Policy: **ISP-S9**
Title: **Use of Computers Policy**
Status: **Revised**

1. Introduction

1.1. This information security policy document contains high-level description of the responsibilities and required behaviour of users of University IT systems, including University networks. It is a sub-document of Information Security Policy (ISP-S1).

1.2. This document includes statements on:

- Departmental policies and procedures
- Connecting devices to University networks
- Use of University IT facilities for private work
- Unacceptable use of University IT facilities
- Accounts
- Passwords
- Unattended user equipment
- Protecting against unknown or malicious code
- Use of email facilities
- Backups

2. Departmental policies and procedures

2.1. Where necessary Heads of Department may specify and implement policies relating to use of IT systems for which they have responsibility, provided that any such policies are consistent with University wide policy and do not have a negative impact elsewhere. Such policies may, for example, include specific rules relating to use of software, managing provision of network services, user behaviour etc.

3. Connecting devices to University networks

3.1. IT Services is responsible for managing, either directly or through an agent, connections to University networks that have connectivity with the Internet. (IT Services may delegate responsibility for authorising connection to its networks to trusted staff in other departments.)

3.2. Minimum required hardware, software and configuration standards for securing devices attached to University networks are determined by IT Services and set out in policy. (IT Services may also publish other more specific requirements.)

REQUIRED HARDWARE, SOFTWARE AND CONFIGURATION STANDARDS

For details refer to: "Hardware and software requirements" in

- **Network Management Policy (ISP-S12)**

3.3. Devices must not be connected to a network, managed or provided by the University, unless the device meets current required hardware, software and configuration standards (see above) and its connection is authorised.

3.4. Any device connected to a network, managed or provided by the University, and deemed not to meet currently required hardware, software and configuration standards (see above) or connected without authorisation is liable to physical or logical disconnection from the network without notice.

3.5. It is the responsibility of the department operating any devices that have fallen below required standards (see above) to take prompt remedial action.

4. Use of University IT facilities for private work

4.1. University IT facilities are provided principally for official academic and administrative purposes. Occasional personal use is, however, permitted so long as:

- It is not in breach of any University policies.
- It is not excessive, in volume, frequency or time.
- It does not disrupt or restrict usage by other users.

4.2. Staff wishing to embark on any significant use of University IT facilities for work which is not part of their official University duties, such as consultancy or private work, must only do so after notifying their Head of Department and in accordance with guidelines issued by Personnel Services.

5. Unacceptable use of University IT facilities

5.1. Cases of unacceptable use of IT facilities may be investigated by authorised staff. The findings will be reported as appropriate to the relevant Head of Department or the Registrar. **(In cases of policy violation deemed to be serious, wilful or repeated the University will not hesitate to take disciplinary action.)**

5.2. The list of unacceptable uses of IT facilities below is applicable to all University IT systems. It is consistent with JANET acceptable use policy and legal compliance requirements. See also Compliance Policy (ISP-S3).

5.3. It is unacceptable to use University IT facilities for any of the following:

- Any illegal activity.
- Creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
- Creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.
- Creation or transmission of material with the intent to defraud.
- Creation or transmission of defamatory material.
- Creation or transmission of material such that this infringes the copyright of another person.
- Creation or transmission of unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their User Organisation has chosen to subscribe.

- Deliberate unauthorised access to networked facilities or services.
- Using communal or “open access” computing facilities for recreational or other non-University work when there are others waiting to use the resource (this may include simultaneously using more than one end user device).
- Deliberate activities having, with reasonable likelihood, any of the following characteristics:
    i. Wasting staff effort or networked resources, including time on end systems and the effort of staff involved in the support of those systems.
    ii. Corrupting or destroying other users' data.
    iii. Violating the privacy of other users.
    iv. Disrupting the work of other users.
    v. Denying service to other users (for example, by deliberate or reckless overloading of access links or of switching equipment).
    vi. Continuing to use an item of networking software or hardware after IT Services has formally requested that use cease or be suspended.
    vii. Misuse of networked resources, such as the introduction of "viruses" or other harmful software.

5.4. Where a network managed or provided by the University is being used to access another network, any breach of the acceptable use policy of that network will be regarded as unacceptable use.

