



Student Email Use Policy (2008)

1 Aims

- 1.1 This policy applies to all students at Canterbury Christ Church University who use the University email system and relates to the proper and effective use of email.
- 1.2 The policy has been developed to help protect the security and integrity of the systems and maintain the reputation of the University. It should be read alongside and in conjunction with the Regulations for the Acceptable Use of University IT.

2 Principles

- 2.1 All students are individually responsible for adhering to this and other policies governing the use of computing services. Students must abide by these rules when using the University email system.
- 2.2 The allocation of computing resources is provided primarily for academic use to support teaching, learning and research.
- 2.3 All electronic communication from the University to students will be to their University email address (*name@canterbury.ac.uk*). Students must check their University email regularly, it is recommended at least weekly during term time.

3 Email Use

- 3.1 Students are prohibited from
 - 3.1.1. Sending any electronic communications whose meaning, transmission or distribution is illegal, unethical, fraudulent, defamatory, harassing or offensive. Material that may be considered inappropriate, offensive or disrespectful to others should not be sent or received as electronic communications using university facilities.
 - 3.1.2. Taking any actions likely to adversely affect the capacity or performance of the email system
 - 3.1.3. Sending unsolicited bulk email messages ("junk mail" or "spam") which is disruptive and generates, or is likely to generate, a significant number of user complaints.
 - 3.1.4. Bulk sending of emails containing attachments.
 - 3.1.5. Forwarding or otherwise propagating chain letters and pyramid schemes, including ostensibly charitable appeals and whether or not the recipient wishes to receive such mailings.
 - 3.1.6. Attempting to conceal their identity when sending electronic mail.
 - 3.1.7. Forwarding or otherwise propagating in bulk unverified information such as hoax virus warnings.
 - 3.1.8. Sending email to any person whom the sender is aware does not wish to receive it.
 - 3.1.9. Harassment, whether through language, frequency, content or size of messages.

- 3.1.10. Malicious email, including "mailbombing" or flooding a user with very large or numerous pieces of email.
 - 3.1.11. Forging of sender information or other concealment of identity with an attempt to deceive.
 - 3.1.12. Sending email for commercial gain, other than relating to a student's employment.
- 3.2 Email resources are limited and an individual student has a quota on the amount of personal disk space. No student may borrow the user-name or resources allocated to someone else.
 - 3.3 If authorisation to use the facilities has been temporarily or permanently withdrawn it is a disciplinary offence to use, or to attempt to gain access to, another user's account.
 - 3.4 Moderate use of e-mail for personal and social purposes is allowed as long as this is reasonable. This is a privilege not a right, and may be withdrawn. Personal use should at no time interfere directly or indirectly with any other person who is trying to work and should be used only in accordance with this policy.
 - 3.5 The University may access information held in a student account in order to investigate a complaint, to investigate a reasonable suspicion of abuse of computer facilities or to cooperate in the investigation of a crime. Otherwise, the University will normally respect the privacy of e-mail messages and data stored on computing systems.
 - 3.6 Emails, archived copies and logs may form part of a record which the University may be required to disclose under civil or criminal law.
 - 3.7 Where email abuse is suspected, accounts will normally be disabled pending an investigation. Under the Regulations, disciplinary action may be taken including denial of access to IT facilities regardless of academic consequences.

Document control/change history				
Version	Author(s)	Date	Circulation	Comments
1	IE	25 Feb. 08	IS policy group	Created from AUP and existing policy pages on web, plus parts from staff policy
2	IE	August 2008		Redraft, slight changes only
3	IE/RM	Sept 08		Final edit and format

Document approval and review	
Approved by:	Information Systems Committee
Date approved:	
Review date:	
Author(s):	Head of Computing Services
Owning Department:	Computing Services