

Email Policy

Contents

1	Introduction	2
2	Scope	2
3	Policy statements.....	2
3.1	Legal, Policy and Regulatory Requirements	2
3.2	Acceptable use	3
3.3	Appropriate use	4
3.4	Investigations.....	5
4	Sanctions.....	5
5	Monitoring	5
6	Exceptions.....	6
7	Definitions	6
8	Related documents	6
9	Related requirements.....	6

Ownership	Chief Information Officer
Policy Contact	Information Security Manager
Approval	Information Security Steering Group
Protective Marking	Public
Policy Unique ID	POL0004_email_v2.3
Last review date	September 2021
Next review date	September 2023

1 Introduction

- 1.1 This policy provides guidance on secure, acceptable and appropriate use of email. Staff can also refer to the Goldsmiths Information Security site, and “Information security awareness 2020” and “Data Protection Training” computer based course’s. Staff and students are expected to follow this policy, and to be aware of the consequences of inappropriate email use.
 - 1.2 The sender of the email must decide whether the content is legal, acceptable and appropriate.
 - 1.3 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.
 - 1.4 This policy also specifies the actions that the University will take when investigating security incidents and data breaches.
 - 1.5 By using Goldsmiths’ email, you are consenting to the terms of use described in this policy.
-

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 and students will lose access to their Goldsmiths email account when they leave Goldsmiths. Former students can access Alumni services from the Alumni website.

- 3.1.3 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.
- 3.1.4 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 University. 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 Users must only use their Goldsmiths email accounts to conduct Goldsmiths business (that is to send or receive work-related emails). Users are not permitted to send or receive emails relating to Goldsmiths business from their personal private email accounts. Emails relating to Goldsmiths business must only be sent or received through Goldsmiths email accounts.
- 3.2.2 Users are not permitted to use their Goldsmiths email accounts to send or receive emails that relate to their own commercial businesses.
- 3.2.3 Using Goldsmiths email accounts to send or receive personal non-commercial emails that do not relate to Goldsmiths business is not advisable. However, it is recognised that this may be necessary in certain limited circumstances, such as:
- personal childcare responsibilities;
 - dependents who are ill or the individuals own health; and
 - responding to urgent exceptional situations.

- 3.2.4 Bulk emails may not be sent to all staff or students without prior approval from the Communications Team.
- 3.2.5 Emails must not contain material that is defamatory, libellous, bullying, harassing, threatening, discriminatory, offensive, illegal or obscene.
- 3.2.6 Users must not deliberately send anonymous or forged messages.
- 3.2.7 Users must not reveal or publicise Protected or Restricted data i.e. confidential data.
- 3.2.8 If Protected or Restricted data must be sent as an attachment, then it must be encrypted or password protected, as advised by IT&IS. The encryption key or password 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 University 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 University.
- 3.3.5 Users should ensure a brief and descriptive subject line is in every email.

- 3.3.6 Staff should follow the Communications Dept signature guidance on Goldmine and create and use an email signature which include 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 University 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 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 the IT&IS Service Desk 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& IS Information Security or Governance and Legal 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](#)
-

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](#)
- Goldsmiths Academic Manual: [IT Services Regulations](#)
- [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 at least every two years. Minor reviews of this policy will be undertaken by the Information Security Manager annually or more frequently 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