoulder surfers viewing UON data and/or noting your authentication credentials.
  - Consider the use of privacy screen filters if you spend a significant amount of time working in public spaces.

- Do not place any sensitive hardcopy documents in public view. Ideally such material should only exist in softcopy form except while in a secure UON location.
- Do not leave your laptop or smartphone unattended.
- Damaged, lost or stolen equipment must be reported to the IT Service Desk immediately.
- Do not use non-UON provided devices, non-personal devices, or shared devices to access UON systems as the contents of the screen can be copied, and your logon credentials can be recorded.
- Do not discuss sensitive or confidential subjects within earshot of members of the public.

6.6. Hot Desks

- When using a UON hot desk, you should note the following:
  - Do not leave sensitive hardcopy documents on the desk when you are not in attendance.
  - Do not discuss sensitive subjects within earshot of teams whose access to this information is inappropriate.
  - Lock your screen when leaving your desk.

6.7. Web Filtering

- IT Services blocks sites or protocols on UON networks and restricts access to undesirable content through the firewall. This is based on reputation and cyber risk to the UON, including: computer viruses, malicious software (malware), spam email, phishing, computer hacking, obscene or indecent content, and use of illegal file-sharing that are highly dynamic and volatile in nature.
- Maintaining freedom of access to the internet is acknowledged as being of business importance to the University. Requests for access changes or exceptions for a given website or category of material can be made via a Service Request to the IT Service Desk.
- It is acknowledged that access to sites or material that the UON has agreed to be filtered may be necessary for some research or other academic teaching purposes. IT Services will review the risk and unblock a website or category for the requesting User only, and where possible will limit the timeframe of availability to minimise exposed risk. IT will track approved exceptions.

6.8. UON Staff Mobile Phone Devices

6.8.1. IT Services Responsibilities

- The purchasing and allocation of UON mobile phone devices.
- Maintaining an asset register of UON mobile phone devices.
- The disposal of UON mobile phone devices.
- Itemised bills will be issued monthly to departmental billing administrators for information purposes.

6.8.2. Acceptable Use and Management

- The User should ensure that the mobile phone device is regularly switched on and connected to the internet, to ensure the operating system and antivirus protection remains up to date.
- The User must ensure that the mobile phone device has a PIN or password, and that the device is not left unattended.
- The User must switch off Bluetooth connectivity on the mobile phone device when not in use. If the screen unexpectedly turns on, look and see why. A key flaw in the Bluetooth exploit is that it will turn on the screen if an attacker attempts to do something once connected.
- The need to make and receive personal communications should be limited.
- The purchase of applications for personal use are subject to the User's own expense and not UON's. The use of personal applications should be limited to avoid unreasonable data usage.
- The sending of high volumes of SMS messages is subject to review by line managers.
- Line managers will have responsibility for keeping control of mobile phone device usage by identifying Users who use a mobile device excessively and taking steps to reduce this.
- If it is noted there have been excessive calls made that result in a calling pattern disproportionate to the overall type, amount and duration expected from usage of the mobile device, it is at the discretion of management to initiate disciplinary action, in line with the staff disciplinary Policy.
- Excessive mobile data usage is subject to review by the line manager. If the amount of data used is disproportionate to the amount which would be expected from reasonable use of the mobile device, it is at the discretion of

management to initiate disciplinary action, in line with the staff disciplinary Policy.

- The use of mobile phone devices overseas can lead to potentially significant costs, for example through data roaming, as well as risks to the device. Users must obtain approval from management for overseas travel with a UON issued device. It is the User's responsibility to contact the IT Service Desk before travel to arrange the correct package to be applied to their phone to ensure no unnecessary and avoidable costs are incurred.

6.9. Leavers or Changing Devices

- UON issued devices must be uniquely identifiable and linked to a User.
- The devices are UON property and as such must be returned to IT Services, via the IT Service Desk in the Learning Hub, by the User upon change of User or termination of employment. They must not be disposed of by the User.
- IT Services will manage recycling of the device to another User.
- IT Services will manage the secure erasure of data when disposing of the device at end of life.
- If devices are not returned, the cost of the device may be deducted from salary or processed for recovery via civil litigation.
- Whereby a User has changed job role, they should seek approval from their new line manager to continue their use of a UON mobile, and inform the IT Service Desk of the change for charging purposes.

