

Email Policy (2013)

1 Aims

- 1.1 This policy and procedure establishes the proper and effective use of email and exists to protect the security of the systems and the reputation of the University.
- 1.2 The policy applies to anyone who uses the University email service.
- 1.3 All Information Technology resources are owned by the University and are provided primarily for academic and business use to support teaching, learning and research.
- 1.4 Users have an individual responsibility to understand their responsibilities under this policy, and to know the rules and abide by them when using the University email service. This policy should be read in conjunction with the other policies and procedures relating to information security, acceptable use, data protection, confidentiality and copyright. These policies, which also apply to the use of email, are available on the website www.canterbury.ac.uk.
- 1.5 Breaches of this policy may result in disciplinary action under the University Disciplinary Procedures or University Regulations for Students.
- 1.6 Use of email should comply with the published Codes of Conduct for staff and students.

2 Good Use of Email

- 2.1 Staff and students should read the Guide to Email Communication which contains advice and help for good practice in the use of email.
- 2.2 Staff must configure suitable signatures to comply with the law (see Appendix A) and such signatures must be applied by staff to email messages destined for outside of the University. Non-work related matter should not be included. The Institution does not support the use of disclaimers in signatures.
- 2.3 All electronic communication from the University to students will be to their University email address (name@canterbury.ac.uk). Students may choose to forward University emails to another account if they so wish.
- 2.4 Staff can choose to forward their University emails to another account. Those staff who regularly receive confidential or personal data should discuss with their manager and get permission first.
- 2.5 Email delivery is not guaranteed. Notifications of delivery failure may not be sent to the originator and read receipt requests can be ignored. Therefore email should not be assumed to be suitable for essential correspondence unless other steps are taken to confirm receipt.
- 2.6 Users are expected to treat electronic information with the same level of confidentiality as they would paper based information. All information should be kept secure, used only for its intended purpose and not disclosed to unauthorised employees or third parties. Any personal data must be

handled in accordance with the University Data Protection Policy which can be found on the University web site.

- 2.7 If email is to be used to communicate confidential or sensitive information then appropriate measures must be taken to ensure authenticity and confidentiality, that the email is correctly addressed and that the recipients are authorised to receive it.
- 2.8 The University blocks considerable volumes of unsolicited email (i.e. SPAM). In order to avoid blocking legitimate email, some SPAM may get through. This should simply be deleted.
- 2.9 The University will never send an email asking you to send your username and password, or other personal details. These are usually attempts to compromise your account and should be deleted.
- 2.10 Electronic messages can easily be archived by other parties and kept and searched over a long period of time. Emails stored electronically by the University are subject to searches and requests under the Data Protection Act 1998 and Freedom of Information Act 2000.
- 2.11 Individual or bulk sending of messages must be done in accordance with English law (especially but not limited to the Data Protection Act). Staff with a requirement for widespread communications to all members of staff, students or other large groups should discuss this with Department of Marketing.
- 2.12 Computing Services may investigate the content of any electronic information when authorised by both a Head of Department and the University Solicitor. Human Resources approval is also required for staff accounts.

3 Unacceptable Email Use

- 3.1 Email, whilst it has benefits for the effective and efficient communication of information, may also have consequences which could potentially impact on the individual and the University. These consequences could represent damage to the reputation of the University, additional costs or fines, and potentially civil or criminal action. It is important therefore that any use of email (whether personal or business) complies with this policy..
- 3.2 Users are specifically prohibited from the following.
 - 3.2.1. 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.
 - 3.2.2. Taking any actions likely to adversely affect the capacity or performance of the email system
 - 3.2.3. 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.
 - 3.2.4. Forwarding or otherwise propagating chain letters and pyramid schemes, including ostensibly charitable appeals and whether or not the recipient wishes to receive such mailings.
 - 3.2.5. Attempting to conceal their identity when sending electronic mail.
 - 3.2.6. Forwarding or otherwise propagating in bulk unverified information such as hoax virus warnings.
 - 3.2.7. Sending email to any person whom the sender is aware does not wish to receive it.
 - 3.2.8. Harassment, whether through language, frequency, content or size of messages.

