

Policy: Email

Department: ITIS

Date: February 2016

Review Date: 1 year

1.0 Purpose

Email is an important means of communication and it provides an efficient method of conducting much of Goldsmiths' business. This document sets out the policy for the use of email by staff (permanent, temporary or contracted) for teaching, research and administration. By conducting the university's business over email, you are consenting to the terms of use described in this policy.

2.0 Scope

All emails created in the course of business are Goldsmiths' legal property regardless of where the emails are stored. As property of the university, emails are subject to the Freedom of Information Act and the Data Protection Act (including Data Subject Access Requests). These laws apply to information held in private emails and other media formats when they are used to conduct business related to the university.

3.0 General Principles

- Staff must use the university email system to conduct business relating to the university. Private email use is not permitted and will be treated as a breach under the Data Protection Policy.
- Staff must use caution when drafting email containing personal data of other individuals. This information can be accessed by those individuals through a Data Subject Access Request under the Data Protection Act.
- Email should not be used for storage.
- Information needing to reach a large number of staff should be posted on Goldmine or in the appropriate folders on the network drives.
- Email that need to be retained for long period should be copied into a file and stored in a folder on the network drives or as part of record in another system.
- All staff emails must be approved by the Communications team.
- The University reserves the right to redirect the email of staff that have left for legitimate business purposes. Those staff are responsible for ensuring personal emails to that account are stopped before they leave.

4.0 Improper Use

- Emails must not contain inappropriate content including material that is defamatory, libellous, harassing, threatening, discriminatory, offensive or illegal.
- Users cannot solicit emails that are unrelated to business activities or for personal gain.

- Users cannot represent personal opinions as those of the University.
- Email must not be used to upload, download or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the University, or the University itself.
- User cannot 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.
- The email system should not be used for personal purposes.

5.0 Monitoring

- The University maintains the right to access user email accounts in the pursuit of an appropriately authorised investigation.
- We are obliged to monitor email use to fulfil our responsibilities with regard to UK law and the JANET Code of Conduct.
- Use of email is subject to monitoring for security and network management issues. Users will be subject to limitations in their use of such resources.
- The specific content of email will not be monitored unless there is a suspicion of improper use.
- Action as deemed appropriate by the Chief Information Officer and, if required, other representatives may be taken.

6.0 Retention

Once a staff member leaves the university, their access to university email system will be revoked. Emails contained in a staff member's account are held for one month after the individual has left the university. If there is a business need that requires access to the account, the emails may be retained up to 3 months, but not longer.

Emails that have been copied and relocated to files on the network drives or other systems should be retained as long as the records category in the retention schedule to which they relate.

7.0 Associated documents

Please refer to:

- [Data Protection Policy](#)
- [Data Subject Access Requests](#)
- [Freedom of Information Policy](#)
- [ICO's 'Official Information held in Private Email Accounts'](#)
- [Information Security Policy](#)
- [Acceptable Use of IT Policy](#)
- [Acceptable Use of IT Staff Procedures](#)
- [De-Activation for Inappropriate Use of IT](#)
- [Retention Schedule](#)
- [Network- see Terms and Conditions](#)

8.0 Review of policy

This policy will be reviewed at least every year or when there are significant changes to it.

9.0 Contact list for queries related to this policy

Data Protection Officer
Chief Information Officer

10.0 Authority for this policy

Senior Management Team