6.10. Monitoring

- UON recognises that the use of the internet is an extremely valuable business, research and learning tool. Misuse of such tools can have effects on other Users and potentially the UON itself.
- UON reserves the right to conduct scans of the network to determine what devices are connected to it and what services they are operating. Users may not configure their UON device to use any network (IP) or physical (MAC) address other than those allocated to them.
- The UON also reserves the right to deploy software and systems that monitor, block or record network activity for productivity and/or investigational purposes.

- Email messages will be filtered and scanned for inappropriate and malicious content.

6.11. Implementation and Enforcement

- The UON reserves the right to limit, restrict, or extend IT Resource privileges, and access to its information resources. This includes the right for IT Services to periodically review privilege access and revoke access where appropriate.
- There may be exceptional circumstances under which the UON may have a legitimate need to read private computer data, including e-mail records and instant messages, or to monitor electronic transmissions. In deciding what amounts to exceptional circumstances, the UON will have due regard to the fact that emails between representatives, officials, or officers of recognised trade unions and those they represent are sensitive, may represent data that belongs to the recognised unions (as opposed to the UON) and may be subject to the rules of privilege. These circumstances include, but are not limited to:
  - Compliance with legal obligations in judicial proceedings.
  - Requests from civil or law enforcement authorities.
  - IT system administration and maintenance.
  - Investigation of suspected violations of UON Policy.
  - Subject Access Requests or requests under GDPR 2018.
  - Freedom of Information requests.
- Access privileges may be revoked, or other sanctions imposed (in accordance with UON Disciplinary Policy and Procedure) by the CIO or the HR Director for violations of this Policy and the supporting processes, as deemed appropriate.
- Unauthorised use, misuse, or intentional corruption of UON IT Resources will be regarded as direct violations of the UON's standards for conduct as outlined in the UON's Code of Conduct Policy, its Policies, Procedures and Handbooks, and all Student Policies, Guides and Handbooks.
- Such violations may be dealt with by the UON'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.

7. PROCEDURE

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 Users must ensure their UON device stays up to date by connecting to the UON network at least once per month, to enable security updates. Users should ensure that they shut down their device each day.

If Users have personal equipment and are unsure about the level of protection on their device, they should visit the IT Service Desk.

7.1. Reporting issues and breaches

- If Users suspect a security or data breach has occurred, they must immediately cease all use of IT Resources and inform IT Services via the IT Service Desk on 01604 893 333 (Ext. 3333), at the Learning Hub, or using the Service Desk Portal (https://uon.saasiteu.com/Modules/SelfService/#home).
- Breaches to the Information Security Policies should be discussed with managers and reported to IT Services via the IT Service Desk.
- In the event of loss or theft of a UON device or device containing UON data, the User must act promptly to minimise the risk of compromise by immediately notifying IT Services. Theft of the device should also be reported to the police.
- Managers should discuss and share Information Security Policies with Users at the earliest opportunity and offer support, help and appropriate training.
- Failure to report a loss will be dealt with under the appropriate disciplinary and GDPR Policies.

8. ASSOCIATED DOCUMENTS

Disciplinary Policy and Procedure
Code of Conduct Policy
Social Media Policy
Prevent Duty Guidelines

9. EQUALITY IMPACT ASSESSMENT

There is no adverse equality impact within this Policy. All responses to breaches of rights will be dealt with in accordance with this Policy and relevant Appendices irrespective of an individual's specific characteristics.

10. VERSION CONTROL

Version Control	3.0	**Approval record**	
Author:	IT Services	Approval:	TU Liaison – 18/09/2018 UMT – 10/10/2018 Board – 11/12/2018
Date written:		August 2018	
Current status:		Live	

Record of Amendments

Date	Version number	Details of Change	Approval
10/12/2018	1.0	The Acceptable Use Policy is a revision of the 2017 Policy. The new Policy is a complete rewrite of the old Policy and has been amended to reduce the number of pages for this individual Policy whilst enhancing the Policy to capture additional security elements including: • Safeguarding of information • Staff mobile phone acceptable use • Leavers or changing roles Procedures • Reporting issues • Repeat Offenders	Trade Union UMT Board
31/05/2019	2.0	Review of web filtering security measures to safeguard staff and	Trade Union JCNC – 19/9/19

		students from malicious malware, illegal, violent and hate activity websites.	UMT - Governors SEC -
10/05/2020	2.1	General Review	Trade Union JCNC – UMT - Governors SEC -
04/03/2024	3.0	Review of entire Policy plus inserting smaller Policies into AUP; Password Policy, Data Backup Policy, Smart Working & Security Policy, and Wireless & Bluetooth Policy.	ITSB – 24/01/2024