Goldsmiths
UNIVERSITY OF LONDON

Email Policy

Contents

Ownership	Chief Information Officer
Policy Contact	Information Security Manager
Approval	Information Security Steering Group
Protective Marking	Public
Policy Unique ID	POL0004_email_v2.4
Last review date	September 2023
Next review date	September 2026

1 Introduction

1.1 This policy provides a framework for secure, acceptable, and appropriate use of email. Staff should also refer to the Goldsmiths Information Security site, and Information Security Awareness and Data Protection Training online training. Staff and students are expected to follow this policy, and to be aware of the consequences of inappropriate email use.

1.2 This policy also specifies the actions that the College will take when investigating security incidents and data breaches.

1.3 By using Goldsmiths' email, you are consenting to the terms of use described in this policy.

1.4 The sender of the email must decide whether the content is legal, acceptable, and appropriate.

2 Scope

2.1 This policy applies to all authorised users provisioned with a Goldsmiths email account, including all permanent staff, temporary staff, students, contractors, suppliers, partners and external researchers.

3 Policy statements

3.1 Legal, Policy and Regulatory Requirements

3.1.1 All emails created in the course of business or study are Goldsmiths' legal property, regardless of where the emails are stored. Goldsmiths reserves the right to conduct searches of email accounts in order to comply with its obligations under the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and the Freedom of Information Act.

3.1.2 Staff will lose access to their Goldsmiths email account when they leave Goldsmiths.

3.1.3 Students will lose access to their Goldsmiths email account when they leave Goldsmiths. Students who have left can use an Alumni email if they do not opt out of the Alumni service.

3.1.4 Goldsmiths reserves the right to access the email of staff that have left Goldsmiths, if there is a legitimate business need. Staff are responsible for ensuring that any non-business emails are deleted from their account before leaving.

3.1.5 Emails contained in a staff member's account will usually be retained for three months after an individual has left Goldsmiths. Exceptions to this may be made where there is a business need to retain records that form part of a formal agreement on behalf of the College. Exceptions will be subject to a business case and require sign off by a member of SMT. A record will be kept of all approved exceptions.

3.2 Acceptable use

3.2.1 Goldsmiths' email system is secure but once an email is sent, it is outside our control i.e., we cannot prevent the recipient forwarding the email to another person or party.

3.2.2 Goldsmiths email accounts should only be used for Goldsmiths' business. Users must not use their Goldsmiths email for non-Goldsmith's communications.

3.2.3 Users are not permitted to use their Goldsmiths email accounts to send or receive emails that relate to their own commercial businesses.

3.2.4 Users must not use an installed email application e.g. Outlook on a Goldsmiths' device to download and access their non-Goldsmiths email accounts.

3.2.5 Bulk emails may not be sent to all staff or students without prior approval from the Communications, Marketing and Recruitment Team.

3.2.6 Emails must not contain material that is defamatory, libellous, bullying, harassing, threatening, discriminatory, offensive, illegal or obscene.

3.2.7 Users must not deliberately send anonymous or forged messages.

3.2.8 If Protected or Restricted data must be shared by email then it must be sent as an encrypted attachment, as advised by IT&DS. The encryption key must be sent using means other than email.

3.2.9 Users must not send emails for the transmission of unsolicited commercial or advertising material, chain letters or other junk mail of any kind.

3.2.10 Users must take all reasonable steps to prevent the transmission of computer viruses through file attachments by using antivirus software on any device they use to access emails.

3.2.11 Users must not open suspicious file attachments or links from any source, being especially cautious where the origin is unknown or unsolicited.

3.2.12 Users must report any suspected phishing emails to phishing@gold.ac.uk to help protect the College from such attacks.

3.2.13 Users must not use email to upload, download or otherwise transmit commercial software or any copyrighted materials belonging to parties inside or outside of Goldsmiths.

3.2.14 Automatically forwarding all Goldsmiths emails by staff to personal email accounts is not permitted and will be treated as a potential data breach.

3.3 Appropriate use

3.3.1 Information intended to reach a large number of staff or students, should be posted on the Goldsmiths website, Goldmine or alternative communication methods as opposed to an email.

