

Acceptable Use Statement - MS Teams

Version – v3 April 2026

Policy Statement Author – IT Strategy & Governance Manager

Procedure Owner – Director Information Technology

Parent Policy Statement – Information Technology Policy Statement

Public Access or Staff Only Access – Public

Version – Version 3 – April 2026

Changes and Reason for Changes – Links updated and aligned to UWS values



CONTENTS

CONTENTS	2
1 UWS Acceptable Use Statement (AUS) for Microsoft Teams	3
1.1 Overview	3
1.2 Purpose	3
1.3 Introduction	3
1.4 Scope	4
2 Policy Statements	4
3 What can you use Teams for?	6
4 Best Practice	6
4.1 Chats	6
4.2 Meetings and calls	6
5 Roles and Responsibilities	7
5.1 Site Owner	7
5.2 All staff (site members)	7
6 Retention & Monitoring	7
7 Support and Training	8
8 AUS Review	8
9 Contact Details	8
10 Feedback	8
11 APPENDICES	8
11.1 Appendix 1 – Glossary of Terms	8

1 UWS Acceptable Use Statement (AUS) for Microsoft Teams

1.1 Overview

This document is an extension of IT Acceptable Use Statement (IT AUS), in that it specifically strengthens and deepens the policy statements in the master IT AUS. This AUS specifically details the steps that need to be in place for this service to be used, monitored, managed and controlled in an efficient and effective manner. Ensuring that this service is conformant and/or compliant with UWS adopted standards, frameworks, patterns, values and guidelines as well as those of UWS.

The Document provides the core set of security principles and expectations on the acceptable use of MS Teams at UWS.

1.2 Purpose

The Acceptable Use Policy (AUP) aims to protect all users of UWS equipment and data, as well as minimising the risks associated with their use by providing clarity on the behaviours expected and required by UWS employees, Agents, Service Providers, Contractors, and Consultants. It sets a framework on how UWS services and systems should be used in order to meet legal, contractual, and regulatory requirements and defines how individuals must behave to comply with this AUS.

To ensure that individuals understand their responsibilities for the appropriate use of UWS resources, systems and services. Understanding what is expected will help individuals to protect themselves, colleagues and UWS equipment, information and reputation and ensure that there is clear accountability.

1.3 Introduction

UWS accepts that use of Microsoft Teams is essential to enabling the University to meet its aims and objectives. It is a requirement that use of this software is legal and appropriate for delivering UWS's responsibilities and does not create unnecessary risk.

Microsoft Teams enables you and your colleagues to send instant messages, make video calls and keep up to date with your teams.

Because Teams allows for greater interaction between UWS employees, IT must implement measures to ensure that it is used appropriately, reasonably and is in keeping with our values, on respect integrity, accountability and inclusivity. This AUS sets out how to do this, makes staff aware of how Teams should be managed and how new Teams, Secure Teams and externally shared Teams can be requested.

Secure Teams can be requested via IT and should be used where data of a confidential or sensitive nature is stored.

This document should be read in conjunction with the following:

- [Dignity and Respect at Work Guidelines](#)
- IT, Information Management and Data Protection Policies, in particular.
 - [Data Handling and Classification Protocol](#)
 - [IT Acceptable Use Statement \(IT AUS\)](#)
 - [UWS Data Protection Code of Practice](#)
 - [IT Software Licensing and Control Statement](#)
 - [IT Password Management Procedure](#)

UWS account holders are also bound by any relevant legislation, such as UK Data Protection and Copyright laws.

Misuse of the service can be investigated and lead to disciplinary action. UWS reserves the right to monitor use and compliance with the law and policy; we may use system analytics to achieve this.

1.4 Scope

This Statement applies to:

- The UWS M365 Tenant
- All UWS employees, students, Alumni, third-parties, third-party associates and UWS partner organisations and agencies.

2 Policy Statements

Policy ID	Statement
AUP.UWSMSTEAMS.001	
001.	All Users shall be made aware of the Acceptable Use Statement – MS Teams (this document) and, where appropriate, provided with security awareness training which covers this statement.
002.	MS Teams sites do not expire when the Team owner account is deleted, but any files assigned to them do. IT will monitor regularly for any orphaned accounts (where no owner is listed) and delete as appropriate.
003.	MS Teams sites must be created with a minimum of two (2) owners. Note: It is the responsibility of the Team owners to ensure that there are always at least two valid and authenticated owners appointed at all times whilst the site exists – for the avoidance of doubt this means at least two site owners must always have valid and current UWS account credentials.
004.	MS Teams sites must be set to PRIVATE and secure.
005.	MS Team sites must not have names that are considered to be offensive or derogatory.
006.	Team owners are responsible for managing guest and/or membership access and participation.
007.	The MS Teams Owner(s) are automatically considered to be the Information Asset Owner (IAO) – and adhere to the responsibilities of this role.

