April 2020

Director of information technology

Version Live 1.1

Microsoft Teams Policy

ITPOL10

Academic excellence for
business and the professions

Uncontrolled Copy when printed

Contents

Uncontrolled Copy when printed

1 Overview

This policy is provided to give authoritative information on the use of Microsoft Team sites including on the applicability and use of the product's sharing capabilities within and outside of the University.

2 Scope and Applicability

This policy applies to staff, students, alumni, contractors, consultants, temporary and visiting staff, including interns, retired staff, honorary staff, volunteers and other workers of the University, including all personnel affiliated with third parties who interact with the information held by the University in all its forms and its related information systems. This includes, but is not limited to, any systems or data attached to the University computer or telephony networks, systems supplied by the University or communications set to or from the University.

This policy applies to all people and assets in the execution of the original and supplemental University Charters pertaining to IT. This policy is reviewed, maintained and updated by the Information Security Manager. This policy will be reviewed, at minimum, annually.

3 Normative Reference

3.1 This document forms part of an ISO/IEC27001 aligned ISMS.

3.2 IT Acceptable Use Policy.

3.3 IT Email Policy.

3.4 IT Security Policy.

3.5 Conditions of Use Policy.

3.6 Data Protection Policy.

4 Terms and Definitions

4.1 For the purpose of this document, the terms and conditions given in ISO/IEC 27001 apply.

4.2 Standard IT terminology is used.

5 General Policy – Microsoft Teams

5.1 Team naming standards

To appropriately manage Teams appropriate naming standards should be used and maintained. This will avoid confusion when you are part of many Team groups. Managers of Teams which are not appropriately named will be contacted and asked to name them appropriately.

Team names must be descriptive and will be prefixed with the abbreviated University name, followed by the department, followed by an identifier ST for staff, SU for students, concluding with a relevant name for the team.

As an example, for a computer science staff team wishing to collaborate cyber security.

CUoL-SMCSE-ST-Cyber Security *(created for staff use)*

CUoL-SMCSE-SU-Cyber Security *(created for student use)*

5.1.1 Student Team Sites

Student Team sites may only be created by a staff member who will sponsor and retain overall responsibility of the site.

5.2 Offensive and inappropriate Team names

Offensive or inappropriate names will not be tolerated. Any Team found to be named with offensive or inappropriate naming will be deleted and the creator of the team will render themselves liable to action under section 7 of this document.

5.3 Creating the Team

There are four types of Team provided. When creating your Team, choose the type which most accurately reflects the purpose of the Team. Refer to the use-cases in section 5.4 as different classes of service will apply to each.

Please note: the retention periods for each of the four Team types is under review and will change.

Although there are two options for Team privacy, it is strongly recommended that the default option **Private Team** is used. Public Teams may be used but are not considered to be as secure as Private Teams. In the rare situation where a Global Team is required contact your BRM for assistance.

Each Team must have two Team owners, with a minimum of one staff owner. Section 5.7 provides further information.

Teams without owners will be deleted.

5.4 Use-cases of Teams

The use of Teams is being supported using four use-cases, dependent upon the purpose of the Team. When creating a Team four choices will be offered for selection.

These are:

- Class
- Professional Learning Community (PLC)
- Staff
- Other

At this time these four use-cases will feature exactly the same retention periods; this will change retrospectively once the proposed retention periods are agreed by senior management. To obtain the longest retention periods once the retention periods are ratified select either PLC or Staff use-cases.

5.4.1 Short-term Teams provided for a specific purpose

For example:

- Training sessions for trainees, not students in SITS.
- Alumni being invited to participate in a University activity.
- Careers events with guests from industry.

If creating a Short -Term Team use the selector button for either Class, PLC or Other. Manually delete the Team when it is no longer required.

Team technical processes will automatically email the Team owner every 180 days requesting they renew their group. If no approval is received the Team site will timeout and delete. Once deleted there is no possible recovery for the Team.

Should the Team continue to be used note that Team chat messages will persist indefinitely until the Team is deleted.

Short-term Teams will be permitted to share files and information with external guests. Although it is possible to connect a guest without a Microsoft account certain features of the Team will not be available to non-Microsoft authenticated Guests, this is a designed feature of the product and cannot be altered by City IT. It is therefore recommended for fuller functionality Guests use a Microsoft account and email. Team owners should ensure Guests have adequate security in place on their systems, as a recommended minimum; antivirus software and password protection. It is recommended that Guests should only edit and view files on the Teams or OneDrive environment and do not download files to their computer unless absolutely necessary and only with the explicit consent of the Team owner.

