UNIVERSITY OF ST ANDREWS

EMAIL POLICY

November 2005

I Introduction

1. Email is an important method of communication for University business, and carries the same weight as paper-based communications. The purpose of this policy is to describe the acceptable use of the University's email and related services, systems and facilities.

2. The document covers:

   Status of the Policy
   Scope of the Policy
   Responsibilities
   Monitoring
   Third party access to email
   Personal use by staff
   Relationship with existing policies
   Guidance for implementation of the Policy
   Contact details

II Status of the Policy

This Policy has been approved by the University Court of St Andrews, and supersedes any previous email policy.

III Scope of the Policy

1. This Policy applies to all University staff, students and any other authorised users. It covers the use, for the purpose of sending or receiving email messages and attachments, of any IT facilities provided by the University, including hardware, software and networks.
2. The Policy describes the University's position on
   - The personal use of email
   - Potential monitoring or interception of email
   - Third party access to email

IV Responsibilities

1. Responsibility for developing and updating this policy lies with the University Court acting, if appropriate, on the advice of the Director of ITS.

2. All users, whether they create or receive emails, have a responsibility to ensure they make appropriate and proper use of the system, and that they comply with this policy and

the guidelines provided by the University. See Appendix C.

3. Any member of staff who fails to comply with the Policy and the guidelines may be subject to disciplinary action. It is the responsibility of Heads of School and of Directors of Unit to ensure that their staff are made aware of the existence and content of the Policy and of the guidelines.

4. Students found to be in breach of this Policy and the guidelines may be subject to disciplinary action.

5. Any other authorised user who breaches the policy may have any privileges in relation to appropriate University facilities withdrawn.

V Monitoring

1. The University complies with the terms of the Regulation of Investigatory Powers (Scotland) Act 2000. This act covers the extent to which organisations can monitor or record communications. The conditions under which monitoring may be lawful are described in Appendix B.

2. Monitoring of the system by IT Services is carried out to ensure its effective operation. Email is checked routinely at the server level by the mail delivery software for spam and virus content. Full details of these and other checks can be found in the ITS Email Service Definition document.

VI Third party access to email (See Appendix B)

In cases of unexpected or prolonged absence which adversely affects the running of the institution, the University may provide access to an employee's email account for business purposes. Requests for this type of access must be made, in the first instance, by the employee's line manager to be approved by a member of the Principal's Office. The request, the reasons behind it, the extent and duration of access, and action taken will be logged.

Once approval has been given, IT Services will arrange access in accordance with instructions from the Principal's Office. When it is appropriate, the owner of the email account should be advised of what has happened.

It is important, in this process, that any emails which are clearly private or personal are treated as confidential.

VII Personal Use

1. The University of St Andrews provides a range of computing facilities and resources for authorised users pursuing legitimate University interests. While users may have the use of an email address(es) while they are authorised users, the University retains ownership of that address and all other parts of the email facility.

   The University accepts, however, that appropriate use of e-mail for private non-commercial purposes is permissible. This use should, nevertheless, not require the University to provide additional resources over that which it provides for business use.

Users should ensure that emails addressed to or sent by them for private purposes are marked as personal, in order to distinguish between business and private emails.

Users should, however, be aware that the privacy of emails cannot be guaranteed, messages can be intercepted or wrongly addressed and they are easily forwarded to third parties.

Users must adhere to the University guidelines in Appendix C when using the system for personal purposes.

2. Personal use by staff
Personal use of the email system may take place in an employee's own time provided it does not interfere with the smooth running of the University, or deny resources to other users.

VIII Relationship with existing policies

1. This Policy has been formulated within the context of the following University documents:

Data Protection Policy
Freedom of Information Policy
Records Management Policy
Conditions for the Use of Computers within the University
Staff and Student Codes of Discipline

all of which are available from the University's Website.

2. Compliance with this Policy will facilitate compliance with other information-related legislation, and specifically the Data Protection Act 1998.

IX Guidelines for Implementation of the Policy

Guidelines with regard to the procedures necessary to comply with this Policy are available on the University's website. This guidance relates, *inter alia*, to:

Personal use
Monitoring
Current legislation
Appropriate use
Inappropriate use
Security

X Contact details

Secretary to the University Court

_____

Appendix A

Definition of terms

Email systems

This covers any IT facilities provided by the University, including hardware, software and networks, for the purpose of sending or receiving email messages and attachments.

Users

This covers

- All staff using the email systems
- All students using the email systems
- Any other authorised individual using the email systems

Appendix B

Regulation of Investigatory Powers (Scotland) Act 2000

This Act covers the extent to which organisations can monitor or record communications at the point at which they enter or are being sent within the employer's telecommunications system, and applies to public and private communication networks. It gives the sender or recipient of a communication the right of action for damages against the employer for the unlawful interception of communications.