5.5. Without prior explicit approval, the University's computing services must not be used for placing or distributing advertisements other than those promoting the activities or trading operations of the University or the Student’s Union. Where a proposed promotion may feature direct marketing, on behalf of a third party organisation, Information Assurance Services should be consulted. *(All advertisements should be 'legal, decent, honest and truthful' and comply with the British Code of Advertising, Sales Promotion and Direct Marketing issued by the Advertising Standards Authority.)*

5.6. University members must not permit information security safeguards and policies to be bypassed, or allow inappropriate levels of access to University information or IT facilities to other members or any third parties such as guests, customers, collaborators, suppliers, consultants or contractors. See also:

- Outsourcing and Third Party Access Policy (ISP-S4)

6. Accounts

6.1. Where a computer account is provided for exclusive use by an individual:

- The account holder should be instructed not to reveal the password or otherwise permit anyone else to use the account.
- The account must not be used by anyone except the account holder.

6.2. Where use of a shared account is necessary to facilitate a specific activity:

- The purpose of the shared account must be clearly understood and the account must be used only for the purpose specified.

- Usage of, and access to, the shared account must be carefully managed. Every shared account must have an “owner” responsible for managing access to the account and supervising its use.
- The owner of a shared account must maintain a current record of which individuals have access.
- When an individual having access to a shared account leaves, or no longer requires access to the account, then the account owner must change the password and securely inform those continuing to require access.

6.3. “Privileged accounts” are those granting special computer system privileges that ordinary users do not need to use. (In addition to special accounts such as e.g. “root” under UNIX or “administrator” under Windows, privileged accounts can be ordinary user accounts that have extra permissions resulting from being added to user groups such as “power users” or “administrators”.)

- These accounts should only be used to undertake specific system administration tasks and should not be used for routine work, where a normal account has sufficient privileges.
- Wherever possible local system administration tasks on departmental user devices should be undertaken by professional departmental or central computing staff in accordance with University and departmental policies. In particular use of privileged accounts should be controlled and periodically reviewed to implement the principle of least privilege.
- Where a privileged account potentially permits access to information belonging to others, effective line management control over who has access to it and the way it is used must be maintained. (This applies to any system that holds or provides access to data belonging to more than one user.)
- Where a computer user also acts as the local system administrator, and so uses a privileged account on their local system, they are required to manage and use the system in accordance with all University and departmental policies.

6.4. Wherever possible both centrally and departmentally provided computing accounts should be managed such that :

- Preferably, computing activities undertaken using a particular account can be associated with a specific individual.
- Alternatively, an identified individual takes active responsibility for the management and activities of users of a particular computing facility or account.

6.5. Students are not permitted to log into more than one University provided computer simultaneously unless special arrangements have been made. (This may otherwise be considered unfair use of resources by an individual or an indication that an account is being shared in breach of University policy.)

7. Passwords

7.1. University IT system managers must wherever technically possible enforce appropriate password related policies. Specific recommendations about configuring password strength, account lockout, password expiry and other password access control parameters on University computer accounts are given in policy implementation document:

- Computer Account Passwords (ISP-I9)

7.2. Using mechanisms that allow automatic login into a computer account (including email accounts) without being challenged to provide a password each time can put security of that account at risk. It is strongly recommended that mechanisms that fill in passwords automatically are not used. However where they are used, it is strongly recommended that there is an additional layer of access control. For example, using a pin number to help protect access to a Smartphone, especially if it is configured for automatic connection to an email account.

7.3. Users of University IT systems must take all reasonable precautions to ensure that their passwords (or other security "secrets") are not disclosed.

7.4. University IT users should be advised about scams intended to make them reveal passwords and how to avoid being caught out.

7.5. Where a computer account user suspects that security of their personal computer account may have been compromised they must:

- Immediately change the password (if possible).
- Immediately report the incident - see Reporting Information Security Incidents (ISP-I3).

8. Unattended user equipment

8.1. Computers and other equipment such as smartphones, used to log into University IT accounts, must never be left unattended if they are logged in and unlocked. (Users of such equipment should be advised to log them out or lock them before leaving them unattended.)

1.1. Except in very special circumstances such equipment must be capable of automatically locking after a timeout period when left unattended. This automatic locking must be enabled and be effective in ensuring that unauthorised access to accounts that are already logged in, or which can be logged into using stored credentials, is prevented. The timeout period should normally be no longer than 20 minutes.

1.2. Computers in the process of being logged out, or shut down, should not be left unattended until it is certain that they have definitely logged out. (This is in case the log out process fails and a logged in account is left unattended).

9. Protecting against unknown or malicious code

9.1. Accidental or deliberate running or installation of malicious code (malware) on computers presents a significant information security risk. The need to restore integrity of systems infected with such code also has an impact on their availability for use and consumes computer support staff effort.

