Information Systems

Computer Use Regulations

Purpose of this Document

This document provides guidelines, which must be followed to ensure that use of University Computer Systems does not interfere with the activities of others and does not damage the reputation of the University.

Acceptance of this Document is required in order to obtain and use a University username, for accessing University Computer Systems, including but not limited to email, internet access and logons to computers.

This document will be reviewed every 12 months

Author:	Information Security Manager
Version:	2.3.1
Date:	30th November 2018

NOTTINGHAM TRENT UNIVERSITY

Review/Approval History for this Document:

Organisation	Action	Date
Information Systems	Overall Content Approval	30/11/2018
Legal Services	Legal Approval for publication	02/11/2015
Academic Office	Prevent Duty	29/10/2015

Document Control:

Version	Author	Date	Version details	Reviewer	Date
2.0	Matt Mason	26/05/11	2011 Issue	Tracy Landon	27/05/11
2.0	Matt Mason	11/07/11	Minor Clarifications	Bill Turner	12/07/11
2.0	Matt Mason	12/08/11	Minor Clarifications	Bill Turner	19/08/11
2.1	Matt Mason	10/09/12	Review. New content at: 1.4; 8.12, 10.0 Clarifications at: 2.1; Section 6; 7.4; 7.5; 8.15	Bill Turner	20/09/12
2.2	Dan Ladle	04/09/13	Review. New content at: 9.7	Matt Mason	04/09/13
2.3	Matt Mason	01/10/15	Review, and Addition of Prevent	Tracy Landon	02/11/15
2.3	Matt Mason	22/08/16	Review, no changes		
2.3	Matt Mason	01/09/17	Review, no changes		
2.3	Matt Mason	01/09/18	Review, no changes		
2.3	Matt Mason	29/11/18	Addition of incident reporting	Peter Nicholson	30/11/18

Contents

Computer Use Regulations

1. Introduction

1.1 This document describes acceptable use requirements, which must be followed to ensure that your use of the University's computer systems does not interfere with the activities of others and does not damage the reputation of the University.

1.2 Any breach of the Computer Use Regulations may be managed by the application of the Disciplinary Policy, which following investigation, could result in disciplinary action which may include dismissal or suspension of studies.

1.3 As a member of staff, an enrolled student or authorised visitor/contractor (applied for and been granted an account for a specific purpose), you are permitted to use the University's computer systems and services. This permission is conditional upon you exercising it in a responsible way. If you misuse University computer systems, you may be committing a criminal offence and/or contravening University regulations.

1.4 As a general principle, the University will always treat computer misuse as a breach of its own regulations, whether or not it is a matter for the criminal courts. However, the University's ability to act under its regulations may be constrained or influenced by the involvement of external parties. This is particularly likely where any misuse has impacted upon a computer, or a user, outside the University; or involved the viewing/transfer of inappropriate materials; or has triggered the involvement of law enforcement agencies.

1.5 The Student Union makes extensive use of the University IT infrastructure. Students should therefore note that misuse of Student Union computer facilities may also constitute misuse of the University's systems, which could result in action being taken (jointly or separately) by the Student Union and the University.

1.6 At all times, the University will exercise its Duty under the Prevent element of the Counter-Terrorism and Security Act (2015), and staff and students are expected to comply with the requirements.

1.7 Please be aware of other Policies that exist which are applicable to University Systems or Services, examples of such Policies include (but are not limited to):

Information Systems Security Manual
(*https://www.ntu.ac.uk/intranet/ecentral/policies/is/120772.pdf*)
Mobile Device Policy
(*http://www.ntu.ac.uk/information_systems/document_uploads/128983.pdf*)
Portable Devices and Media Policy
(*http://www.ntu.ac.uk/information_systems/document_uploads/128981.pdf*)
Bring Your Own Device Policy
(*http://www.ntu.ac.uk/information_systems/document_uploads/148296.pdf*)
Social Media Policy
(*https://www4.ntu.ac.uk/corporate-hr/document-uploads/170993.pdf*)

2. Authorised Users

2.1 As a member of staff, an enrolled student, or authorised visitor/contractor, you are authorised to use the University's computer facilities or services, in pursuance of your employment, or studies, at the University. It is a condition of your employment, or enrolment as a student, that you agree to abide by the University's regulations, including but not limited to, the Computer Use Regulations. Other persons engaged by the University (associates or affiliates) to whom IT access is granted are also required to comply with these regulations.

