USE OF UNIVERSITY COMPUTERS AND DATA NETWORKS

University Policy

It is the policy of the University to encourage the proper use of its computing and networking facilities in support of its teaching, learning, scholarship and research activities. In pursuance of this policy the University will promote good practice guidelines and implement and publicise procedures for enabling it to comply with the provisions of the relevant legal acts and with the conditions of the JANET Acceptable Use Policy. (JANET is the UK's Joint Academic Network, to which the University's network is connected.)

Rules

The following rules apply to any person using any kind of computer hardware or software, for any purpose, at the University, including the use of personal equipment on University premises and remote use of the University's network.

1. Users

1.1 All users of the University's IT facilities must be registered with IT Services. All users will be registered staff or student members of the University. Use of the facilities by non-members of the University may be arranged in certain cases and may be subject to charge.

1.2 Registration to use IT facilities or the use of IT facilities constitutes acceptance of these Rules and Regulations.

1.3 Users are responsible for all use of the computer logon account allocated to them, defined by an identifier (username or logon name) and password. They must not use another user's identifier or password nor allow any identifier or password issued to them to become known to any other person.

1.4 The University's IT facilities are for bona fide University activities. Permission must be sought via the Head of IT to use the facilities for commercial or outside work and such use may be subject to charge. Use of the facilities for personal work or recreation will only be permitted within reasonable levels and must not jeopardise or interfere with the system so as to reduce the level of service for University business.

2. Law

2.1 It is the user's responsibility to comply with all statutory and other provisions and regulations currently in force in the field of data protection and information policy.

2.2 Laws applicable to the use of the University's IT facilities include:

a) Data Protection Act 1998
b) Copyright, Designs and Patents Act 1988
c) Computer Misuse Act 1990
d) Criminal Justice and Public Order Act 1994.

Users must comply with the provisions of the above acts and particular attention is drawn to the following:

Under the Computer Misuse Act, hacking and the introduction of viruses are criminal offences. The Act identifies three specific offences:

- Unauthorised access to computer material (i.e. a program or data)
- Unauthorised access to a computer system with intent to commit or facilitate the commission of a serious crime
- Unauthorised modification of computer material.

All three offences are punishable by fine or imprisonment or both.

2.3 The University's rules for the use of IT facilities apply subject to and in addition to the law. In all cases involving a breach of the law legal sanctions may apply.

3. Use of Software and Data Networks

3.1 Users must adhere to the conditions laid down by the JANET Acceptable Use Policy. Copies of the Policy are available from the IT Services helpdesk and are displayed in student computer rooms and on the University Web site.

3.2 Users must not access, or try to access, any computer material or system for which access

authorisation has not been given.

3.3 The creation, display, production or circulation (other than for properly supervised and lawful research purposes) of offensive, obscene or indecent material in any form or medium is forbidden.

3.4 Users must adhere to the terms and conditions of all licence agreements relating to software and data networks.

3.5 Users are required to respect the copyright of all materials and software made available by the University's IT facilities. The unauthorised copying or modification of software is an offence under the Copyright, Designs and Patents Act 1988.

3.6 Users must not load onto the IT facilities any software without permission from IT Services. IT Services shall maintain a register of authorised software installed on University computers and shall have the right to remove without notice any software not so registered.

3.7 Users must not deliberately introduce, or risk introducing, any virus or other harmful or nuisance program or file into any IT facility, nor take deliberate action to circumvent any anti-virus precautions established by IT Services.

3.8 Users must not construct or maintain computer files containing data about living individuals without complying with the principles of the Data Protection Act. Advice on the requirements of the Act can be obtained from the Data Protection Officer.

3.9 Users must not use the system or networks in a way that denies service to other users (for example, deliberate or reckless overloading).

3.10 Users' data and software will be subject to published procedures for their removal and archiving after specified periods.

3.11 Users of networks and remote IT facilities shall obey any published rules for their use.

3.12 Users must not in any way cause any form of damage to the University's IT facilities, nor to any of the accommodation or services associated with them.

3.13 All internet access to websites is monitored and matched against threat intelligence services (for example https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/url-filtering-pandb.html).

3.14 For staff and student protection the firewall will block sites that are known to contain phishing (attempting to acquire sensitive information such as usernames, passwords, and credit card details etc.), malware (viruses, trojans etc.) or other such malicious sites.

