Goldsmiths
UNIVERSITY OF LONDON

Goldsmiths

University of London

Information Security Steering Group

Microsoft Teams Policy for Teaching and Learning

Contents

Ownership	IT&DS
Policy Contact	Associate Director of Digital Technologies
Approval	Information Security Working Group
Protective Marking	Public
Policy Unique ID	POL0005_Teams
Last review date	06 Nov 2023
Next review date	March 2026

1 Introduction

1.1 This policy states the acceptable use of Microsoft Teams for Teaching and Learning, and it should be read in conjunction with the Information Security Policy and other related documents included in this policy. Staff and students can also refer to the guidance produced by TaLIC on how to use Teams for Teaching and Learning purposes.

2 Scope

2.1 This policy applies to all authorised users, staff, students and external guests provisioned with access to a Goldsmiths Microsoft Teams for the purpose of Teaching and Learning.

3 Policy statements

3.1 Legal, Policy and Regulatory Requirements

3.1.1 All content created in the course of business or study are Goldsmiths' legal property, regardless of where the Teams messages or other contents are stored. Goldsmiths reserves the right to conduct searches of Microsoft Teams 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 Teams linked to a teaching module will be set to expire after 2 years and 3 months from the Academic start date. After such period Teams will be fully deleted, including Teams messages and any other content.

3.1.3 Other Teams created for project activities as part of the Teaching and Learning will be retained for the specific time requested.

3.1.4 The content of private chats (1:1 or 1: many chats) older than 3 months will be deleted automatically from Teams as per organisational retention policy.

3.1.5 Staff and students will lose access to their Goldsmiths Teams when they leave Goldsmiths.

3.2 Acceptable use

3.2.1 Users must use Goldsmiths Teams linked to a teaching module only for purposes related to Teacrecorhing. Other types of Teams must be used for activities outside teaching.

3.2.2 External guests' access to Teams must be given by Team Owners and in line with the Information Security Policy.

3.2.3 Users must not forward or copy and share a Microsoft Teams meeting link to anonymous users (users who do not have a Goldsmiths IT account, or guests invited in a team) without the permission of the meeting organiser.

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

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

3.2.6 Staff and Students should be aware that recording in Microsoft Teams should only be used for business-related purposes and with the consent of all parties involved

3.2.7 Staff and students should be mindful that messages created in Teams 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.

3.2.8 Staff and students should be mindful that all Teams messages and other content relating to the business of the University may be disclosable under the Freedom of Information Act 2000 and Data Protection Act 2018.

3.2.9 Staff and students should be aware that some technical controls have been put in place for staff and students to comply with the appropriate usage of Teams for Teaching and Learning at Goldsmiths.

3.2.10 Staff and students should ensure that best practice is followed as provided by guidance produced by TaLIC for the use of Teams for Teaching and Learning in instances where features have been enabled for use.

3.3 Investigations

3.3.1 Goldsmiths may investigate any suspected security incidents, complaints or suspected non-compliance with this policy in line with the Information Security Policy

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.

4.2 Staff and students that continue to transgress guidance on Teams for Teaching and Learning usage which can cause disruption to others will have additional technical controls applied at a user level which can prevent them from using the full features of Teams.

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.

7 Definitions

- GDPR: General Data Protection Regulation

8 Related documents

- Digital Recording of 'Live' Educational Activities Policy
- 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

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 two years. Minor reviews of this policy will be undertaken by the Head of Data Management and Integration annually or more frequently as required by consulting with the Business Service Owners Group (BSOG) and getting final approval by ISSG

11 Revision history

Version	Date	Details	Author	Approved
V.1	23 April 2021	Approved version from ISSG	Alma Shala	ISSG
V.2	24 March 2023	Version history updated	Alma Shala	ISSG
V.2.1	6 Nov 2024	Included recording practices in the AUP	Alma Shala	