There are two areas where monitoring is not unlawful. These are:

- where the employer reasonably believes that the sender and intended recipient have consented to the interception

- without consent, the employer may monitor for certain purposes [Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.] These include:

    - to ensure standards of service are maintained
    - to prevent or detect crime
    - to protect the communications system – this includes unauthorised use and potential viruses
    - to determine the relevance of the communication to the employer's business – ie picking up relevant messages when someone is away from work
    - to ensure compliance with regulatory practices

The University does not routinely monitor or intercept email except as described in the ITS Email Service Definition document, but it reserves the right to do so in exceptional circumstances within the terms of the Act.

The member of the Principal's Office responsible for Business Improvements will maintain a log of authorised interceptions.

Appendix C

Guidelines on email use – to be read in conjunction with:

University email policy

JANET acceptable use policy

ITS email service definition

1 Introduction

A written email policy and guidelines, known to all staff and students, establishes the boundaries and uses that may be made of the University's equipment and infrastructure. Adhering to this guideline document will:

- facilitate implementation of the University's email policy
- help users avoid legal risks that they might inadvertently take
- notify users of any privacy expectations in their communications
- prevent damage to systems
- avoid or reduce inappropriate time being spent on non-work related activities
- help protect the University against liability[1] for the actions of its staff and students.

2 Legislation

All users of the University email system must comply with the relevant legislation. (See Appendix C.)

Users should remember that the laws of the land relating to written communication apply equally to email, including laws on data protection, freedom of information, defamation, copyright, obscenity, fraud and wrongful discrimination.

---

[1] An employer is vicariously liable for negligent acts or omissions by his employee in the course of employment whether or not such act or omission was specifically authorised by the employer. To avoid vicarious liability, an employer must demonstrate either that the employee was not negligent in that the employee was reasonably careful or that the employee was acting in his own right rather than on the employer's business.

3 Personal Use

The email system is provided to facilitate the work of the University. This applies to both staff and students.

The University accepts, however, that using email for private non-commercial purposes is permissible, provided it does not interfere with the smooth running of the University, or deny resources to other users. Staff and students should ensure that they do not make inappropriate use of the system.

For advice on managing personal email in folders, see section (5.3) below and ITS Email Service Definition document.

4 Inappropriate use

Inappropriate use includes, but is not limited to, the creation or transmission of emails:

- that bring the University into disrepute
- that consist of unsolicited commercial or advertising material, chain letters or other junk-mail of any kind
- that infringe the copyright of another person, including intellectual property rights
- that unreasonably waste staff effort or networked resources, or that unreasonably serve to deny service to other users
- that contain any offensive, obscene or indecent images, data or other material
- that are designed to cause annoyance, inconvenience or anxiety to anyone
- that include material which is sexist, racist, homophobic, xenophobic, pornographic, paedophilic or similarly discriminatory and/or offensive
- that contain defamatory material
- that contain material that includes claims of a deceptive nature
- that by intent or otherwise harass the recipient
- that violate the privacy of others, or unfairly criticise or misrepresent others
- that are anonymous messages or deliberately forged messages or that have deceptive email header information (ie without clear identification of the sender).

5 How to use email appropriately

5.1 Receiving email

- Check your email regularly.
- Staff are expected to check their email at least once every working day.

- Students are expected to check their email at least once every 48 hours.

5.2 Sending email

5.2.1 General advice

- Always remember that sending email from your University account is equivalent to sending a letter on the University letterhead.
- Make sure that you use the ‘subject’ line in every message, and that it is meaningful. Where someone receives many messages, it helps to be able to judge the subject matter correctly from its subject line.
- Try to restrict yourself to one subject per message, sending multiple messages if you have multiple subjects. This helps recipients to use the ‘subject’ line to manage the messages they have received.
- Create a ‘signature’ and use it. Most email programs allow you to create a few lines of text that appear at the end of every email. You can use your signature to provide information such as your role and telephone number.
- Try to keep email messages fairly brief.
- Delete unwanted messages to conserve disk space. Develop an orderly filing system for those email messages you wish to keep.

5.2.2 Replying to email

- Reply, even if a brief acknowledgment is all you can manage in the meantime.
- Reply promptly.
- When you use the ‘reply’ option, ensure that the subject field (automatically filled in for you) still accurately reflects the content of your message.
- Be careful when using ‘cc’ and ‘bcc’. Only copy the email to those people who really need to see it.
- When replying include a relevant chunk of the original message – replying to a message with just ‘I don't think so’ can be confusing even with a relevant subject line.

5.2.3 Forwarding email

- Think twice before forwarding to someone else an email you have received. Would the author expect or be willing for this to happen?
- The laws of copyright must be respected. It is not, in general, legal to forward material without permission from the copyright owner.