- 3.2.9. Malicious email, including "mailbombing" or flooding a user with very large or numerous pieces of email.
 - 3.2.10. Forging of sender information or other concealment of identity with an attempt to deceive.
 - 3.2.11. Sending email for commercial gain, other than relating to staff or students looking for employment elsewhere.
 - 3.2.12. Mass emailing or bulk sending of email, unless authorised and in accordance with this policy.
- 3.3 Electronic mail must not be used to communicate confidential or sensitive information unless appropriate measures have been taken to ensure authenticity and confidentiality, that it is correctly addressed and that the recipients are authorised to receive it.
 - 3.4 If authorisation to use email has been temporarily or permanently withdrawn it is a disciplinary offence to use, or to attempt to gain access to, another user's account.
 - 3.5 Email 'disclaimers' have limited or no value and should not be added to any University email.

4 Staff Private Use of Email

- 4.1 Whilst the use of the email service is intended for the effective delivery of our business the University recognises the benefits of allowing staff to use email as a way of developing and maintaining an appropriate work-life balance.
- 4.2 The personal use of email is allowed as long as this is reasonable. Wherever possible the personal use of email should be outside normal working hours, should at no time interfere directly or indirectly with work commitments and should be used only in accordance with this policy.
- 4.3 University email should not be used to enter into any private contract or business relationship. It may however be used to receive acknowledgement only for purchases made from a website.
- 4.4 Failure to use the system in accordance with the guidance or the abuse or misuse of email may result in disciplinary action.

5 Email Retention Guidelines for Staff

- 5.1 There is a natural tendency to hang on to the emails for longer than is necessary 'just in case'. Now that emails are stored in the Cloud, with far higher capacity per person, there is a huge increase in the number of emails that can be kept.
- 5.2 Therefore, there is a need to be proactive in managing emails, especially deleting them after they are no longer needed.
- 5.3 Remember that any email that concerns University business is covered by the Data Protection Act 1998 and the Freedom of Information Act 2000. This means that an email may need to be released if requested.
- 5.4 Emails concerning University business should not be kept for longer than is necessary. The purpose of keeping an email is because it has value as a record. There are administrative, financial and legal, reasons for maintaining a record. You should have a good reason for keeping an email after you have read it and made any response.
- 5.5 Before keeping any email, you might consider these three questions:
 - Could this email help make it clear how a business decision was made?

- Could this email help me explain my actions?
- Could this email form part of a financial, legal, or business audit trail, claim, or obligation?

A 'no' to these three questions indicates that the email unlikely to be needed and can be deleted.

- 5.6 Even if you keep an email because you answered 'yes' to any of these questions, it is important to recognise its value as a record reduces over time. Therefore, older emails should be reviewed periodically. In setting up the structure of your folders, you might think about including a dates for review (which might be months and/or years). There is likely to be no business case for keeping emails for longer than six years after a case has closed, unless you are working in a specialised area where there are statutory retention times. (For further general guidance, please see, Retention and Disposal of Records containing Personal Data. For academic processes, please see Retention Schedule for Documents Relating to Examinations, Validation and Review.)
- 5.7 Remember that a record could be kept elsewhere, and so you do not need to keep the email. If you are sure that the email is retained elsewhere, this is a good reason for deleting it sooner rather than later.

6 Access to your email by others

- 6.1 Your email will not normally be accessed or made available to anyone else. However, this may be done in certain circumstances, either with or without the permission of the individual.
- 6.2 Those who need to give permission for checking and managing their email to a colleague or assistant may do so through the "delegates" facility within Outlook. Having added the appropriate username as a delegate, various levels of permissions can be set for all aspects of Outlook including managing of both calendar functions and sending and checking of email.
- 6.3 In the event of unplanned absence by a member of staff and access is required to information held only by that person, then in the first instance the staff member will be contacted and consent sought.
- 6.4 If consent is not or cannot be obtained, then a business case may be made by the Head of Department to the University Solicitors Office to gain access to specific data in email. If the case is accepted, this will allow an authorised independent third party to search the absent member of staff's email for the specific information required which will then be passed to the Head of Department. Due to the administrative cost of this procedure, genuine business need must be proved.
- 6.5 The privacy of an individual's emails will normally be respected; however there are a number of situations in which access may be made without your knowledge/permission:
- 6.5.1. Where a request is made under the provisions of relevant legislation in relation to the prevention or detection of crime, authorised staff may be requested to make an individual's emails available
 - 6.5.2. At the request of the data owner (the Vice Chancellor) or one of his named representatives
 - 6.5.3. By Systems Administration Staff in connection with the maintenance of the systems
 - 6.5.4. Where an allegation or evidence of breach of the Regulations needs to be investigated, which will be carried out in accordance with the IT Investigation Policy.
- 6.6 Prior to departure, an out-of-office message can be set up on your email to inform people that you are leaving the University and provide an alternative address for contacts. This will allow the sender to re-email to the appropriate address; and will be sent until the email account is deleted. Staff and students retain full access to email for approximately 1 month after their leave date. If one has been

