University of Warwick - Electronic Mail Policy

Introduction

Email is an important means of communication for the University and needs to be managed and used appropriately. The purpose of this document is to set out the University’s policy on the use of email in order to:

- Establish rules on acceptable use of email
- Safeguard the operation of the email facilities and minimise risk of disruption to those facilities
- Clarify issues of privacy, ownership and security of electronic communications

Scope

The policy applies to all email facilities provided by the University, including any operated by departments. It applies to all users of these facilities.

Access

Only staff, students and other persons authorised by appropriate University authority are entitled to use the University’s email systems and resources. If IT facilities are misused access may be withdrawn according to the procedures defined in the Regulations Governing the Use of University Computing Facilities (see University Calendar or IT Services web site).

Acceptable Use

University email facilities are provided to support the University’s activities including learning, teaching, research, administration and approved business activities. The principles of academic freedom, as set out in University Statute S.28, apply to its use.

Email must be used responsibly and in compliance with the law and with all University regulations and policies. In particular all users are subject to the ‘Regulations governing the use of University Computing Facilities’. These are published in the University Calendar and are available on the University web site.

Use of email requires the same care and imposes the same obligations as any other medium of communication. As a written medium it may persist in the sender’s and the recipient’s filestore and on backup media, and in transit it may be observed in much the same way as a postcard.

Personal Use

The University permits reasonable personal use of email facilities. Reasonable use means use that does not:

- create an identifiable cost to the University
- interfere with use of email for University purposes
- adversely impact the work of any employee
- conflict with University objectives or interests
- conflict with obligations between the University as employer and individual as employee
- involve personal financial gain or non-University commercial/profit making activities

Any such personal use is subject to the University regulations and the provisions of this policy.

Prohibited use

The University email facilities may not be used for:
the creation, transmission or storage of text, images or other material which could be considered offensive such as pornographic, unlawfully discriminatory, or libellous material.

harassment of any person or group of persons

production or promulgation of material which could bring the University into disrepute. Where such a question may arise prior permission must be sought in writing from the appropriate Chair(s) of Department(s) in the case of academic activity and from the Registrar in respect of any other matter.

undertaking, assisting or encouraging a criminal act

the transmission of unsolicited commercial email or bulk non-commercial e-mail unrelated to the legitimate educational activities of the University which is likely to cause offence or inconvenience to those receiving it (spamming); this includes but is not limited to advertisements and political and religious materials

emails which purport to come from an individual other than the user actually sending the message, or with forged addresses (spoofing)

unauthorised transmission to a third party of confidential material concerning the activities of the University. This does not conflict with the University policy on public interest disclosure

transmission of material that infringes copyright including intellectual property rights

personal gain or commercial purposes unrelated to the legitimate activities of the University

Unreasonable or excessive personal use – see above

Privacy, Security and Confidentiality

Users should be aware that:

email is not a secure medium and could be seen other than by the intended recipient, including systems administrators carrying out their normal support duties. It is not advisable to send confidential information via email

the University does not routinely monitor email content, but may make interceptions and inspections in certain circumstances within the law. These include the investigation of incidents, such as cases where there are reasonable grounds for believing there has been a contravention of rules, regulations or the law, and the investigation of abnormal systems behaviour. For more details of see the University Statement on the Regulation of Investigatory Powers Act

in the event of unplanned absence and access being required to email held in a user's account reasonable efforts must be made to contact the account holder and seek an agreed means of access to the material. In circumstance where such arrangements cannot be agreed, and with due regard for the importance and urgency of the situation, the Head of Department can request privileged access be granted, Such access will be subject to the University Electronic Mail Policy and limited to the stated need.

email containing personal information comes within the requirements of the Data Protection Act which includes the need for disclosure, on request, to the subject of that information

email credentials can be forged so messages received might not be from the purported sender

messages may be retrievable from backup, even when the sender and recipient have both deleted their copies. However this policy does not require holders of backup material to provide a retrieval service.

Users may not, under any circumstances, monitor, intercept or browse other users' e-mail messages unless authorised to do so.

Network and computer operations personnel, or system administrators, may not monitor or view other users’ e-mail messages other than to the extent that this may occur incidentally in the normal course of their work eg. postmasters may need to inspect messages when dealing with delivery failures. Where they are asked to monitor or view email to investigate an
incident (see second bullet point above) this will require the permission of the Registrar, the Head of Department or the Director of IT Services.

The University reserves the right to access and disclose the contents of a user's e-mail messages, in accordance with its legal and audit obligations, and for legitimate operational purposes. The University reserves the right to demand that encryption keys, where used, be made available so that it is able to fulfil its right of access to a user’s e-mail messages in such circumstances.

Penalties for Improper Use
Failure to comply with this policy may lead to suspension or withdrawal of a user’s email facilities.

Staff
Failure of an employee to comply with this policy may lead to the instigation of disciplinary procedures as contained in the employee’s terms and conditions of employment, and in certain circumstances legal action may be taken. Minor infringements, such as causing inconvenience to other users, may lead to a verbal or written warning. Major infringements, such as major breach of confidentiality, harassment, or illegal activities may lead to a formal warning, suspension or termination of employment. This is not an exhaustive list of possible offences and the University will determine whether a case is minor or major having regard to all the circumstances of each incident.

Students
Failure of a student to comply with this policy may lead to the instigation of disciplinary procedures under Regulation 24 and in certain circumstances legal action may be taken. Minor infringements, such as causing inconvenience to other users, may lead to disciplinary action under the Minor Offences procedure (Regulation 24 Subsection 6 and 7). Major infringements, such as major breach of confidentiality, harassment, or illegal activities may lead to action under the Major Offences procedure (Regulation 24 Subsections 8 and 9). This is not an exhaustive list of possible offences and the University will determine whether a case is minor or major having regard to all the circumstances of each incident.

Contractors
Failure of a contractor to comply with this policy may lead to the cancellation of a contract and in certain circumstances legal action may be taken.