3.15 As part of the University's PREVENT policy, if a user tries to access to a website classed in the 'Weapons' or 'Questionable' (which includes Hate and Racism) categories by the threat intelligence service, the user will receive a message saying that the website is classed in such a way. Access information for these sites will be logged and used as per the PREVENT policy.

4. Use of Equipment and Computer Rooms

4.1 Users are responsible for ensuring that they are sufficiently familiar with the operation of any equipment they use to make their use of it safe and effective and to avoid interference with the use of it by others.

4.2 Users must take every precaution to avoid damage to equipment caused by smoking, eating or drinking in its vicinity. In particular, smoking, eating or drinking in any student computer room is forbidden.

4.3 Users must not transfer within or remove from University premises any item of computer hardware (including peripheral devices such as printers) without written permission from IT Services.

4.4 No equipment may be connected in any way into any University network without the prior written agreement of IT Services.

4.5 Users must not interfere with the use by others of the IT facilities; they must not remove or interfere with output belonging to another user.

4.6 Users shall adhere to any procedures pertaining to the security of IT facilities. In particular:

a) Access to student computer rooms must be by uCard only, doors must not be propped open;

b) uCards are the responsibility of the assigned user and must not be used by any other person.

5. Disclaimer of Liability

5.1 Whilst IT Services takes appropriate security measures to protect data and software, the University cannot and does not accept any responsibility for the loss of any data or software or the failure of any security or privacy mechanism.

5.2 The University accepts no responsibility for the financial or other consequences of the malfunctioning of any IT facility or part thereof, whether hardware, software or other.

5.3 No claim shall be made against the University, its employees or agents in respect of any loss, damage or inconvenience alleged to have been caused whether by defect in the resources or by act or neglect of the University, its employees or agents.

6. Failure to Observe the Rules

6.1 Any infringement of these Rules may be subject to penalties under civil or criminal law and the University is prepared to invoke such law.

6.2 Any infringement of these Rules constitutes a disciplinary offence and, regardless of legal proceedings, established disciplinary procedures will be followed for staff and students.

6.3 For the general guidance of students, the least serious offences are liable to resu in temporary withdrawal of facilities and a formal warning. More serious offences will carry longer terms of suspension and possibly fines, together with a formal warning. In the most serious offences termination of studies will be considered.

6.4 Authority is vested in the Head of IT and Officers of the University temporarily to suspend access to IT facilities by any user suspected of a breach of these Rules pending full investigation.

EMAIL POLICY

1 The Policy

1.1 The purpose of this Policy is to provide information about the provision of the University's email services and to provide guidelines for users to help ensure effective, safe, and responsible use.

1.2 The Policy applies to all University staff and students and to any other authorised user.

1.3 The Head of IT Services is responsible for drafting the Policy, directing it through the consultative and approval processes and for periodically reviewing it.

1.4 Email services are part of the University's overall IT provision and this Policy should therefore be read in conjunction with the following related documents:
- 1.4.1 Rules and Regulations on the Use of University Computers and Data Networks.
- 1.4.2 The JANET Acceptable Use Policy.

1.5 The Policy will be distributed to all users and made available on the University Web site.

2 Principles of Email Provision

2.1 The University provides email facilities to authorised users for the purposes of teaching, learning, research, administration and approved business activities. Limited personal use is allowed under certain conditions (specified in 7.4 below).

2.2 All email use is subject to:
- 2.2.1 The relevant legislation.
- 2.2.2 The University's Rules and Regulations on the Use of University Computers and Data Networks.
- 2.2.3 The conditions of the JANET (Joint Academic Network) Acceptable Use Policy.
- 2.2.4 The conditions and guidelines established in this Email Policy.

2.3 Email cannot be assumed to be a secure medium and should not be used for the transmission and/or storage of confidential data.

3 Statement of Responsibilities

3.1 The Head of IT Services is responsible for developing and communicating policies and procedures for the University's email system and its usage. The Head of IT Services is also responsible for dealing with complaints regarding email usage and, in the first instance, for dealing with breaches of the conditions of this Policy.

3.2 IT Services is responsible for the administration of user email accounts and for the provision of a reliable and effective email system.

3.3 The users of the email system are responsible for ensuring that they are acting in compliance with legal and acceptable use conditions.