set, then an out-of-office message will be sent for a further 6 months, but email cannot be read or accessed. After this point the account and all email is deleted.

Document control/change history				
Version	Author(s)	Date	Circulation	Comments
1	IE	September 2012		Adapted from existing Staff and Student separate polices
2	IE	October 2012		Edit after comments and added Sec. 5 and App. C
3	IE	May 2013		Sec 2 reduced and new Sec 6 added. Reworded to link to new guide to email
4	IE plus others	May 2013		Edits and corrections
<u>4.1</u>	<u>IE</u>	<u>August 2015</u>		<u>Change only to approval/owner</u>

Document approval and review	
Approved by:	<u>UNDER REVIEW</u>
Date approved:	<u>n/a</u>
Review date:	
Author(s):	<u>Head of Computing Services</u> <u>Head of IT Architecture</u>
Owning Department:	<u>IT Computing Services</u>

Appendix A – Signature guidelines for Staff

A.1 The Companies Act (1985) *requires* the following information to be included on business correspondence :

- Company registration number;
- The company's place of registration (e.g. Scotland or England & Wales); and
- The company's registered office address

A.2 An amendment to the Companies Act that came into effect on 1st January 2007 made it clear the duty that existed for all business letters to include company information now also applied to emails. A recommended email signature for the University is:

```
<full name>  
<job title>, <department>  
Canterbury Christ Church University  
Rochester House, St. Georges Place, Canterbury, Kent, CT1 1UT, England  
Registered Company limited by guarantee (No: 4793659)  
Registered Charity (No: 1098136)
```

Or

```
<full name>  
<job title>, <department>  
Canterbury Christ Church University  
Rowan Williams Court, Universities of Medway Campus  
Registered Company limited by guarantee (No: 4793659)  
Registered Charity (No: 1098136)  
Registered office: Rochester House, Canterbury, Kent, CT1 1UT, England
```

A.3 As staff can legitimately use the University's email system when representing more than one role it is not appropriate to centrally configure the email system to automatically apply such required information to all out going messages

A.4 Staff should create a standard signature based on this guidance and apply it to all email. Most staff will have a single role, and will not need multiple signatures. Staff should try to avoid using long or complex signatures on internal email, as this will save storage space, especially on multiple contributor email discussions.

A.5 Where they have multiple roles, staff must select signatures appropriate to the purpose of the email message, for example the University has several companies. Staff must also remove or delete their standard signature when sending email which is not related to the work for the University.

A.6 Email 'disclaimers' have limited or no value and must not be added as part of any signature.

Appendix B – Multiple User account guidelines for Staff

B.1 It is recognised that in addition to the 'personal' account that each member of staff is entitled to, there is the occasional need for some form of shared email account and/or shared email address. Prior to the current Exchange/Outlook service the requirement was met by way of additional standard email accounts that were referred to as 'Generic accounts', these had a number of flaws.

B.2 There are four aspects of multi-user or shared email use that will be accommodated:

Multi-user aspect:	Example:	Provision:
A role with a single staff occupant	Head of an administrative department	Email alias forwarding to personal account
Many staff acting in a role	An administrative department	Shared email account
Staff group coordination	Collective calendar	Limited access shared email account
One way communication to many staff	All staff	Email mailing list

B.3 Computing Services must act to avoid excessive proliferation of email addresses or accounts, for both technical reasons and in order to maintain a sensible approach to email address books. Computing Services has to account for all IT resources, and establish a life cycle that clearly sets out how the resources come into existence and how they are managed through their use and when they are removed.

B.4 The University owns the 'email address space' – i.e. all addresses @canterbury.ac.uk – it is incumbent on the University to ensure that email addresses are appropriate from the perspective of the whole University and to all users, be they internal or external.

B.5 All multi user or shared email must comply with this policy.