2.2 Unauthorised use of the University's facilities and services is a breach of University regulations and may also be deemed as a criminal offence.

2.3 As an authorised user, you must familiarise yourself with and abide by other relevant external rules and regulations applicable to users of the University's computer facilities and services. These include, but may not be limited to:

2.3.1 the JISC (JANET) Acceptable Use Policy;
https://community.jisc.ac.uk/library/acceptable-use-policy

2.3.2 the counter-Terrorism and Security Act;
https://www.gov.uk/government/collections/counter-terrorism-and-security-bill

2.4 As an authorised user, you are required to inform Information Systems of any Security Incident that you have become victim to or that you have witnessed such that the Incident can be managed, and risks minimised to the University.

Security Incidents can come in many forms, some examples are given below. The reporting method is the same regardless of Incident. To report an incident please contact the Service Desk by email support@ntu.ac.uk or by phone 01158488500 giving details of the Incident and also any supporting information.

Example of Incidents to report:

General:

- Any observed or suspected physical or IT related security weaknesses;
- Any suspicion or evidence of internal fraud (financial, suspected spoofed email);
- Non-compliance with NTU IT and other University Policies or Guidelines.

Information Security:

- Inappropriate or inadvertent release of restricted or sensitive information, whether electronic or hard copy, into the public domain;
- Theft or loss of any personal information relating to staff, students or any other third-party member(s) of the public generally;
- System malfunctions;
- Any evidence or suspicion of hacking or attempted hacking or cyber security incident to facilitate system interruption, ransom or data and identity theft;
- Sharing / disclosure of user accounts and or account passwords.

3. Computer Misuse

Access to Other Computers and Systems

3.1 You must not access, or attempt to access, a computer system that you are not authorised to do so. The ability to connect to another computer system or service does not automatically give you permission to use it.

3.2 If you do not see or receive an explicit message giving you permission you must not attempt to access or use a system, without seeking authorisation from the system owner.

Access to Computers Related to Other Offences

3.3 You must not access any computer systems as preparation towards committing a criminal act. Where such access is identified by the University the matter would normally be passed to the police for action and the University may impose further penalties, such as removal of access to University computer systems.

Altering Other Users' Material

3.4 You must not alter data, programs, files, e-mail or any other computer material belonging to another user, without that user's express permission. This also applies to system data and programs, and includes the deliberate introduction of computer viruses and other malware.

Using Another's Programs or Information

3.5 You may access information or any program which you yourself have written, or which is freely available on the computer systems you are authorised to use. You must not access, or copy, information or programs belonging to another user, without that user's permission.

3.6 You must not use another user's username and password, even if s/he offers to make them available to you. A user who gives details of his/her password to another user is guilty of an offence, under the University's regulations. If the person receiving those details attempts to use them to access University systems, he/she would be deemed to be guilty of breaching University regulations.

Storage

3.7 You must not use University computer equipment to store copies of personal files, which are not related to your employment, studies or work on behalf of the University. Such personal files may have copyright implications for the University.

3.8 Where University computer equipment is found to hold personal files such files may be removed, without warning.

3.9 The University does provide access to online storage offered by OneDrive in which to store your personal files.

3.10 Please note, that any files stored on University provided storage must be in accordance with the University's Data Protection Policy.