9.2. An appropriate combination of proactive measures should be used to help manage the risk of malicious code being run on University systems. The measures should be promoted and supported by management and implemented by computers system administrators and users. Some combination of the following measures is recommended:

- Deploying antivirus software developed by a reputable supplier, which should be kept fully up to date and used to scan all files: downloaded from the internet, received as attachments to email (or other forms of messaging) and all removable media when inserted. (Applicability of this varies between operating systems).

- Advising computer users to avoid running software or opening files obtained from untrusted sources and to be particularly cautious of accessing files attached to unsolicited email and stored on untrusted media. (This should be issued in conjunction with the advice about when it is appropriate to use privileged accounts.)
- Managing support of computers such that privilege to install software is restricted to staff, typically experienced computer support staff, who would be more aware of the problems that can result from installing code from untrustworthy sources.
- Implement departmental or Network Organisation level policy requiring staff to obtain approval from the Network Authority before installing items of non-standard software on University computer equipment. (The approval procedure should include a basic assessment of whether use of the software is justified and assurance that any software licensing requirements are met.)

9.3. See also:

- Software Management Policy (ISP-S13)

10. Use of email facilities

10.1. University email services are provided for official academic and administrative purposes, occasional personal use is permitted so long as such use is not excessive, in volume, frequency or time and does not disrupt or restrict usage by other legitimate users.

10.2. Staff must not configure their University email accounts to automatically forward incoming email to services that are not operated by the University, unless such an arrangement has been formally approved by the Director of IT Services and is subject to an appropriate bilateral contract. Also refer to:

- Outsourcing and Third Party Access Policy (ISP-S4)

10.3. Users of University email services should be advised that whilst privacy of their email messages is respected there are circumstances in which the content of their messages may be disclosed. This may be in response to a Data Subject Access Request made under the Data Protection Act. In addition there is provision for officers of the University to access the contents of University email. Also refer to:

- Institutional IT Usage Monitoring and Access (ISP-I6)

10.4. The University encourages the use of Out of Office functionality on email systems to inform colleagues and trusted third parties of your absence from the Office. For your personal security, telling unknown or un-trusted 3rd parties about your whereabouts is best avoided. It is strongly recommended that wherever possible you restrict sending Out of Office Replies to "people inside your organisation" and only to "Contacts" outside of your organisation. Detailed advice on how to do this is available on the IT Services website.

10.5. University email systems may not be used for any of the following:

- Unapproved transmission of commercial material (see also section 5 above).
- Spamming, i.e. sending unsolicited and unauthorised messages to a large number of people; this includes misuse of mailing lists. (Mass emailing to members of the University may be undertaken for purposes approved by the Registrar.)

- Messages requesting recipient to re-forward thereby setting up a chain action (chain mail).
- Messages likely to cause offence.
- Messages purporting to come from someone other than the actual sender (spoofing).
- Material advocating criminal activity or which may bring the University into disrepute.
- Material which violates copyright restrictions.
- Material which is defamatory or libellous.
- Material which could be used to breach computer security or facilitate unauthorised access.
- Material likely to prejudice the course of justice.
- Personal data about a third party in contravention of the Data Protection Act.

10.6. Other policy documents referring to use of email include:

- Information Handling Policy (ISP-S7)
- Mobile Computing Policy (ISP-S14)
- Cryptography Policy (ISP-S16)
- Guide to Information Legislation (ISP-I5)

11. Backups

11.1. University business must not be exposed to undue and unnecessary risk as a result of inadequate computer data backup arrangements. The information owner or custodian is responsible for checking, or seeking assurance, that the backup arrangements for the computer facility or service being used are suitable.

11.2. Computer system managers are responsible for ensuring that backup arrangements published, or agreed with users of the system, are reliably implemented and that users are informed promptly should there be any problems with, or changes to, the backup arrangements.

11.3. For further details also refer to the Backups section in:

- Information Handling Policy (ISP-S7).

Failure to comply with University Policy may lead to disciplinary action.

Document history:

27	August	2008	(C. Nelson)	Began first draft.
24	September	2009	(C. nelson)	Revised policy relating to shared accounts.
09	October	2009	(C. Nelson)	Added a statement about email out-of-office replies.

01	March	2010	(C. Nelson)	Minor revisions to sections 5 and 10.
18	May	2011	(C. Nelson)	Revisions resulting from review within IT Services.

The official version of this document will be maintained on-line. Before referring to any printed copies please ensure that they are up-to-date.