4 Access

4.1 Authorised users are issued with an email account by IT Services. This account should be secured by the user with a personal password. Most passwords can be cracked easily so your choice should be made with great care, changed frequently and never disclosed to another. (The only exception to this is that passwords may need to be imparted to IT Services staff for PC upgrades or, in exceptional circumstances, to deal with technical faults. In such circumstances the password should be changed immediately after the work has been carried out.) For advice on choosing and managing passwords see the JANET factsheets *Using* Passwords and *Threats to* Passwords at http://www.ja.neVservices/publications/security-publications.html

4.2 Account holders must not allow any other person to access their accounts (remember to log off or lock your workstation when leaving your desk). In situations where temporary access is required by another, IT Services should be contacted for alternative arrangements. An example of this would be where a secretary was required to access a manage s email account.

4.3 In cases of unexpected absence, a line manager can request access to an employee's email account for business purposes. Such access must be authorised by the Dean or Administrative Head of Department.

4.4 Email accounts are created on the authorisation of the HR Department for staff and on the authorisation of Registry for students. Accounts for honorary or associate members of staff are created on the authorisation of the relevant Dean or of the Vice-chancellor and are subject to annual renewal.

4.5 Staff email accounts are closed immediately after a staff member leaves the University. Accounts may remain open for a discretionary period if approved by the relevant Dean, Head of Department or the Vice-Chancellor. Notification of leaving is the responsibility of the HR Department.

Honorary Fellows and Fellows will be provided with a staff mailbox. Former members of staff in receipt of this reward will retain their staff mailbox.

4.6 Once a student has completed their studies, their computer account will be terminated. Notification of leaving is the responsibility of Registry. The following is the account termination timeline:

4.6.1 7 days after completion – uCard expires.

4.6.2 35 days after completion – student will receive an email warning that their account will be disabled in 7 days. The student should back up any emails and data that they require at this time.

4.6.3 42 days after completion – student account will be disabled.

4.6.4 70 days after completion – student account will be deleted.

4.7 Student accounts are subject to a maximum storage quota of 1OOMB. Appeals for an increase in this quota, for legitimate academic purposes, should be made to the Head of IT Services.

4.8 Remote access via the Web is available to all email accounts.

5 Mailing Lists and Public Folders

5.1 There are a number of official University mailing lists from which users cannot opt out. The static mailing lists are: Staff; Academic Staff; Students-Announce. Hierarchical dynamic mailing lists are also available with membership determined from the Human Resources system. These take the form of -<dept> Admin Staff, -<dept> Academic Staff, and these contribute to -<dept> Staff and -All-Staff. Postings to these mailing lists should therefore be restricted to official departmental or University messages and not used as open discussion lists. Discussions or notices that are of interest to particular groups should be communicated using specific mailing lists or Public Folders, see 5.2 and 5.3below.

5.2 Staff mailing lists for departments or specific groups can be set up, subject to approval by IT Services. Mailing lists for student societies should first be authorised by the Students Union.

5.3 Staff open or group restricted Public Folders can be set up, subject to approval by IT Services. Public Folders for student societies should first be authorised by the Students Union. Public folders are provided for discussion issues that may not be relevant to all users.

6 Standards of Acceptable Use: compliance with legislation

With email, as with all other uses of the University's IT facilities, it is the user's responsibility to make themselves aware of the laws that apply to such use. Breaches of the law could result in liability for individual users, as in a recent libel case, and/or for the University. It should be noted that email messages (deleted or otherwise) may be treated as written evidence in law.

Following are some of the areas of law which apply to use of email; explanatory comment has been added where thought to be helpful:

6.1 Copyright.
Users should not use email to send or store text, images, software or recordings to which the users do not hold the copyright or intellectual property rights, unless they have the written permission of the rights holder. This includes forwarding messages to a third party without the permission, explicit or implied, of the originator.

6.2 Computer Misuse.
Users must not attempt to gain unauthorised access to computer material. Users must take all reasonable steps to prevent the receipt and dissemination of computer viruses or other such malicious software. In practice this means following the guidelines issued by IT Services and notifying the Helpdesk if in any doubt.

6.3 Data Protection.
If you include in your email any personal data, including photographs, about a living, identifiable individual, the law deems you to be "processing" personal data and you must therefore abide by the terms of the law.

6.4 Malicious Communications.
This Act makes it an offence to send a message intending to cause distress or anxiety, whether this takes the form of threat, offensive material or false statements.