5.4.2 Teams created for Teaching purposes

For example:

- Training and teaching sessions for students registered in SITS.

Uncontrolled Copy when printed

- Students or external persons being invited to participate in a University activity.

If creating a Teaching Team use the selector button for either PLC or Class.

Team technical processes will automatically email the Team owner every 180 days requesting they renew their group. If no approval is received the Team site will timeout and delete. Once deleted there is no possible recovery for the Team.

Should the Team continue to be used note that Team chat messages will persist indefinitely until the Team is deleted.

Teaching Teams will be permitted to share files and information with external Guests. Although it is possible to connect a guest without a Microsoft account certain features of the Team will not be available to non-Microsoft authenticated Guests, this is a designed feature of the product and cannot be altered by City IT. It is therefore recommended for fuller functionality Guests use a Microsoft account and email. Team owners should ensure Guests have adequate security in place on their systems, as a minimum antivirus software and password protection. It is recommended Guests should only edit and view files on the Teams or OneDrive environment and do not download files to their computer unless absolutely necessary and only with the explicit consent of the Team owner.

5.4.3 Business-as-usual Data Sharing and Collaboration

For example:

- School Partnerships and College Partnerships sharing plans for collaboration.
- Events Partners – planning events such as graduation and recruitment fairs.
- Media Opportunities i.e. working with TV and radio, sharing knowledge for promotion.
- Enterprise Activities sharing business and project plans
- Member of a research activity sharing (non-sensitive or personal) data.
- Meeting with an external such as a supplier, or consultant, where documents need to be shared and discussed.
- Mentoring scheme - providing action plans and notes from working groups.

If creating a BAU or Data Sharing / Collaboration Team use the selector button for either Class or PLC. Manually delete the Team when it is no longer required.

Team technical processes will automatically email the Team owner every 180 days requesting they renew their group. If no approval is received the Team site will timeout and delete. Once deleted there is no possible recovery for the Team.

Should the Team continue to be used Team chat messages will persist indefinitely until the Team is deleted.

Data Sharing and Collaboration Teams will be permitted to share files and information with external guests. Although it is possible to connect a guest without a Microsoft account certain features of the Team will not be available to non-Microsoft authenticated Guests, this is a designed feature of the product and cannot be altered by City IT. It is therefore recommended for fuller functionality Guests use a Microsoft account and email. Team owners should ensure Guests have adequate security in place on their systems, as a minimum antivirus software and password protection. It is recommended Guests should only edit and view files on the Teams or OneDrive environment and do not download files to their computer unless absolutely necessary and only with the explicit consent of the Team owner.

5.4.4 Publicly Accessible Information

For example:

- *Community links sharing local information or guidance.*
- *Prospective students provided with information as part of a virtual tour.*

If creating a Publicly Accessible Team use the selector button for Other. Manually delete the Team when it is no longer required.

Team technical processes will automatically email the Team owner every 180 days requesting they renew their group. If no approval is received the Team site will timeout and delete. Once deleted there is no possible recovery for the Team.

Should the Team continue to be used Team chat messages will persist indefinitely until the Team is deleted.

Publicly Accessible Information Teams will be permitted to share files and information with external Guests. Although it is possible to connect a guest without a Microsoft account certain features of the Team will not be available to non-Microsoft authenticated Guests, this is a designed feature of the product and cannot be altered by City IT. It is therefore recommended for fuller functionality Guests use a Microsoft account and email. Team owners should ensure Guests have adequate security in place on their systems, as a minimum antivirus software and password protection.

5.5 Group Chat / Teams messages

All messages and conversations are automatically saved within hidden files in Teams. Care must be taken with what is posted or written in chat, as it is subject to the same discovery as email under Freedom of Information and data protection legislation. There are provisions in law to provide certain messages upon request; because of this all chat strings and postings should be viewed as potentially viewable by others both within and outside of the University. Users should refresh themselves of the Email and Acceptable Use Policies to ensure compliance.

5.6 File Sharing

The Teams product can act as a link to OneDrive and SharePoint online, providing a secure means by which to hold edit and transfer files. There is no perceived security issue in transferring files to City-provided mobile equipment as these devices are encrypted and password protected by default.