4. Copyright

General

4.1 When using the University's computer systems you must not infringe copyright laws. The creator of original work has automatic copyright in that work. Copyrighted works include, but are not limited to, text and drawings (whether on paper or electronic media), animations, images, graphs, software, 3 dimensional works, designs, sculptures, etc. Downloading or transmitting information, without the consent of the copyright owner, from or via the internet, risks infringing copyright. You must not use, make, transmit or store an electronic or other copy of copyright material without consent from the owner. Some materials published on the internet have their own license requirements which must also be adhered to.

Fair Dealing

4.2 Under certain circumstances you may use copyright material, provided that there is sufficient acknowledgement of the source ("Fair Dealing"). This includes the following uses – research; private study; reporting current events; and criticism or review. If you wish to use copyright material for teaching purposes you should first obtain advice from Libraries and Learning Resources or check the terms of any relevant licences the University may have.

4.3 Fair Dealing only permits a single copy to be made. Where there are to be multiple copies permission will be required from the copyright owner, or from a copyright licensing body.

Further information relating to copyright is available from Libraries and Learning Resources:
http://ntu.ac.uk/library/developing_skills/copyright/index.html

Or the United Kingdom Intellectual Property Office (UKIPO):
http://www.ipo.gov.uk/home.htm

5. Data Protection

5.1 The Data Protection Act 1998 provides a set of rules, known as "Data Protection Principles (DPP)", which apply to the recording, storage, and processing of all computerised (and some manual) information that relates to identifiable individuals ("personal data"). Failure to observe the DPP may result in both criminal charges and civil actions for compensation.

5.2 As a general principle the legislation prohibits the processing of personal data about an individual without receiving that individual's ("data subjects'") consent.

Sensitive Personal Data

5.3 Data relating to racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, physical and mental health or sex life, commission of an offence or criminal court proceedings is known as "sensitive personal data".

5.4 Except in very limited and specified circumstances processing of such data requires the individual's ("data subjects'") explicit consent.

5.5 If you are using the University's computer systems to process such data (including personal and sensitive personal data), you must ensure that you have obtained the consent (explicit consent, in the case of sensitive personal data) of the data subject, prior to the processing and use of this data.

5.6 If you are using the University's computer systems to process personal data, this must be stored on Corporate Systems, or on University File Servers; personal data must not be stored on the local hard disk of computer equipment or on your desktop. Should the data be required to be processed elsewhere, it must be transferred in an encrypted format. Please contact the ITS Service Desk should you need advice on encrypting data.

5.7 If you are involved in the transfer of Data which is considered personal data, the data must be encrypted to at least 256bit AES standard prior to transfer and that the passphrase is not transmitted via the same method of transfer. If you need any assistance in the preparation of data for transfer or the transfer itself, please contact the Service Desk for advice.

5.8 Data which is considered personal data, must not be transferred to external 3rd parties without a suitable Data Sharing Agreement or similar in place prior to the transfer taking place, please contact Legal Services for advice.

6. Inappropriate Materials

6.1 The University's equipment and systems must not (except as described at 6.6 below) be used to view, access, transmit or download materials which are (or may be reasonably considered to be) obscene, indecent, sexist, racist, homophobic, xenophobic, pornographic, unlawfully discriminatory, extremist, violent or offensive.

6.2 Obscene materials include the depiction of sexual acts, in pictures or text, as well as pamphlets advocating the use of drugs, and material showing scenes of violence.

6.3 Indecent materials include indecent photographs or pseudo-photographs of children. The term "photograph" includes 'data stored on a computer disc or by other electronic means which is capable of conversion into a photograph' and covers digital representations of physical photographs, thus gif, jpeg and png image files, downloaded from FTP sites, embedded in Web Pages, or compiled from USENET messages, will be treated as photographs. A pseudo-photograph means any data which is capable of being resolved into an image which appears to be a photograph. If the image appears to show a child, then the image is to be treated as if that of a child.

6.4 Given the University's duty under the Counter-Terrorism and Security Act (2015), steps will be taken to prevent people being drawn into terrorism. To meet this duty, the University's systems must not be used to create, access, transmit or download inappropriate materials as defined in this document and under the Prevent legislation. The University reserves the right to monitor, alert and report attempted access to, or dissemination of, such inappropriate material.

