

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 result 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.net/services/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 manager'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 remain open for a discretionary period, usually three months, after a staff member has left. Notification of leaving is the responsibility of the HR Department.
- 4.6 Student email accounts are closed after the cessation of studies with a grace period of two months from the last day of the final term being granted to finalists. Notification of leaving is the responsibility of Registry.
- 4.7 Student accounts are subject to a maximum storage quota of 100MB. 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 currently three official University mailing lists from which users cannot opt out, these are: Staff; Academic Staff; Students-Announce. 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 5.3 below.
- 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 Discrimination: Sex, Race or Disability
- 6.6 Defamation.
- 6.7 Obscenity.

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 Code of Practice on Dignity at Work.
- 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 (<http://www.buckingham.ac.uk/lift>) 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, regularly 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 earlier communication.
- 8.7 Remember that email is not a secure medium. Treat your message as you would a postcard.
- 8.8 Again with the postcard analogy in mind, email is a medium for informal, brief communications, so try to keep your messages short. If responding to a chain of earlier communication, only include what is relevant to the latest message and recipient.
- 8.9 Ensure that your subject line adequately describes the content of your message and do not use an email message for more than one subject.
- 8.10 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.
- 8.11 Take care to ensure that the tone of your message is clear; irony and humour, for instance, are easily misunderstood in this medium.
- 8.12 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.

## **9 Monitoring**

- 9.1 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.
- 9.2 There are, however, permitted exceptions to the principle that interception without consent is unlawful. These include:
  - 9.2.1 Ensuring the effective operation of the system, for instance:
    - 9.2.1.1 Scanning for viruses and other potentially harmful attachments.
    - 9.2.1.2 Monitoring email storage usage.
    - 9.2.1.3 Forwarding messages to the correct address.
    - 9.2.1.4 Eliminating spam.

- 9.2.2 Investigating or detecting unauthorised use.
  - 9.2.3 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.
  - 9.2.4 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.
  - 9.2.5 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.
- 9.3 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.

## **10 Breaches of the Conditions of this Policy**

- 10.1 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.
- 10.2 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.
- 10.3 Investigations that involve accessing a user's email account should be referred to the University Secretary for authorisation.
- 10.4 Any disciplinary action taken will follow the University's agreed disciplinary procedures for staff and students.

## **11 Related Documents**

- 11.1 Rules and Regulations on Use of University Computers and Data Networks  
**Location: the University Web site: <http://www.buckingham.ac.uk/its/rules/>**
- 11.2 JANET Acceptable Use Policy  
**Location: linked to from the University Web site via the above link, or at: <http://www.ja.net/company/policies/aup.html>**
- 11.3 Code of Practice on Dignity at Work  
**Location (staff only): HR Department.**

IT Services, Version 1.1, 23 Nov 2009

# **UNIVERSITY POLICIES**

## **The Environmental Policy**

The University's policy in respect of the environment can be found at:  
<http://www.buckingham.ac.uk/about/environmentalpolicy>

## **Disability Policy**

The University's policy in respect of disability can be found at:  
<https://intranet.buckingham.ac.uk/governance/Pages/PoliciesandProcedures.aspx>