3.3.2 Users should avoid sending attachments and instead send links to Goldsmiths recommended file storage.

3.3.3 Attachments received that need to be retained and edited should be saved to recommended Goldsmiths' file storage.

3.3.4 Users should be aware that sending a Goldsmiths email, may be interpreted as the opinions of the College.

3.3.5 Users should ensure a brief and descriptive subject line is in every email.

3.3.6 Staff should create an email signature which includes their name, job title, department, and phone number.

3.3.7 Staff should be mindful that emails created that contain personal data of other individuals, can be accessed by those individuals through a Data Subject Access Request under the Data Protection Act 2018 and GDPR.

3.3.8 Staff should be mindful that all emails relating to the business of the College may be disclosable under the Freedom of Information Act 2000.

3.4 Investigations

3.4.1 Goldsmiths may investigate any suspected security incidents, complaints or suspected non-compliance with this policy.

3.4.2 Goldsmiths maintains the right to access user email accounts to perform senior management authorised investigations and record evidence.

3.4.3 Goldsmiths complies with the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 to intercept communications.

3.4.4 Where there is evidence of a criminal offence, the issue will be reported to the police. Goldsmiths will fully cooperate with the police and other appropriate external agencies in the investigation of alleged offences.

3.4.5 Users must be aware that once a Data Subject Access Request for information has been received by Governance and Legal Services it is a criminal offence to intentionally delete information or documents to prevent their disclosure.

3.4.6 Goldsmiths maintains the right to monitor emails sent from Goldsmiths accounts to prevent potential data breaches of Restricted/Protected classified data for data loss prevention.

4 Sanctions

4.1 Failure to comply with this policy may result in withdrawal of access to Goldsmiths IT services and may result in staff or student disciplinary action, termination of contract or legal action.

5 Monitoring

5.1 This policy and its implementation will be subject to internal monitoring and auditing, and the outcomes from these processes will inform and improve practices as part of a commitment to continual improvement.

6 Exceptions

6.1 If an individual or third party cannot comply with this policy, they must contact IT&DS Service Support for advice on security controls to enable compliance otherwise they must cease using Goldsmiths IT services. Staff who may not be able to comply for research purposes should contact line managers, supervisors and IT&DS Information Security or Governance and Legal Services representative before sending material.

7 Definitions

- GDPR: General Data Protection Regulation
- JANET: Is a high-speed network for the UK research and education
- Jisc: A UK not-for-profit company whose role is to support post-16 and higher education, and research.

8 Related documents

- Data Breach and Information Security Incident Reporting Procedure
- Protective Marking Policy (Data Classification)
- Information Security Policy

- Acceptable use of IT Services Policy

9 Related requirements

- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBPR)
- Data Protection Act 2018
- Freedom of Information Policy
- Data Protection Policy
- Retention Schedule
- Records Management Policy
- IT Services Regulations for Students
- JANET Acceptable Use Policy
- Information commissioner's office: GDPR guidance

10 Review plan

10.1 This policy shall be updated regularly to remain current in the light of any relevant changes to any applicable law, Goldsmiths' policies or contractual obligations and reviewed by the Information Security Steering Group (ISSG) at least every three years. Minor reviews of this policy will be undertaken by the Information Security Manager as required and will be approved by the ISSG.

11 Revision history

Version	Date	Details	Author	Approved
1.0	01/02/16	Submitted to SMT	David Swayne	Approved
2.0	25/09/19	Submitted to ISSG	Peter Hircock	Approved with minor amendments
2.0	11/11/19	Submitted to E&IC	Peter Hircock	Noted
2.1	17/12/19	Submitted to IT SMT	Peter Hircock	Minor correction to 3.2.1
2.2	28/01/20	Submitted to IT SMT	Peter Hircock	Minor amendment to section 3.2.1
2.3	01/09/21	Re submitted to ISSG	Peter Hircock	Approved in two yearly review

Version	Date	Details	Author	Approved
2.4	20/09/23	Re submitted to ISSG	Peter Hircock	Approved with deletions and rewriting of 3.2.3