6.5 The definition of extremist material will be governed by Home Office definitions within the Prevent Guidance (2015).

6.6 You may request permission to access material of the kind described in sections 6.1 to 6.4 above, where that use is deemed by the University to be necessary for your legitimate academic or research purposes. Such use must be authorised, in advance, by your Head of College or Head of Professional Service (as appropriate). In requesting authorisation, you must provide a sufficiently detailed explanation of the material you wish to access/use and the purposes for which the material is required. Authorisation is at the discretion of the relevant Head of College or Head of Professional Service. To ensure that the University's monitoring systems do not inhibit authorised access to such materials Information Systems must be provided (via the ITS Service Desk) with evidence that authorisation has been granted, in advance of any attempt by you to access the material in question.

6.7 Access to material on the Internet Watch Foundation list will require a license from the Home Office prior to attempting to view such materials, a copy of the license is required to be held by Information Systems.

6.8 If you discover inappropriate material on a University computer or system you MUST inform the ITS Service Desk immediately, on 0115 848 8500, and leave the material in its original state in order that an investigation into its origin can be conducted.

6.9 The University reserves the right to prevent access to materials it feels are inappropriate and also where the University is required to by Law, Policy or Statutory Duty.

7. Software Use

7.1 The making, use, and possession, of any copy of computer software without a licence from the owner of the software is illegal, and may expose both you and the University to criminal and civil proceedings.

7.2 It is therefore of the utmost importance that you comply with the following requirements:

7.2.1. You may not make, or use, any more copies of any computer software than the relevant licence permits; and

7.2.2 Except where otherwise allowed by legislation, you must comply with the terms and conditions held in that licence.

7.3 Computer software may only be installed on University systems, or stored on University premises, where:

7.3.1 The software is approved by Information Systems for use on the University Computer Network; and

7.3.2 The software is for legitimate University business or academic use; and

7.3.3 A valid licence for the software is held. Unlicensed copies of computer software must not be brought onto University premises; installed on any University computer; uploaded to or downloaded from University systems; or passed across University networks.

7.4 Staff must not install or use unlicensed copies of computer software, and must report the existence of such to Information Systems.

7.5 You must not install software on a University computer, or system, without gaining the prior approval of Information Systems (via the ITS Service Desk).

7.6 Information Systems has the right to remove from University equipment, or systems, any software which was installed without prior approval from Information Systems.

7.7 Where Admin rights have been granted to a computer, and software installed by the user, a detailed copy of the license MUST be produced if requested and should any software be found where a license cannot be validated the software must be removed. Where software has been installed knowingly breaching the license, the software will be removed and Admin Rights revoked.

8. Electronic Communications

Introduction

8.1 Electronic Communications are an important means for the University to conduct much of its business, it is anticipated that its use will continue to increase. This section sets out the University's Regulations on the proper and acceptable use of all forms of Electronic Communication, including teaching, instruction, research, public service, and administration. For the purposes of this section Electronic Communications will (despite some functional differences) be taken to include (but is not limited to) email, IRC, USENET, Messenger Services, Social Networking, Chat, Wiki, Blogs, Lync and using the University's printers/copiers and telephones.

Overview

8.2 To prevent loss of data the systems involved in the transmission and storage of electronic communications at the University are "backed up" on a routine basis.

8.3 It is usual practice for individual user accounts to be password protected. While this security measure is beyond the usual measures taken to protect access to paper records and telephones, it does not confer a special status on electronic communications with respect to the applicability of laws, policies, and practices.

8.4 Access to electronic communications is a privilege and certain responsibilities accompany that privilege. Users are required to be ethical and responsible in their use.