Team owners should satisfy themselves Guests have adequate security in place on their systems to protect City data, which would include antivirus software, password protection and if possible, encryption. All data shared outside of City systems remains the property of City and personal data may not be further disseminated without authority of City's Data Protection Officer.

It is strongly advised any user of a computer which is not City-provided only edits and views files only within the Teams environment. Users of such equipment should not download these files to their devices, unless this is publicly available information or part of collaborative workings.

If there is a requirement to share personally identifiable information outside of the City environment you must seek guidance from Information Assurance before doing so (dataprotection@city.ac.uk).

5.7 Ownership

The initial Team creator will be considered in all circumstances to be the owner and controller of the Team site. They are accountable for the provision of the second Team owner, the content, naming, provision of administrative controls and to whom access is provided. Once another Team owner is allocated they too are considered as owners and controllers of the Team site. Owners are responsible in ensuring all persons using the site are aware of and abide by this policy.

To ensure the Team is adequately administered two owners must be provided for every Team, one of which must be a staff member.

Team owners should remove participants when they are no longer part of the team, with due diligence being applied to other administrators and external guests.

Guests may not be Team owners.

5.8 Recording

Occasionally meetings or other events may be recorded via Teams. A message appears at the top of the screen to advise that recording is taking place. Participants can object to the Chair if they do not wish to be recorded. City is the data controller for these recordings. Recordings should not be further disseminated unless to do so is compatible with the purpose for which they were made. Recordings should be deleted as soon as they are no longer necessary.

It is recognised that students may choose to record lectures or tutorials on their personal devices i.e. without using the official Teams recording function, for personal use. This is not within City's control but students are reminded that it is courteous to ask permission of other participants and to be respectful of fellow students and staff members.

5.9 Archiving

The archiving of Teams material is not normally undertaken buy IT services as it may be completed by the Team owner. Do remember archived material will still be searchable under the terms of data protection and Freedom of Information legislation and therefore should only be kept for as long as it is required and no longer.

5.10 Policies Applicable to Teams

By creating a Team, the owner accepts the Terms of Use, which comprise*:

a. IT Security Policy:
https://staffhub.city.ac.uk/_media/intranet-site/documents/policies2/information-technology/Information-Security-Policy.pdf

b. Conditions of Use Policy:
https://staffhub.city.ac.uk/_media/intranet-site/documents/policies2/information-technology/Conditions-of-Use-Policy.pdf

c. Acceptable Use Policy:
https://staffhub.city.ac.uk/_data/assets/pdf_file/0004/332356/Acceptable-Use-Policy.pdf

d. Data Protection Policy:
https://staffhub.city.ac.uk/_media/intranet-site/documents/policies2/information-technology/Data-Protection-Policy.pdf

*These will need to be made available to users without a City login for sharing with Guests by the Team owner.

6 Roles and Responsibilities

All users of information systems are responsible for the security of data in their charge and care. It is their duty to ensure University systems are used appropriately and securely. Any person who suspects misuse of University systems should report the matter to their manager, supervisor or Service Desk without delay.

Suspected data breaches should be notified without delay via Service Now.

7 Compliance

7.1 Compliance Measurement

The Information Security team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

7.2 Exceptions

Any exception to the policy must be approved by the Director of IT in advance.

7.3 Non-Compliance

Any reckless or wilful conduct by any person or persons using City, University of London's network and computer systems which undermines this policy or puts at risk the security of data may have disciplinary action being taken against them. All such cases will be fully investigated according to the University's disciplinary procedures and may be reported to the regulatory authorities.

In the case of a criminal offence being committed, City, University of London will involve the appropriate authority.

8 Risk Management

Risk management for each department is defined within their Risk Management Policy.

9 Policy Review

This policy will be reviewed by the process owner and updated alongside the security operating procedures on a regular basis, not to exceed 12 months.

10 Process Owners

ITD.

11 Review Schedule

This policy shall be reviewed and updated regularly to ensure that they remain appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations by the Information Security Manager and the Information Security Committee. Additional regulations may be created to cover specific areas as required.

Document Control

Document approval	
Approving Committee	**Approval Date**
ExCo	**27/4/2020**

Document review		
Reviewer	**Role**	**Review Date**

Change History			
Version	**Date**	**Author**	**Details of Change**
1.1	**24/3/2020**	**MC**	**Accepted by ExCo -Live**

Process Owner

ITD	

Uncontrolled Copy when printed