Goldsmiths
UNIVERSITY OF LONDON

Acceptable Use of IT Services Policy

Contents

Ownership	Chief Information Officer
Policy contact	Information Security Manager
Approval	Information security Steering Group
Protective Marking	Public
Policy Unique ID	POL0005_accep_use_v2.1
Last review date	December 2021
Next review date	December 2023

1 Introduction

1.1 Goldsmiths' IT services are provided to all users to enable them to conduct learning, teaching, research, approved business activities or College related pursuits.

1.2 This policy outlines what is acceptable and where relevant, what is unacceptable, when using the Goldsmiths or College partners' IT services.

1.3 This policy also details the sanctions for non-compliance with this policy. Contact the IT Service Desk to report instances of non-compliance with this policy and to request advice on compliance.

1.4 This policy complies with the JANET Acceptable Use Policy.

1.5 Where specific constraints on the use of Goldsmiths' IT services have been communicated by the College, the more restrictive constraints apply.

1.6 Every user of Goldsmiths' IT services must ensure that their use is acceptable, and they are accountable for all actions undertaken using their College IT credentials.

1.7 By using the Goldsmiths or College partners' IT services you are consenting to the terms of use as described in this policy, and to abide by all other relevant Goldsmiths policies. This policy should be read in conjunction with the Email Policy, Information Security Policy and Remote Working Policy.

2 Scope

2.1 This policy applies to all users of Goldsmiths IT services, whether the IT service is located on the College campus or hosted by third parties, whether the service is accessed on campus or remotely and identifies specific responsibilities of staff, students and third parties where appropriate.

2.2 Goldsmiths' IT services include, but are not restricted to:

2.2.1 Network infrastructure, including physical Infrastructure whether cable or wireless, firewalls, switches and routers.

2.2.2 Network services, including Internet access, web services, email, wireless, messaging, network storage, telephony, CCTV, door and access control.

2.2.3 Computing hardware, both fixed and portable, including workstations, laptops, tablets, mobile devices, smart phones, servers, printers, scanners, disk drives, monitors, keyboards and pointing devices.

2.2.4 Software and databases, including applications, web applications, SaaS and 3rd party hosted services, virtual learning environments, video conferencing, software tools, e-library services, electronic journals and eBooks.

2.2.5 Collaborative IT services provided by Goldsmiths.

2.2.6 Goldsmiths' data of all types (whatever format) created by or on behalf of the College by staff, deemed as College property.

3 Policy Statement

3.1 Unacceptable use of Goldsmiths' IT services

3.1.1 Using Goldsmiths IT services to create, download, store, transmit, share or display any unlawful material, or material that is indecent, offensive, defamatory, threatening or extremist.

3.1.2 Using Goldsmiths IT services to unlawfully discriminate, or to encourage unlawful discrimination, on the grounds of age, disability, sex, gender reassignment, pregnancy, maternity, race (which includes colour, nationality, ethnic or national origins), sexual orientation, religion and belief or because someone is married or in a civil partnership. All unlawful activity carried out, on, or through the use of College IT services is unacceptable: the police will be informed where there is any evidence of such activity.

3.1.3 Using Goldsmiths IT services to harass, bully, abuse, libel or cause needless anxiety.

3.1.4 Using Goldsmiths IT services to corrupt or destroy any users' data or to violate their privacy.

3.1.5 Unauthorised access of the network, restricted areas of the network or IT systems, or assisting the unauthorized access, or not reporting any known unauthorised access to the IT Service Desk.

3.1.6 Unauthorised disclosure of Goldsmiths' data that is classified as Protected or Restricted (i.e. sensitive or confidential information) that is obtained from, or disseminated through use of, College IT services.

3.1.7 Unauthorised creation and maintenance of local IT systems that process sensitive data that is stored on Goldsmiths IT systems.

3.1.8 Using College IT services to access and use personal data in breach of Goldsmiths' policies and the Data Protection Act 2018.

3.1.9 Storing Goldsmiths' data in locations and services that have not been approved by the College. This includes any unauthorised personal storage, cloud storage, and SaaS services.

3.1.10 Using Goldsmiths IT services to deny services to other users. For example, by overloading network capacity and not following cease and desist instruction from IT&IS SMT.

3.1.11 Deliberately wasting Goldsmiths IT services resources or the time of other users of College IT services.

3.1.12 Bulk emails of any format may not be sent to large numbers of recipients without prior approval from the Communications Team.

3.1.13 Unauthorised anonymous internet browsing.

3.1.14 Using Goldsmiths IT services to create, download, use, transmit, disseminate, share and/or display material, including software, which is subject to copyright without appropriate permission(s).

3.1.15 Connecting devices to the Goldsmiths wired network that are not owned, leased, hired or otherwise provided by Goldsmiths. Devices attached without permission will be blocked and investigated by IT&IS.

3.1.16 Connecting privately owned devices to the wireless network or halls of residence networks that do not meet Goldsmiths' policies.

3.1.17 Knowingly participating in any form of denial of service attack.

3.1.18 Unauthorised use of vulnerability, packet-sniffing or port scanning software.

3.1.19 Installing and using software on Goldsmiths IT services that is not compliant with College policies or explicitly prohibited by the College.

3.1.20 Introducing malware, crypto mining software, password detection software, and other malicious or unwanted programs.

3.1.21 Unauthorised tampering with Goldsmiths' IT equipment.

3.1.22 Using Goldsmiths IT services to undertake actions which undermine the security controls, policies or procedures which have been implemented to protect IT systems and data; for example, by sharing passwords or uninstalling antivirus software.

