IT Acceptable Use Policy

1 INTRODUCTION

Whilst the University expects its employees and staff to comply with this policy, it does not confer contractual rights or form part of any contract of employment and 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.

This policy will be reviewed by the IT Service and HR departments on a 3-year basis or amended in response to changes in future legislation and/or case law.

2 OWNERSHIP

The IT Services and Human Resources departments owns and manages this policy on behalf of The University of Northampton.

3 ORGANISATIONAL SCOPE

This Acceptable Use policy is a corporate policy and applies to all employees (and workers, as applicable) and students of The University of Northampton including any wholly owned subsidiaries, unless an alternative policy exists, subject to any qualifying conditions.

4 POLICY STATEMENT

4.1 The University of Northampton (UoN) IT Services are provided to users primarily to support: learning, teaching, research, professional and administrative activities. The UoN seeks to ensure technologies and facilities that are made available to all students, staff, alumni and associates, meet legal and social responsibilities and are therefore used safely, lawfully and fairly.

This policy and procedure applies to all usage including at University premises, partnership sites and when working off premises.

Limited personal use of the facilities by staff and students is allowed. The use of IT Resources for personal use should be kept to a minimum is permitted during breaks, before and after working hours and should not obstruct, delay or in any way impede the completion of University related activities and is for legal usage only. This Acceptable Use Policy is taken to include the JANET Acceptable Use Policy and the JANET Security Policy published by JANET (UK).

It is the responsibility of all users of the University's IT facilities to read, understand and comply with this policy and any additional policies related to their activities, including other relevant information security policies.

5 DEFINITIONS

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

Users
All parties who have been granted access to the University's IT Resources.

IT Resource
All equipment that connects to the University network or accesses University applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

Systems Owners
A System Owner is an individual or group with the responsibility to ensure that the programs and applications which make up the system achieve the specified objective or goals established for that system. System Owners are responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system, including ensuring that appropriate security safeguards are in place.

Data
Data is defined as the representation of information factual or fictional, concepts, or instructions in a formalised manner suitable for communication, interpretation, or processing by humans or by automatic means. It may be stored either digitally or on paper and may take many forms, including, but not limited to, text, graphics, images, sound, and video.

General Data Protection Regulation
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.

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

Web filtering
A term for content-filtering software, especially when it is used to filter content delivered over the internet. Content filtering software determines what content will be available on a machine or network; the motive is often to protect children, or to prevent employees from viewing non-work-related sites.

Malware
Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

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

Sensitive information
There are three main types of sensitive information: personally identifiable (medical information or passport number), business (research or financial

information) and classified (confidential information). This information must be protected from unauthorised access to safeguard its privacy and security of the individual and organisation.

6 KEY PRINCIPLES

6.1 Acceptable Behaviour

When using University IT facilities, you must not:

- Attempt to authenticate yourself using another person's or organisation's credentials.
- Knowingly receive, access, create, change, store, download, upload, share, use or transmit: any illegal, obscene or indecent images, data or other material, or any data capable of being resolved into such material (other than while material is being properly supervised, is lawful or for authorised research);
- Share sensitive information outside the University, such as research and development information and customer lists.
- Cause needless offence to others including posting of inappropriate comments about students or members of staff (genuine scholarly criticism and debate is acceptable);
- Use IT Resources for criminal activities.
- Removal of University IT Resources from the organisation's premises without prior authorisation. If IT Resources are removed from the University's premises, all reasonable actions should be taken to safeguard the resource and protect from theft, loss or damage.
- Send spam (unsolicited bulk email), forge addresses, or use University mailing lists other than for legitimate purposes related to University or Trade Union activities;
- Deliberately or recklessly consume excessive IT resources such as processing power, bandwidth, storage or consumables;
- Knowingly undertake any activity which jeopardises the security, integrity, performance or reliability of electronic devices, computer equipment, software, data and other stored information. This includes undertaking any unauthorised penetration testing or vulnerability scanning or the monitoring or interception of network traffic, without permission;

- 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.
- Attempt to disrupt or circumvent IT security measures.
- In association with the UoN Code of Conduct policy, participation in activities deemed inappropriate for the University to be associated with and/or are detrimental to the University's reputation is not acceptable.
- Use of internet-based email services (e.g. Hotmail) for UoN business purposes should not be used, unless all reasonable attempts have been made to access and use UoN emails.
- Create or build applications for use within their department or business area. These are subject to review and approval by IT Services.

System administrators and other University personnel with Administrator Access to computing and information resources are entrusted to use such access in an appropriate manner.

6.2 Safeguarding of Information

- A user will be held responsible for any breach of regulations carried out using a connection authenticated with their username, this includes action taken by others. For example, if a password has been shared or entered into a phishing email.

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

- You must not knowingly infringe copyright or break the terms of licences for software or other material.

- All users are expected to;
  - Be mindful of, and safeguard the University's reputation.
  - Be aware of the permanent record and electronic footprint a user makes on the internet using social media.