6.5 Equality
It is an offence to send emails which discriminate against persons based on their gender, sexuality, race, disability or age. The act covers direct discrimination by sending messages intended to treat the recipient less favourably than others based upon protected characteristics, indirect discrimination intending to put in place systems for everyone which unfairly disadvantage those of a protected characteristic, or sending emails intended to harass or victimise. Defamation. You must not send emails that are likely to cause serious harm to the reputation of a person or company. Statements which are true, are stated as an honest opinion, form part of a matter of public interest, or have been peer-reviewed as part of a scientific or academic investigation and are made without malice are permitted.

6.6 Obscenity.
It is an offence to send messages, whether for gain or not, where the content will tend to deprave and corrupt the recipient. This includes images of a sexual nature or torture.

Further guidance on copyright and computer misuse is available from the Head of IT Services and on data protection from the HR Department.

7 Standards of Acceptable Use: compliance with University guidelines

7.1 Use of the University's IT facilities constitutes acceptance of the University's Rules and Regulations and of the JANET (Joint Academic Network) Acceptable Use Policy.

7.2 Users should note that the JANET Policy specifically prohibits the transmission of unsolicited commercial or advertising material apart from that relating to the University's own products and services.

7.3 Users are expected to comply with University policies and codes of behaviour. Relevant ones include:
7.3.1 Intellectual Property.
7.3.2 Dignity at Work and Study Policy and Procedures.

7.4 Use of the University's email for personal purposes is permitted within reasonable levels. For

guidance such use should not:

7.4.1 Interfere with the user's required University responsibilities or with those of other University users.

7.4.2 Jeopardise or interfere with the system so as to reduce the level of service for University business.

7.4.3 Have a negative impact on the University in any way.

7.5 Attachments to internal email messages place a heavy load on the network and the email server, thereby reducing the level of service to other users.

7.5.1 Large attachments (between 500KB and 100MB) should be placed on the University's Large File Upload facility (https://lift.buckingham.ac.uk/) and the URL resulting from the upload should be sent by email.

7.5.2 Attachments to emails are limited to 20MB. Users with requirements over this limit should contact IT Services.

7.5.3 If documents can be held in a shared area of the network or on the Web site, then users should point the recipient to this location rather than sending the document by email. Staff users, for example, can use departmental drives or the interdepartmental area: drive N.

7.5.4 Attachments received and kept for future reference should be moved to the user's home directory and not stored within the email system.

7.6 Users are responsible for their handling of received email messages and attachments.

7.6.1 To protect themselves and others from viruses users should not open unexpected attachments and should report suspicious attachments to the Helpdesk.

7.6.2 Users must not make changes to their computers on outside advice (for example: emails claiming to be virus removal instructions). Such information should be passed to IT Services for evaluation.

7.7 Users should use their email storage areas responsibly, regular1y clearing all folders of non-current messages.

7.8 Users are required to access their email accounts on a frequent and regular basis as the email medium is used for official University communications.

8 Standards of Acceptable Use: best practice or 'netiquette' guidelines

8.1 Always avoid using email where face-to-face or telephone communication would be more courteous or effective.

8.2 Before sending an email, double-check that you have the correct addressee and correct format of the address. (For internal messages, use the Check Names facility.)

8.3 Be sparing in your use of the cc facility. Only copy in those who really need to know.

8.4 Similarly, avoid the 'Reply to All' button unless 'All' really need to know.

8.5 Similarly, use group emailing facilities with great care. Only email those who really need to know and make sure your group contains the correct members and addresses.

8.6 Never forward another's message to a third party without the permission, explicit or implied, of the originator. In this respect, great care should be taken when forwarding that you are not including a string of ear1ier communication.

8.7 Remember that email is not a secure medium. Treat your message as you would a postcard.

When replying to an email avoid including all previous discussions and only include earlier sections relevant to your response.

8.8 Ensure that your subject line adequately describes the content of your message and do not use an email message for more than one subject.

8.9 Avoid using the high priority exclamation mark (unless absolutely essential) or using capitals in your text. Both of these devices have the effect of shouting at your recipient.

8.10 Take care to ensure that the tone of your message is clear; irony and humour, for instance,

are easily misunderstood in this medium.

8.11 Remember the laws relating to harassment, libel, etc. and think twice before making any remarks that may appear critical of the recipient or a third party.

