Goldsmiths
UNIVERSITY OF LONDON

IT Services Regulations

Contents

Ownership	Associate Director IT Service Strategy and Planning
Approval	Academic Board
Last review date	June 2019
Next review date	May 2020

1 Introduction

1.1 The aim of these regulations is to help ensure that Goldsmiths' IT services are used safely, lawfully and equitably. The issues covered by these regulations are complex and you are strongly urged to read the Information Security Policy and individual policies referred to, which gives more detailed information.

2 Intended use

2.1 The IT services are provided for use in furtherance of the mission of Goldsmiths, for example to support a programme of study, research or in connection with your employment by the institution. Use of these services for personal activities (provided that it does not infringe any of the regulations, policies and does not interfere with others' valid use) is permitted, but this is a privilege that may be withdrawn at any point. Use of these IT services for non-university commercial purposes is prohibited.

2.2 You must abide by the regulations applicable to any other organisation whose services you access such as Janet and Jisc. When using Eduroam at another institution, you are subject to both the regulations of Goldsmiths and the institution where you are accessing services.

2.3 Some software licences procured by Goldsmiths will set out obligations for the user – these must be adhered to. For example, certain licences only permit use for academic purposes.

3 Information Security

3.1 You must take all reasonable precautions to safeguard any IT credentials issued to you. For example, a username and password, email address, ID card or other identity hardware.

3.2 All passwords must comply with the Goldsmiths Password Policy. You must not allow anyone else to use your IT credentials. Nobody has the authority to ask you for your password and you must not disclose it to anyone.

3.3 Do not use your Goldsmiths campus password for any other system.

3.4 You must not attempt to obtain, use or share anyone else's IT credentials.

3.5 If you handle personal, confidential or sensitive information, you must take all reasonable steps to safeguard it, particularly with regard to removable media, mobile and privately owned devices. For example, password protection, encryption and data storage in accordance with Goldsmiths' Data Protection and Information Security policies.

3.6 All personal equipment connecting to Goldsmiths IT services must have anti-virus software installed and utilise an operating system actively receiving security updates, if available.

3.7 In order to ensure that your data is recoverable in the event of a security incident, you must use a Goldsmiths recommended storage location.

4 Conduct

4.1 You must not do anything to jeopardise the integrity of the IT services, for example, doing any of the following:

- Deliberately or recklessly introducing malware or viruses;
- Attempting to disrupt or circumvent IT security measures;
- Damaging, reconfiguring or moving equipment;
- Setting up servers or services on the network other than in approved circumstances;
- Utilise any software for monitoring or scanning devices on the Goldsmiths network;
- Installing software on Goldsmiths' equipment other than in approved circumstances;
- Reconfiguring or connecting equipment to the network other than by approved methods.

4.2 You must not do anything to jeopardise the IT services in a way that interferes with others' valid use of them, for example, by doing any of the following:

- Infringe copyright, download copyrighted material or break the terms of licences for software;
- Attempt to access, delete, modify or disclose information belonging to other people without their permission;
- Corrupt or destroy information belonging to other people;
- Access any IT system that you are not authorised to use;
- Create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening or discriminatory;
- Deliberately or recklessly consume excessive IT resources such as processing power, bandwidth or consumables. See Appropriate Use of IT Policy;
- Send unsolicited bulk email. See the Email Policy;

- Cause needless offence, concern or annoyance to others.

5 Sanctions

5.1 Infringing these regulations may result in sanctions under the Student Disciplinary Policy. Penalties may include withdrawal of services and/or fines.

5.2 Information about infringement may be passed to appropriate law enforcement agencies, and any other organisations whose regulations you have breached.

5.3 You must inform the Service Desk:

- If you become aware of any infringement of these regulations by any person;
- If you become aware of any security concern, and follow the advice provided;
- If you require clarification or advice.

6 Monitoring

6.1 Goldsmiths monitors and records the use of its IT services for the purposes of:

- The effective and efficient planning and operation of the IT facilities;
- Detection and prevention of infringement of these regulations;
- Investigation of alleged misconduct.

6.2 Goldsmiths will comply with lawful requests for information from government and law enforcement agencies.

7 Definitions

7.1 Janet is a high-speed network for the UK research and education community provided by Jisc.

7.2 Jisc (formerly the Joint Information Systems Committee) is a UK not-for-profit company whose role is to support post-16 and higher education, and research, by providing relevant and useful advice, digital resources, network and technology services, including researching and developing new technologies and ways of working. It is funded by a combination of the UK further and higher education funding bodies, and individual higher education institutions.

7.3 Eduroam is an international roaming service for users in research, higher education and further education. It provides researchers, teachers, and students easy and secure network access when visiting an institution other than their own.

8 Policies referred to

- Password Policy
- Data Protection Policy
- Information Security Policy
- Appropriate Use of IT Policy
- Email Policy