- Comply with University Policies, particularly protecting sensitive or confidential information or material protected by copyright law or GPDR/Data Protection Act.
- Have appropriate authorisation and technical protection before sending or transmitting University confidential information external to the University network.
- Comply with all relevant copyright legislation, licences and agreements for software and electronic information resources when accessing and connecting to University IT Resources.
- Be aware of the appropriate procedures for handling any confidential University information to which you have access.
- Where possible .pdf (Portable Document Format – Adobe Reader compatible) format should be used, to protect the integrity of documents attached to emails.
- Not attempt to access, delete, modify or disclose information belonging to other people without their permission.
- Utilise good information security and management practices for the storage, access, retention and deletion of University Data.

6.3 Web Filtering

IT Services block site(s) or protocols on University networks and restrict access to undesirable content through the firewall. This is based on reputation and cyber risk to the University, including: computer viruses, malicious software (malware), spam e-mail, phishing, computer hacking and use of illegal file-sharing that are highly dynamic and volatile in nature.

IT Services shall periodically review and recommend changes to web and protocol filtering rules.

Maintaining freedom of access to the internet is acknowledged as being of business importance to the University. Processes will be implemented to allow requests for changes or exceptions to be made for a given site or category of material.

It is acknowledged that access to sites or material that the University has agreed be filtered may be necessary for some research or other academic teaching purposes. An exemption may be applied for via Head of Faculty or department. IT Services will review the risk and unblock that site or category for that associate only and where possible, will limit the timeframe of availability to minimise exposed risk. IT will track approved exceptions.

6.4 Mobile Phone Devices – only applicable to staff

6.4.1 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.

6.4.2 Mobile Phone Acceptable Behaviours

- Ensure the mobile phone device is regularly switched on and connected to the internet, to ensure the operating system remains up to date and scans antivirus protection.
- Mobile phone devices are provided for University business use, however it is recognised that there may be a need to make and receive occasional private communications.
- The use of personal applications should be limited to avoid unreasonable data usage.
- The purchase of applications for personal use are subject to the user's own expense and not to the University.
- Itemised bills will be issued monthly to departmental billing administrators for information purposes.
- Line managers will have responsibility for keeping control of mobile phone device usage by identifying those individuals who use a mobile device excessively and taking steps to reduce this.
- The sending of high volumes of SMS messages is subject to review by line managers.
- 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, 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 University issued device. It is the user's responsibility to contract 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.

6.5 Leavers or Changing Devices

- University issued mobile phone devices must be unique identified and linked to a user.
- The devices are University property and as such must be returned to IT Services 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 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.

6.6 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 computers are connected to it and what services they are operating. You may not configure your UON device to use any network address other than those allocated to you.

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

6.7 Implementation and Enforcement

Users must not seek to gain unauthorised access to restricted areas of the network.

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

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

There may be exceptional circumstances under which the University 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 university 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 University) and may be subject to the rules of 'privilege' . These circumstances include, but 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 University policy.
- Subject Access Requests or requests under GDPR 2018.
- Freedom of Information requests

Access privileges may be revoked or other sanctions imposed (in accordance to UON disciplinary procedure) by the Head of IT or the HR Director for violations of this policy and the supporting processes, as deemed appropriate.

Unauthorised use of University IT Resources, intentional corruption or misuse of resources will be regarded as direct violations of the University’s standards for conduct as outlined in the University’s Code of Conduct, its Policies, Procedures and Handbooks, and all Student Policies, Guides and Handbooks.

Such violations may be dealt with by the University'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 device stays up to date by connecting to UON network at least once per month, to enable security updates.

If a site or protocol is blocked and access is required, an IT Service help desk ticket should be raised to enable IT Security to review the risk and unblock

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

7.1 Reporting issues and breaches

If users do receive or suspect they have received malware they must immediately cease all use of IT Resources and inform IT Services via the IT Service Desk on x3333.

Breaches to the Information Security policies should be discussed with managers and reported to IT Services via the portal or Portal or the IT Service Desk.

In the event of loss or theft of a UoN device or device containing UoN information or data, the user must act promptly to minimise the risk of compromise to UoN information by immediately notifying IT Services. Theft of the device should also be reported to the police.

Managers should discuss the concerns Information Security policies with employees at the earliest opportunity with the intension to resolve issues informally, for by example, offering support, help and appropriate training to members of staff.

Failure to report a loss will be dealt with under the appropriate disciplinary and GDPR policies.

7.2 Repeat Offenders

Repeat offenders to Information Security policies will follow the HR Disciplinary procedure structure.

8 ASSOCIATED DOCUMENTS

- Disciplinary Policy and Procedure
- Code of Conduct
- Social Media Policy
- Password Protocol

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, Procedure and relevant Appendices irrespective of an individual's specific characteristics.

10 VERSION CONTROL

Version Control	2.1	**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	Details of Change	Approval
10/12/2018	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	Review of web filtering security measures to safeguard staff and students from malicious malware, illegal, violent and hate activity websites.	September 2019