Policy ID	Statement
AUP.UWSMSTEAMS.001	
008.	MS Teams must not be used to download, process, create, store and/or transmit any form of language, graphics/images and/or material that could be offensive or derogatory.
009.	MS Teams sites that have the following words embedded or included in their names will be deleted by the MS Teams System Administration function at the earliest opportunity after detection. The embedded names (in any combination of upper or lowercase) are: • Test • Testing • Dummy • Temp
0010.	One-to-one and one-off group (e.g. non-Channel) chats are retained for as long as the account exists. UWS account holders are responsible for appropriate retention of data based on UWS data retention policies.
0011.	MS Teams sites are retained for 18 months after last activity. At that point the Team owner(s) will be contacted and asked whether there is any business need for the Teams site to be kept for longer. Otherwise, the Team will be deleted.
0012.	Team channel chats are retained for 3 months after UWS user account deletion.
0013.	MS Teams site owners are fully accountable and responsible in ensuring their sites and this service is used in an appropriate and relevant manner.
0014.	All users are responsible for ensuring that MS Teams usage is compliant with this AUS and other relevant supporting policies.
0015.	All users are responsible for assuring that their activities and actions are compliant with this AUS and other relevant supporting governance documents.
0016.	The system may retain chats, channels and sites beyond the retention periods above, even if they are no longer accessible to you. These can also be used in e-discovery activity.

Policy ID	Statement
AUP.UWSMSTEAMS.001	
0017.	Non-compliance with this AUS may result in user access privileges being revoked or suspended, permanently or temporarily, for this service.

3 What can you use Teams for?

Currently you should use Teams for the following:

- Chats and calls UWS colleagues.
- Creating and joining meetings with UWS colleagues and partners from other organisations.
- Teaching activities, including one-to-one sessions with students.
- Supporting students with IT/Student services issues/requirements.
- Collaboration with external colleagues

4 Best Practice

Below are some best practice guidance you should follow or be aware of.

4.1 Chats

- You should not create separate channels for private one-to-one chats or group chats. You can do this without creating new Teams Sites or Channels.
- Do not share sensitive information through the chat. Teams is not an appropriate way to share sensitive information relating to staff, students or other UWS confidential business information. There are security procedures in place to prevent this.
- If you are asking a colleague to check a certain record in a system, use reference numbers instead of names to minimise the risk to personal data.
- You can get a colleague's attention by typing @ and their name into the chat, but please try to avoid them whilst they are in meetings so as not to disturb them. Their presence status will tell you if they are busy.
- Any instant messages you receive while offline for under a week will be available next time you come online.
- Remember that all chat content, whether direct or within channels is searchable and therefore could be disclosable under Freedom of Information requests or Subject Access requests.

4.2 Meetings and calls

- Double check you have sent any meeting invites to the correct attendees.
- Follow our guidance on when and how to safely record meetings in [Teams](#).

- Be careful not to enter information into the chat that should not be discussed in the meeting. Anyone invited to the meeting can see what is written in the chat, even if they do not attend.
- Do not use one meeting to meet with multiple guests, where the guests should be met with individually. All guests to a meeting have full access to the chat that is created from the meeting, even after leaving.

5 Roles and Responsibilities

There are two roles within M365 for a Team: Owners and Members. Most users of a Teams Site will be members. There are three types of Team members.

- Member (internal)
- External Member – Someone from outside UWS who has been invited to a specific meeting
- Guest – an External Member who has been given access to a Teams Site.

5.1 Site Owner

The site owner should be the Information Asset Owner (IAO) , IAOs are accountable for:

- Ensuring that any of their information assets, or extracts from those assets, are managed appropriately within Microsoft Teams, in line with their responsibility, including adding or removing members and guests when necessary.
- Creating and deleting Teams Channels when necessary and in accordance with UWS design principles.
- Ensuring there are sufficient active system owners for the specific Team site (a minimum of 2 per site).
- Ensuring that the use of information on the Teams site is compliant with this AUS and the UWS IT – Acceptable Use Statement.
- Ensuring that chats within Teams Channels are used in an appropriate manner and follow UWS policies on appropriate behaviour.

5.2 All staff (site members)

All staff are responsible for:

- Their own activity within Teams.
- Ensuring that the use of information on the Teams site is compliant with this AUS and UWS policies, and
- Ensuring that chats within Teams are used in an appropriate manner and follow UWS policies on appropriate behaviour.

6 Retention & Monitoring

The following will be applied:

- One-to-one and one-off group (e.g. non-Channel) chats are retained indefinitely. Colleagues should consider whether chats in Teams feed should be retained or deleted.
- Dormant Teams sites are retained for 18 months. At that point the 'site owner' will be contacted and asked whether there is a business need for the Teams site to be kept for longer. Otherwise, the site will be deleted.
- Team channel chats are retained indefinitely. Colleagues should consider whether chats in Teams feed should be retained or deleted.
- Please note that the system may retain chats, channels and sites beyond the retention periods above, even if they are no longer accessible to you. These can also be used in e-discovery activity.

7 Support and Training

- The University will provide training and support for staff members on the proper use of OneDrive, Teams and general data security best practices.

8 AUS Review

This policy will be reviewed annually.

9 Contact Details

For any further questions or advice relating to this AUS, contact: IT Service Desk

10 Feedback

If you have any questions or comments about this AUS, such as suggestions for improvements, please contact: the IT Service Desk

11 APPENDICES

11.1 Appendix 1 – Glossary of Terms

Term	Description
ADC	Adequacy Decision Country
IAO	Information Asset Owner
SyOPs	Security/Secure Operating Procedures