Acceptable Use Statement MS Teams

Version – v1 – December 2023

Policy Statement Author – IT Security and Customer Support Manager

Procedure Owner – Director of Information Services

Parent Policy Statement – Information Services Policy Statement

Public Access or Staff Only Access – Public

Version – Version 1 – December 2023

Changes and Reason for Changes – New Statement

CONTENTS

1 UWS (University of the West of Scotland) Acceptable Use Statement for Microsoft Teams

1.1 Overview

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

This document is the UWS Acceptable Use Statement (AUS) for MS Teams. It provides the core set of security principles and expectations on the acceptable use of UWS MS Teams.

1.2 Purpose

The Acceptable Use Statement (AUS) 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 the UWS services and systems should be used in order to meet legal, contractual, and regulatory requirements and defines how individuals must behave in order 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 your use of this software be legal and appropriate for delivering the UWS's responsibilities 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. Additionally, you can collaborate, share, and edit files as a Team with colleagues where appropriate. Documents must be removed from Teams groups when no longer required and guidance on data classification must be followed at all times. The 'Guidance Document for Staff - Microsoft Teams Do's and Don'ts' provides additional useful advice on using Teams effectively and safely.

Because Teams allows for greater interaction between UWS employees, the university must ensure that it is used appropriately and responsibly. This usage statement sets out how to do this, makes staff aware of how Sites should be managed and how new Sites can be requested. It should be read in conjunction with the following:

- Code of Conduct for Employees
- IT (Information Technology), Information Management and Data Protection Policies, Procedures and Policies; in particular;
    - M365 Teams Guidance Document for Staff
    - Information Security Procedure
    - IT Acceptable Use Statement
    - Copyright Guidance
    - IT Password Management Procedure
    - Software Management Statement

- Social Media Guidelines
- Protocol for Use of Cloud Storage
- Data Classification Schedule

You are also bound by any relevant legislation, such as Data Protection and Copyright laws and the information below.

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 statement; we may use system analytics to achieve this.

1.4 Scope

This statement applies to:

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

2 Statement Statements

Statement ID **AUS.UWSMSTEAMS.nnn**	**Statement**
001.	All Users shall be made aware of the Acceptable Use Statement (this document) and, where appropriate, provided with security awareness training.
002.	MS Teams sites must be created with a minimum of two (2) owners. Note: It is the responsibility the site owners to ensure that there are always at least two valid and authenticated owners always appointed whilst the site exists – for the avoidance of doubt this means at least two site owners must always have valid and current Active Directory (AD) credentials.
003.	MS Teams sites must be set to PRIVATE and secure.
004.	MS Team sites must not have names that are considered to be offensive or derogatory.
005.	Site owners are responsible for managing guest and/or membership access and participation.
006.	The MS Teams Owner(s) are automatically considered to be the Information Asset Owner (IAO) – along with having the responsibilities of this role.
007.	MS Teams owners must ensure that any shared files or meeting /chat content held within the Team(s) they are the

Statement ID AUS.UWSMSTEAMS.nnn	Statement
	owner for conforms to the requirements for data storage set out in the Data Classification Schedule. Consideration should be given to classifying documents stored in Teams using the M365 data classification options
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 until the Team is removed.
0011.	MS Teams sites are retained for 12 months after last use. At that point, the Site Owner(s) will be contacted and asked whether there is any business need for the Teams site to be kept for longer. Otherwise, the Site will be deleted.
0012.	Team channel chats are retained for until the Team is removed
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 policies.
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.

Statement ID AUS.UWSMSTEAMS.nnn	Statement
0017.	Non-compliance with this AUS may result in user access privileges being revoked or suspended, permanently or temporarily, for this service.
0018.	Addition of external Team members must be done by request to IT Services and the Team created by IT Services with the Name beginning EXTERNALS -

3 What can you use Teams for?

Currently you should use Teams for the following:

- Chat and call with UWS colleagues,
- Use Teams to create meetings with UWS colleagues and partners from other organisations.
- Collaboration, file sharing with colleagues.

4 Best Practice

Below is 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 about customers. We have implemented security policies 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 FOI 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 rather than discuss it 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 they need to be met with individually. Guests to a meeting have full access to the chat that is created from the meeting, even after leaving.

4.3 File Sharing

- Documents must be removed from Teams groups when no longer required.
- Guidance on data classification must be followed at all times.
- Files deemed to be in the 'special category' data class must not be stored on Teams groups.
- Prior to sharing files within a Team, you must check that all members of the group have permission to view these files.

5 Roles and Responsibilities

There are three roles within M365 for a Team; Site Owners and Site Member. Most users of a Teams Site will be members. There are three types of site members;

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

Within UWS we have an additional role, with a senior officer being allocated accountability for the information within each site – this is the Information Asset Owner (IAO) or Manager (IAM) – also known as Data Steward.

5.1 Site Owner (Accountability) – IAO

IAOs (Information Asset Owner) 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 responsibilities.

5.2 Site Owners (Administrative)

Site Owners are responsible for:

- Removing members and guests when necessary/appropriate.
- Creating and deleting Teams Channels when necessary/appropriate and in accordance with the UWS's 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 UWS policies.
- Ensuring that chats within Teams Channels are used in an appropriate manner and follow UWS policies on appropriate behaviour.
- Ensuring Teams are named appropriately using acceptable terms and language.

5.3 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 until the Team is removed.
- Team's sites are retained for 12 months after last use. At that point, the Site Owner will be contacted and asked whether there is any business need for the Teams site to be kept for longer. Otherwise, the Site will be deleted.
- Team's sites will expire 12 months after last use.
- Team channel chats are retained until the Team is removed.
- 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.
- Content owners are responsible for ensuring that data held within Teams groups adheres to departmental/School data retention policies.

7 AUS Review

This statement will be reviewed as it is deemed appropriate, but no less frequently than annually.

8 Contact Details

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

9 Feedback

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

10 APPENDICES

10.1 Appendix 1 – Glossary of Terms

Term	Description
ADC	Application Delivery Controller
UWS	University of the West of Scotland
SyOPs	Security/Secure Operating Procedures
FOI	Freedom Of Information