Appropriate Use of University Electronic Communication Resources

8.5 Access to electronic communications is governed by two principles:

8.5.1 Compliance with appropriate use of University resources and policies.

8.5.2 Provision of services only to University staff, students or authorised affiliates.

8.6 The University's staff, students, and authorised visitors/contractors may be provided with, at the discretion of the University, access to University electronic communications facilities for the performance of University activities.

8.7 Individuals who do not have authorised affiliation with the University, or those with authorised affiliation but whose use of the University's computer or systems is for a non-University purpose, must not access the University's electronic communication services.

8.8 Users must read the privacy policies on third party websites before disclosing their University email address, and should consider whether it is appropriate to do so. If unsolicited emails are received to a University email address on a regular basis the User should take appropriate steps to be removed from these lists.

8.9 Electronic communications are subject to the same laws, policies, and practices that apply to the use of other means of communications, such as telephones and written records/correspondence. Users must, therefore, ensure that their use of University electronic communication facilities is consistent with appropriate use of the University's resources and facilities.

8.10 Users may not use University electronic communications facilities to transmit:

8.10.1 Commercial material unrelated to the legitimate educational business of the University, including the transmission of adverts (spamming);

8.10.2 Bulk non-commercial email unrelated to the legitimate educational activities of the University that is likely to cause offence or inconvenience to those receiving it. This includes the use of e-mail exploders (e.g. list servers) at the University, or elsewhere, where the email sent is unrelated to the stated purpose for which the relevant email exploder is to be used (spamming);

8.10.3 Unsolicited email messages requesting other users, at the University or elsewhere, to continue forwarding the message to others, where those e-mail messages have no legitimate educational or informational purpose (chain e-mails);

8.10.4 Emails which purport to come from an individual other than the user actually sending the message, or with forged addresses (spoofing);

8.10.5 Emails which purport to come from an individual, or organisation, asking users to reply with personal information, which could be used for criminal activities or to impersonate others (phishing);

8.10.6 Material which could be considered sexist, racist, homophobic, xenophobic, pornographic or similarly discriminatory or offensive;

8.10.7 Material that advocates or condones, directly or indirectly, criminal activity, or which may otherwise damage the University's research, teaching, and commercial activities, in the UK or abroad;

8.10.8 Text or images to which a third party holds intellectual property rights, without the express permission of the owner;

8.10.9 Material that is defamatory;

8.10.10 Material that could be used to breach computer security, or to facilitate unauthorised entry into computer systems, either on campus or elsewhere (which can also be a criminal offence);

8.10.11 Material that is likely to prejudice or seriously impede the course of justice in criminal or civil proceedings;

8.10.12 Material containing personal data (as defined by the Data Protection Act 1998) about any individual, unless their explicit consent has been provided, or communication of the information required by law or is covered by a relevant exemption within the Act;

8.10.13 Emails which offer the sale of goods or services by users to others within and beyond the University.

8.11 The University provides electronic communication systems for the conduct of University business. Incidental and occasional personal use of these systems is permitted, provided that such use complies with section 8, does not disrupt or distract the conduct of University business (due to volume, frequency or cost) and that such communications do not bring the University into disrepute for clarification please check with your line manager.

8.12 The University has a specific policy on the use of Social Media by staff (available via the NTU staff intranet). In addition, the terms and conditions by which students are permitted to use University systems for Social Media purposes are documented in Section 10 of this document.

Disclosure, Privacy and Technical Controls

8.13 Users may not, under any circumstances, monitor, intercept or browse other users' electronic communications.

8.14 The University has the right to access and disclose the contents of User's electronic communications, as required by University legal and audit obligations.

Portable Devices and Email

8.15 Users who access and check their University e-mail via a portable device, such as a laptop computer, mobile phone, iPod®/iPad®[1], PDA or other portable device, MUST have, and use a Device PIN or passphrase for that device. Failure to comply with this requirement poses a risk to the security of University data and systems. This may result in disciplinary action and barring of the user's access from such devices.

8.16 The University has a specific policy on the use of portable computing devices, storage media and Bring Your Own, which should be read in conjunction with the Computer Use Regulations. Please see the information available on the Information Systems intranet site for further details and policy announcements.

