UNIVERSITY ACCEPTABLE USE POLICY FOR TELEPHONE, EMAIL AND INTERNET USE

Introduction

1.1 The use of Electronic Mail (email) and Internet has grown considerably in recent years. The Internet is one of the most popular sources of information whilst ease of use and speed has made email the most common form of communication between people. When used correctly, the internet and email provides an efficient way of sharing information. Correspondingly, incorrect or improper use will have the opposite result.

1.2 Any serious misuse of the systems may be regarded as a disciplinary offence.

1.3 This policy respects and complies with the applicable laws including (but not limited to):

- Telecommunications Act 1984
- Copyright, Designs & Patents Act 1988
- Computer Misuse Act 1990
- Disability Discrimination Acts & SENDA 1995
- Data Protection Act 1998
- Human Rights Act 1998
- Regulation of Investigator Powers Act 2000
- Freedom of Information Act 2000
- Electronic Communications Act 2000

No provision contained in the policy is intended to contradict or contravene such legislation. Neither is this policy meant to restrict legitimate and authorized academic activity.

1.4 All University members must comply with this policy as set out below, and must be aware that the use of any system is not confidential. Use may be monitored (as described below) to ensure compliance with University policies and legislation.

General Policy Statement

2.1 A breach of this policy may result in disciplinary action in accordance with the University's disciplinary procedure. In certain circumstances, *e.g.* using email to communicate obscene material, a breach of this policy may be considered to be gross misconduct resulting in dismissal.

General Use

University systems must not be used inappropriately. The following is an illustrative list of inappropriate use, but it is not intended to be exhaustive.

Telephones, Email and the Internet, including social networking sites, must **not** be used for:

- Harassment or bullying – all communications should be consistent with the University's Equal Opportunities Policy and Guidelines for Dealing with Harassment.
- Private commercial purposes.
- Breaching copyright or confidentiality.
- Intentional propagation of viruses.
- Disrupting or damaging other systems by carrying out acts of a malicious or disruptive nature.
- Excessive personal use.
- Excessive use without due regard for the load this places on the University systems and the effect on other users for example downloading games to play against others across the Internet or sending bulk emails (please refer to the annex at the back for further information).

Monitoring Use

The Regulation of Investigatory Powers Act does not allow the interception of communications by an employer unless the employer has "lawful authority". The Lawful Business Practice Regulations authorise monitoring for a number of purposes (listed below) and the University has selected the least intrusive methods of monitoring. While the University has no wish to interfere with the privacy of its members, it is required to discharge a number of legal duties that are laid down on all employers and managers of computer systems concerning what passes through, and is stored within, their systems – for example, to ensure that these are not used for criminal or other improper purposes, to prevent the spread of computer viruses, and to avoid other situations that might corrupt or degrade the operations of the University's computer systems or those of other systems elsewhere.

Thus, the University reserves the right to monitor telephone use, Internet use, access email and other material on its computer systems from time to time for various reasonable and necessary purposes including those below:

- Checking compliance with all University regulations and policies;
- Preventing or detecting crime;
- Investigating or detecting unauthorized use;
- Checking for viruses or other threats to the performance of the system;
- Investigating abnormal system behaviour;
- Resolving a user problem;
- Monitoring standards of service or training;
- Maintaining or carrying out University business.

Such monitoring will be kept to a reasonable minimum and every care will be taken to comply with all applicable data protection and privacy legislation in respect of the confidentiality of any material that is monitored in so far as this does not conflict with duties laid down in other legislation or with the prevention of harassment or other serious breaches of the University's disciplinary code.

Personal emails will not be read by anyone except the sender or recipient if they are clearly marked as such. However, this will not be the case where access to the content of the email is required for the prevention or detection of a suspected crime or to prevent the inappropriate use of email as detailed below.

Any investigation other than day-to-day monitoring requires the written authority of the Director of Human Resources or his/her nominee in order to take place. The person who grants the authority should be satisfied there are reasonable grounds for this request.

Personal Use

The personal use of email or the Internet by staff is permitted providing that it is not excessive and does not interfere with the proper performance of that person's duties. It is good practice to maintain a distinction between what is a business email and what is a personal email, for example by marking personal emails as 'personal'.

The personal use of email and Internet for students is permitted and it is acknowledged that use of these services is not only an integral part of study and engagement with member of staff but particularly on ResNet use might be expected to be social as well as academic.

Telephones, email and the Internet must not be used to carry out private commercial activities

Personal telephone calls should be kept as brief as possible. Personal calls should not be made to non-geographic numbers (starting 084 or 087), mobile phones or overseas numbers without prior permission. The faculty or department must be reimbursed for the cost of the calls.

Internet Use

The Internet is accessed via the university network which is provided via the Joint Academic Network (JANET). All traffic must adhere to the JANET Acceptable Use Policy. Users should be aware of and comply with this policy.

