Email Acceptable Use Policy

This Email Acceptable Use Policy (AUP) applies to all University staff (including temporary staff), visitors, contractors, students and researchers of this University and to those any others using the University’s IT resources. This policy should be considered part of the Conditions of Use for Computers and Networks at City University. You should also read the University’s Information Security Policy.

General Principles

Use of email is permitted and encouraged where such use is suitable for business purposes and supports the goals and objectives of the University. Email is to be used in a manner that is consistent with the University’s standards of business conduct and as part of the normal execution of an employee’s job responsibility. [This last sentence is still very much staff-oriented]

- University email accounts are to be used for University business. Limited personal use is considered acceptable.
- The University will directly access email accounts in the pursuit of an appropriately authorised legal or disciplinary investigation.
- Use of email may be subject to monitoring for security and/or network management reasons. Users may also be subject to limitations on their use of such resources
- The distribution of any information through the University’s network is subject to the scrutiny of the University. The University reserves the right to determine the suitability of this information.
- The use of computing resources is subject to UK law and any illegal use will be dealt with appropriately. For example the Police can have a right of access to recorded data in pursuit of a crime.
- Staff Email messages are to be treated as potential corporate messages of the organisation.
- The University reserves the right to redirect the email of staff that have left for legitimate business purposes. Users are responsible for ensuring personal emails are stopped. [Should there be something here about students who have finished their courses? I would expect the university to ‘expire’ many more student accounts than staff accounts every year]

Unacceptable Use or behaviour:

It is unacceptable to:

- Solicit emails that are unrelated to business activities or for personal gain
- Send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person [How can you control what e-mail you receive? Taken at face value this puts me in the wrong if somebody sends me an e-mail that’s offensive to anybody]
- Represent personal opinions as those of the University
- Upload, download or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the University, or the University itself
- Reveal or publicise confidential or proprietary information which includes, but is not limited to financial information, databases and the information contained therein, computer network access codes, patient information and business relationships
- Waste time on non-University business [This seems very general and inappropriate in a document that otherwise is quite specifically about computer/e-mail use]

Users should:

- Keep emails brief and use meaningful subject lines
- Re-read messages before sending to check for clarity and to make sure that they contain nothing which will embarrass the organisation or make it liable
- Understand how to use – and don’t mismanage – CC and BCC: only CC in people that really need to receive the email
- Use file compression techniques for large documents or send then using an alternative method
- Archive effectively – use folders and delete any messages you no longer need
- Don’t overuse the “URGENT” flag as it will lose its value
- Never reply to spam
- Avoid using email for sensitive or emotional messages or offensive content
- Take care in drafting emails, taking into account any form of discrimination, harassment, University representation, and defamation or Data Protection issues.

19th January 2004
• Staff Emails are a form of corporate communication and therefore should be drafted with the same care as letters.
• Users should be careful when replying to emails previously sent to a group.
• Where terminals are left open and logged in when you leave your desk, a malicious user could send messages in your name. Ensure your terminal is locked or logged out.
• Avoid ‘Mail Storms’ – long discussions sent to a distribution list – consider verbal communication.

**Monitoring**

The University accepts that the use of email is an extremely valuable business, research and learning tool. However misuse of such a facility can have a detrimental effect on other users and potentially the University’s public profile. As a result;

• The University maintains the right to access user email accounts in the pursuit of an appropriately authorised investigation
• The specific content of any transactions will not be monitored unless there is a suspicion of improper use [I still think that you need a few words to explain that there is a due process for monitoring e-mails and/or that this must be authorised at a senior level].

We are obliged to monitor to fulfill our responsibilities with regard to UK law and the JANET Code of Conduct.

Action as deemed appropriate by the Director of Computing Services and, if required, other representative such as the Director of HR or School Dean may be taken.

---

**Protect Yourself**

Follow the University’s AUP or risk disciplinary action. The University also retains the right to report any illegal violations to the appropriate authorities.