Remote Access to University Data

8.17 The use of any personal computers, or other capable devices, to access University Systems from remote locations (for example home, internet cafés or hotels) must be protected by a username and password, as per internal University computers.

8.18 Where access is required to University systems in order to view, modify or transmit Personal Data, all access MUST utilise NTUanywhere, in order that all access is secured and logged. Should unsecure remote access be discovered, it will be terminated.

[1] Registered Trademarks of Apple Inc.

9.0 Computer Systems Monitoring

9.1 The University has the right, at any time, to inspect all data held on University computer equipment, and to inspect all email and other electronic data entering, leaving, or within the University network to ensure it conforms with:

9.1.1 University regulations

9.1.2 Contractual agreements with third parties

9.1.3 The law

9.2 The University is obliged, by law, to report to the police the discovery of certain types of electronic data (e.g. indecent images), if that data is found on University equipment or transmitted across University networks.

9.3 Routine computer service tasks may involve members of Information Systems or Libraries and Learning Resources having access to data held about staff and students of the University. The University will not routinely access, monitor or scrutinise data held on University computers, or systems, unless formally authorised to do so by the Director of Information Systems or his deputies. Such authorisation shall only be granted on a case-by-case basis, which would include permission to investigate suspected material breaches of University regulations or other matters that might expose the University to action under criminal or civil law. Where data is discovered that indicates a breach of these regulations has occurred, this information may be passed onto HR or Student Services for further investigation.

9.4 All network traffic is monitored for the purposes of bandwidth management; prevention of misuse; and in order to satisfy the University connection agreement to the JISC Network. This monitoring includes all websites visited, and records the username of users accessing those websites.

9.5 Only Information Systems staff, authorised by the Director of Information Systems or his deputies, are permitted to conduct monitoring.

9.6 Users must not set up, or implement, network servers/services on University systems, without the explicit permission of Information Systems. Any such servers or systems, set up without the University's authority, may be disconnected from the University's network by Information Systems without notice and will be subject to an investigation regarding their use and purpose.

9.7 As stated in the Bring Your Own Device Policy, 'in exceptional circumstances the University will require access to University data and information stored on your personal device'.

9.8 Where following an investigation, data required to be passed to HR or Academic Departments, the data can only be released with the permission of the Director of Information Systems or his deputies.

9.9 The University uses aggregated location data (both GPS and where you are physically on campus) collected from connected devices on campus and whilst using University Apps. By using the University Wifi and Apps you are consenting to us collecting this data. This data is only used to improve the services provided by the University.

10.0 **Use of Social Media**

Use of Social Media for Students

10.1 The University recognises that students may wish to use social media for personal use by means of the University's computers, networks and other IT resources and communication systems. Such use must comply with the University's Computer Use Regulations; it should not be intrusive or disruptive to the conduct of University business and such communications should not bring the University into disrepute.

10.2 Students are personally responsible for their words and actions in an online environment and should remember that, as social networking platforms are in the public domain, participants cannot be sure what is being viewed, shared or archived.

10.3 Students must not engage in any conduct online that would not be acceptable in a lecture, live discussion or other face-to-face situation, such as making derogatory remarks, bullying, intimidating or harassing other users, using insults or posting content that is hateful, slanderous, threatening, discriminatory or pornographic.

10.4 Students must not associate the University with personal views or comments that they post on social media. The University may require students to remove internet postings which associate the University with the message. Failure to comply with such a request may result in disciplinary action.

10.5 Students should be aware that posting potentially controversial views and comments on social media sites can often attract strong and widespread criticism – mention of NTU in such postings (even the fact that the contributor is a student at NTU) can bring complaints to the University, which may result in disciplinary action against those involved.

Use of Social Media Use for Staff

10.6 There is a Social Media Policy available on eCentral
https://www4.ntu.ac.uk/corporate-hr/document-uploads/170993.pdf