Staff should note that personal use is a privilege and must not be excessive or interfere with the proper performance of an employee's duties.

The Internet must not be used inappropriately. The following is an illustrative list of inappropriate use, but it is not intended to be exhaustive. The Internet must not be used for:

- Accessing, downloading, storing recording or bookmarking sites that are offensive, obscene, defamatory, abusive or otherwise unlawful. (for instance, those that facilitate hacking or contain pornographic material).
- Publishing material that brings the University's reputation into disrepute.
- Downloading software which breaches the software company's rights or licence agreements.

Unfortunately the largely uncontrolled nature of the Internet means that users can inadvertently access sites containing offensive, obscene, defamatory, abusive or otherwise unlawful material. In these instances users must exit such sites immediately. Prolonged or regular access to such sites is considered as intentional misuse of the facility.

The University takes no responsibility for any online transactions and is not liable for the failure of security measures. All users should be aware that Internet use may be recorded.

Email Use

In terms of the law, email communications are no different to any other form of written communication; they can be legally binding. Consequently they are, for instance, actionable within the laws of defamation and libel; they are recognised as being capable of contributing to harassment; and they can create or break contracts.

Emails frequently carry information about individuals (personal data) in the form of facts, intentions or opinions about individuals. Any emails produced in the course of University business that contain personal data must be managed in compliance with data protection legislation. This includes the right of individuals to request a copy of the data held about themselves on request.

The email system is the property of the University of Surrey but this does not alter the intellectual property rights in the work. Staff should note that personal use is a privilege and must not be excessive or interfere with the proper performance of an employee's duties.

The email system must not be used inappropriately. The following is an illustrative list of inappropriate use, but it is not intended to be exhaustive. Email must **not** be used for:

- Sending messages that are offensive, obscene, defamatory, abusive or otherwise unlawful. Emails, like any other form of written communication, can be used as evidence in a court of law.
- Sending material that brings the University's reputation into disrepute.
- Sending links to web pages or bulletin boards that are offensive, obscene, defamatory, abusive or otherwise unlawful (for instance, those that facilitate hacking or contain pornographic material).
- Sending unsolicited commercial or advertising material

- Sending personal data to countries outside the European Economic Area without the agreement of the Information Compliance Unit.

Unfortunately the largely uncontrolled nature of the Internet means that email users can be identified remotely and streams of offensive advertising and other material directed to them, although they themselves may have taken no action to solicit this. All email users are, therefore, asked to contribute to the monitoring and control of this nuisance by reporting the receipt of offensive email as promptly and fully as is reasonably practical, *via* the relevant management chain (or as may from time to time be advised) in order to assist the University in taking steps to block the offending material.

All should be aware that deleting an email may not remove all instances of that message. There may be copies of the message elsewhere, for instance, the recipients system or back up files held on central servers.

Access to Email Accounts on Departure

Entitlement to access an individual's email account will normally automatically cease on the date on which an individual's relationship with the University of Surrey has terminated; with the exception of Students who will continue to have access up to 30 days after this date. If additional access is required to an email account then this must be authorised by the Director of HR for staff or the Dean of Students for students.

Key Points of Reference

- Write all email messages in a professional manner. The content of an email should be to the same standard as a letter.

- Consider carefully the full implications of sending bulk emails (emails to large numbers of recipients). For example, a 5MB email sent to 2000 staff could consume 1000Mb of server disk space.

- Try and minimize the size of emails. Most emails should be less than 5 Kb. Emails larger than 5Mb should not be sent without first consulting IT Services and your System Administrator.

- The University Email Mailing List System is provided for the support of academic activities and University business only. If you wish to use the Mailing Lists please only send short, text messages and never send attachments. We strongly recommend you use internal web pages to publish information and pictures and then circulate the web link (URL) in your email messages.

- Be careful when sending emails containing personal or confidential information. Check the recipient's name, especially if there is more than one person with the same name.

- Avoid sending sensitive information in an email. Sending an email is like sending a postcard through the post.

- Try to minimize the use of graphics, different fonts, formats stored within a document when sending it as an attachment to an email.

- Do not open attachments from unknown sources. Always virus scan a document received as an attachment in an email before opening the document.

- The receipt of any email communication containing obscene material must be reported immediately to either your manager or the Director of Information Services.

- Emails should **not** be accepted if they contain inappropriate language and/or content. They should be returned immediately to the sender with a request for a revised version to be submitted. If appropriate, your manager and/or IT Services should be informed.

- You should endeavour to ensure that personal email cannot be interpreted as official University correspondence.

- Avoid using uppercase text unless for particular emphasis, as this is interpreted as shouting.

- Be careful when using humour or sarcasm within a message as this can be easily misinterpreted.

- Try to save email within a meaningful file structure and delete messages in line with agreed retention periods.