3.1.23 Not reporting the loss of Goldsmiths' IT equipment to the IT Service Desk or loss of personal data to the Data Protection Officer.

3.1.24 Transmitting communications containing commercial or promotional material which do not allow recipients to opt-out of receiving such communications.

3.1.25 Disguising, or attempting to disguise, the identity of the sender/origin of an electronic communication.

3.1.26 Using Goldsmiths IT services to misrepresent any views and/or opinions held personally by the user as the views and/or opinions of the College, unless the user is explicitly authorised to do so.

3.2 Statutory Duties

3.2.1 Goldsmiths has a range of statutory duties including Prevent, Safe-guarding and others. Any behaviour that causes concern will be reported to the appropriate authority.

3.3 Personal Use of Goldsmiths IT Services

3.3.1 Personal use of Goldsmiths IT services by staff is acceptable provided this does not interfere with their duties or the availability of IT services.

3.3.2 Personal use of Goldsmiths IT services by students (i.e. use not related to a student's studies or college-related activities) is acceptable, provided this does not interfere, either by its timing or extent, with the availability of College IT services to other users for learning, teaching, research or administrative purposes.

3.3.3 Goldsmiths provides no guarantees regarding the privacy or safety of any personal use of College IT services. Goldsmiths has no liability for any personal loss or damage suffered by a member of staff through personal use of College IT services, for example the theft of credit card data used online.

3.3.4 Storing of personally owned files on Goldsmiths IT services such as eBooks, music, videos or photography is not permitted. Storage of any other personally owned files must not be excessive, infringe copyright or data protection legislation. As Goldsmiths is not a data controller in respect of such data it holds no obligations in relation to it under data protection law.

3.4 Investigations

3.4.1 No member of Goldsmiths staff is permitted to routinely monitor an individual's use of College IT services. However, IT&IS SMT may grant permission for the monitoring or investigation of an individual's use of College IT services in the following cases:

- Where there are reasonable grounds to suspect unacceptable use of College IT services.
- To detect potential IT service problems.
- To investigate security incidents.
- Upon receipt of a Data Subject Access Request.
- Where a legitimate request is made by the police or other authority.

3.4.2 Goldsmiths reserves the right to routinely monitor, scan or otherwise probe College IT services, systems and networks to identify unacceptable use.

3.4.3 Any monitoring will take place within the terms permitted under the Regulation of Investigatory Powers Act (RIP) 2000 and The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000).

3.4.4 There may be other circumstances requiring in-depth temporary monitoring, for example where a member of staff is suspected of excessive use of IT services. Goldsmiths reserves the right to:

- Monitor the nature, volume and content of communications where the member of staff is representing the College, or the College is the subject of the communications.
- Monitor internet usage where it is un-related to a staff member's job role.
- Trace extensive and repeated telephone calls by staff to irregular destinations and in extreme cases record calls, where reasonable grounds exist to suspect serious misconduct.

4 Sanctions

4.1 Compliance with this policy is mandatory and non-compliance must be reported to the IT Service Desk, who will record and escalate to the appropriate authority.

4.2 Failure to comply with this policy may result in withdrawal of access to Goldsmiths IT services.

4.3 Staff should note that non-compliance of this policy may be treated as misconduct under Goldsmith's relevant disciplinary procedures and could lead to disciplinary or other actions. Serious breaches of this policy may constitute gross misconduct and lead to disciplinary action, termination of contract or summary dismissal. For extreme cases, in contravention any applicable laws, non-compliance may also be reported to the appropriate external authorities.

4.4 Students should note that non-compliance of this policy may be treated as misconduct under Goldsmiths' relevant disciplinary procedures and could lead to disciplinary action or other actions, such as removal of access to Goldsmiths' IT services and/or fines. For extreme cases, in contravention of any applicable law, non-compliance may also be reported to the appropriate external authorities.

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. Heads of Department and Directors of Services are responsible for ensuring that all users are made aware of and act in accordance with this policy.

6 Exceptions

6.1 If an individual or third party cannot comply with this policy, they must cease using Goldsmiths' IT services.

6.2 If you need to use Goldsmiths' IT services for what would be considered unacceptable use under this policy (such as lawful research into e.g. racist or offensive material), you must seek the prior written permission of IT&IS SMT.

7 Definitions

- GDPR: General Data Protection Regulation
- CCTV: Closed circuit television
- JANET: Is a high-speed network for the UK research and education community provided by Jisc
- Jisc: A UK not-for-profit company whose role is to support post-16 and higher education, and research.
- SaaS: Software as a service
- ISSG: Information Security Steering Group

8 Related Documents

- Protective Marking Policy (Data Classification)
- Information Security Policy
- Email Policy
- JANET Acceptable Use Policy
- Remote Working Policy

9 Related Requirements

- Data Breach Procedure
- Data Protection Act 2018
- Data Protection Policy
- Goldsmiths Academic Manual - IT Services regulations
- Information commissioner's office - GDPR guidance
- Malicious Communications Act 1988
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000
- Investigatory Powers Act 2016
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Communications Act 2003
- Counter-Terrorism and Security Act (2015)
- JANET Security Policy
- Copyright (Computer Programs) Regulations 1992
- Goldsmiths Safeguarding Policy

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	01/06/15	Reviewed by SMT	David Swayne	SMT
2.0	04/12/19	Reviewed by ISSG	Peter Hircock	ISSG
2.1	01/12/21	Reviewed by ISSG	Peter Hircock	ISSG