B.6 The University discourages the use of role based email accounts where the role has a singular occupant.

B.6.1. Roles that require a persistent address across changes in occupant should have an email alias that re-directs the email to the current role holder.

B.6.2. Role holders may delegate access to their personal email account to cover absences, or for administrative assistance.

B.6.3. When the role holder leaves post they may extract email addressed to the alias by a simple search, but note that important messages should not be stored in email long term

B.6.4. Existing role-based accounts will be allowed to continue, but their existence may be reviewed at a later date.

B.7 Where there is a role that has many staff operating in it then a shared email account can be provided. Each shared account will have an owner, who is responsible for its use and decides who else is given delegated access.

B.7.1. Those delegated 'full access' (i.e. read, write, delete permissions) must manage the account.

B.7.2. Sub-roles will not justify separate shared accounts but will be catered for by email aliases pointing to the main role. Rules in the shared email account can then pre-process the sub-role email into separate folders.

B.7.3. Staff using the shared account must use their identity when sending email.

- B.7.4. The shared account is not a medium for storage and the account must be actively managed.
- B.8 Where a formal group of staff need sight of a group calendar then a limited shared account can be provided.
 - B.8.1. It is recommended that the number of staff with full (edit) access be kept as few as reasonable. This reduces possibilities for error or mistake.
 - B.8.2. The 'limited shared account' will not allow any email to be sent on its behalf.
- B.9 Where groups of people need to receive email but do not need to work collaboratively on the email, mailing lists should be used.
 - B.9.1. Mailing lists enable the University comply with E-commerce Regulations, such as allowing recipients to withdraw from the mailing list, to know who is on the list and for the list owners to control misuse.
 - B.9.2. Owners of lists must be University staff who have agreed to take active responsibility for the lists they manage.
- B.10 Shared accounts will have quotas as applied to individual accounts. The resources consumed by a shared account will be accounted for by the 'owner'.
- B.11 Shared accounts will only be created for a persistent purpose. Transient requirements will be catered for by means of email aliases forwarding email to either an existing shared account or to a personal account.
- B.12 All shared account identifiers, email aliases and email list addresses must reflect their true nature, be unambiguous, and be appropriate for use across the whole University.
- B.13 Life cycle management:
 - B.13.1. Computing Services will from time to time note the traffic levels of multi-user accounts.
 - B.13.2. Any accounts with no or very little traffic will be candidates for removal.
 - B.13.3. The owners of candidate shared accounts will be consulted prior to any possible deletion. The owners will need to justify the continued existence of the shared account.
- B.14 The procedure for multi-user account creation will be published on Computing Services web site, and must be followed when applying for a multi-user account.
- B.15 All multi-user accounts, email aliases, mailing lists must be arranged prior to any publicity of email addresses. It is not sufficient justification when asking for a particular email address to claim that publicity has already started.
- B.16 Decisions as to relevance, address suitability, etc will be handled by Computing Services. Appeals will be to the Head of Computing Services in the first instance and then to the Strategic Director (Resources), whose decision will be final.

Appendix C – Technical Limits Schedule

- C.1 The University email service is provisioned via the Microsoft Office 365 Cloud service. This provides a robust, resilient email service at little cost to the University.
- C.2 However, by using a Cloud based service, we are subject to various capacity and other limits which we cannot adjust as they are set by Microsoft for everyone. These are usually far higher than anyone will reach. Some other settings can be set, and we have made choices based on our experience of running email systems.
- C.3 The table below shows the limits of the system:

Mailbox Quotas	
Mailbox Quota	250 GB (25,600MB)-[Non-extendable]
Daily warning issued	4924.5 GB (25,088MB)
Stops sending	4924.75 GB (25,344MB)
Stops receiving	5025 GB (25,600MB)
Mailbox Limits	
Message size	25MB Send / 25MB Receive
Attachment size	10MB in Outlook Web App / 25MB in Outlook
Number of attachments	125
Recipients	send to a max. of 100 recipients per message (To, Cc, Bcc)
Message rate	send a maximum of 30 messages per minute
Recipient rate	send to a maximum of 10,000 recipients per day
Retention Limits	
Deleted items folder	items automatically deleted after 30 days
Items moved from deleted items	recoverable for 14 days
Items in junk e-mail folder	items automatically deleted after 30 days