5.2.4 Good manners

- Be careful how you express yourself. Email can easily convey the wrong impression.
- Remember that people other than the person to whom it's addressed may see your message.
- Never email something you wouldn't say to the recipient's face.
- Don't criticise other people harshly. Assume that the email will be forwarded to them and will be read by them.
- Don’t forward email to other people without informing the author.
- Don't send unnecessary attachments. If you must send an attachment, give the recipient advance warning.

5.3 Storing email

- Delete all unwanted messages in order to conserve disk space.
- Develop an orderly filing system for those email messages you wish to keep.
- Create a mail folder to store your personal messages.
- Remember that stored messages in Eudora are not password-protected – anyone with access to your computer will be able to read them.
- For advice on efficient management of your mail using Eudora see ITS Email Service Definition document.

5.4 Legal Issues

- Remember that any email you write or store may be liable to be disclosed under the Data Protection Act 1998 or the Freedom of Information (Scotland) Act 2002.
- Don't make changes to someone else's message and pass it on without making it clear where you have made the changes. This would be misrepresentation.
- Remember that the various laws of the land relating to written communication apply equally to email messages, including the laws relating to defamation, copyright, obscenity, fraudulent misrepresentation, and wrongful discrimination.

6 Confidentiality

- Email is fairly insecure. Do not put anything in an email message that you would not want read by everybody.
- The commonest breach of confidentiality is wrongly addressed mail.
- If you receive a message intended for someone else, let the sender know.

- Anything you receive may not have originated from where it says it does, as email headers are easily forged. Therefore never disclose anything confidential, such as your password or credit card number, in an email message.

- Be aware that the recipient of your message might forward it to others without recognizing the need to seek your consent. You cannot be sure who these other recipients will be.

7 Interception of email

In general, the privacy of the content of emails will be respected.

There will be exceptional circumstances, however, when the University may require access to email accounts including their contents. These reasons include:

- unexpected or prolonged absence of a member of the University where not dealing with his or her email in a timely manner adversely affects the running of the University.

- to fulfil a legal requirement e.g a Subject Access Request under the Data Protection Act.

Where the content of emails is to be accessed for either of the above purposes, the action must be approved by a member of the Principal's Office and that action logged (see University of St Andrews Email Policy Section VI).

For a description of the framework within which the University may intercept email see University of St Andrews Email Policy, Appendix B

For a detailed explanation of ITS practice in this area see ITS Email Service Definition document.

Legal considerations

Human Rights Act 1998

This provides for the concept of privacy – giving a 'right to respect for private and family life, home and correspondence.' The provision is directly enforceable against public sector employers, and all courts must now interpret existing legislation in relation to the Human Rights Act.

Regulation of Investigatory Powers (Scotland) Act 2000

This Act covers the extent to which organisations can monitor or record communications at the point at which they enter or are being sent within the employer's telecommunications system, and applies to public and private communication networks. It gives the sender or recipient of a communication the right of action for damages against the employer for the unlawful interception of communications.

Data Protection Act 1998

Individuals have a right, within certain limits, to have a copy of any personal data the University

holds about them. Personal data includes any expression of opinion about an individual, whether held on paper or electronically. The individual's right of access may extend to material held in an individual's email mailboxes, or on the server.

Freedom of Information (Scotland) Act 2002

The University has only 20 working days to supply information requested under this Act. The Scottish Information Commissioner has made it clear that he will interpret the 20 working days as beginning the day after the request is made. In other words, an FoI request made by email will be deemed to have been received by the University without it's even having been opened. The request may also cover material contained in emails in an individual's mailboxes.

Copyright law

The Copyright, Designs and Patents Act 1988 (as amended) gives the same protection to digital and electronic publications as it does to printed books and other forms of publication.

Obscene Publications Act 1959, Protection of Children Act 1988, Criminal Justice Act 1988

These acts are concerned with material that might be criminal, cause harm to young persons or be otherwise unlawful. Circulating text or images via email might subject an individual to charges of criminal behaviour.

In Scotland, where the Obscene Publications Act does not apply, the Civic Government (Scotland) Act 1982 makes it an offence to publish obscene material and prosecution is the responsibility of the Procurator Fiscal Service.

Privacy and Electronic Communications (EC Directive) Regulations 2003

This covers unsolicited direct marketing activity by telephone, by fax, and by email.

Malicious Communications Act 1988

This act deals with the offence of sending letters etc with intent to cause distress or anxiety and states:

> It is an offence to send an indecent, offensive or threatening letter, electronic communication or other article to another person.

The Protection from Harassment Act 1997

This act was mainly passed in order to deal with problems in the law applying in England and Wales. However sections 8 to 11 apply to Scotland.

> **8.** - (1) Every individual has a right to be free from harassment and, accordingly, a person must not pursue a course of conduct which amounts to harassment of another and-
>
> (a) is intended to amount to harassment of that person; or
>
> (b) occurs in circumstances where it would appear to a reasonable person that it would amount to harassment of that person.