8.12 Use blind copy (bee) when sending messages to a group where the recipients do not know each other's email addresses or it is intended to keep the distribution list private (such as a mass emailing to recipients outside the University). This prevents unauthorised distribution of email addresses where the recipients would not wish to know or be contacted by other's on the distribution list. Note that if you respond to an email that you were blind copied you will only be able to reply at most to those who were in the "to" or "cc" lists.

9 Official University correspondence

9.1 Where a member of staff undertakes email correspondence on behalf of a school or department and there is a reasonable expectation of a reply they should, where possible, send from/on behalf of a departmental mailbox rather than a personal mailbox. This both ensures the email looks official, and ensures the respondent replies to the departmental mailbox rather than an individual (who may be absent when the reply is received).

9.2 Departmental mailboxes can be requested by any department, and should be monitored by more than one person to avoid message being missed during periods of absence on the part of any one person. Requests for departmental mailboxes should be made by the Dean or Administrative Head of Department to the IT Services Helpdesk.

10 Out of office

The Universities email system provides an "Out of Office" facility for all staff and students to enable users to advise correspondents of alternate arrangements during a period of absence. Out of office replies can be sent to internal correspondents and (subject to the user's preferences) external email correspondents.

10.1 Prior to any planned absence (e.g. annual leave) staff should activate their Out of Office message with alternative contact arrangements and details of any departmental mailbox. This ensures important business correspondents are made aware of the alternate arrangements during absence.

10.2 If a staff member does not tum on their Out of Office message and important business emails are likely to be sent direct to the user's mailbox rather than a departmental mailbox, their line manager may request a staff members Out of Office message to be turned on. This must be authorised by the Dean or Administrative Head of department and can then be turned on by IT Services.

10.3 If a staff member sets an out of office message which, in their line manager's opinion, does not contain appropriate alternate arrangement information, the line manager can request the message is changed by IT Services. Such action requires approval from the Dean or Administrative Head of Department.

10.4 Out of Office messages (for external recipients) should avoid detailing the users leave plans as this may increase personal security risks.

11 Monitoring

11.1 The University complies with the terms of The Regulation of Investigatory Powers Act 2000. This Act makes it an offence intentionally or without lawful authority to intercept communications without the express or implied consent of both the sender and the recipient of the communication.

11.2 There are, however, permitted exceptions to the principle that interception without consent is unlawful. These include:

11.2.1 Ensuring the effective operation of the system, for instance:

11.2.1.1 Scanning for viruses and other potentially harmful attachments.

11.2.1.2 Monitoring email storage usage.

11.2.1.3 Forwarding messages to the correct address.

11.2.1.4 Eliminating spam.

11.2.3 Investigating or detecting unauthorised use.

11.2.4 Checking whether communication is relevant to the University's business, for instance, in cases of unexpected absence due to illness or accident. This must be

authorised as described in 4.3 above.

11.2.5 Ascertaining compliance with regulatory practices or procedures. This must be authorised by the Secretary to Council and only in instances where there is reasonable suspicion of misuse.

11.2.6 Preventing or detecting crime or in the interests of national security. This must be authorised by the Secretary to Council and only in instances where there is reasonable suspicion of criminal misuse or on the request of the police or specified public officials.

11.3 Most of the monitoring carried out by IT Services to ensure effective operation is done automatically and at the server level. There is no routine monitoring of the content of users' emails by IT Services staff.

12 Breaches of the Conditions of this Policy

12.1 Complaints about usage and notification of alleged breaches of the rules and regulations relating to network use should be made, in the first instance, to the Head of IT Services.

12.2 If a breach of the Rules and Regulations on Use of University Computers and Data Networks is suspected, authority is vested in the Head of IT Services (or nominated deputy) and Officers of the University to suspend temporarily access to email accounts by any user suspected, pending full investigation.

12.3 Investigations that involve accessing a user's email account should be referred to the Secretary to Council for authorisation.

12.4 Any disciplinary action taken will follow the University's agreed disciplinary procedures for staff and students.

13 Related Documents

13.1 Rules and Regulations on Use of University Computers and Data Networks
Location: the University Web site: http://www.buckingham.ac.uklits/rules/

13.2 JANET Acceptable Use Policy
Location: linked to from the University Web site via the above link, or at:
http://www.ja.net/company/policieslaup.html

IT Services
June 2016