

University of East Anglia Norwich

Microsoft Teams Governance Policy

Publication:	Internal only
Date approved:	19 November 2026
Approving body:	Senior Information Risk Owner
Date of next review:	November 2028
Review frequency:	Every 2 years
Policy/Regulation Owner:	Head of Infrastructure Services Associate Director for Information Compliance (& DPO)

1. Overview and Purpose

1.1 Microsoft Teams ('MS Teams') is a collaboration tool that integrates with other Microsoft Office 365 services to create a dynamic online team working space.

1.2 The University uses MS Teams as its preferred solution for:

- instant messaging (via 'Chat', meetings, and 'Groups')
- document storage and collaboration
- online meetings and events

1.3 This policy sets out the procedures for the creation and use of Microsoft Teams, including the roles and responsibilities associated with a Team, archiving and deleting of information or a Team, and the use of additional apps within Teams.

2. Scope

2.1 This policy applies to all staff and Guests that create, store, share and dispose of information using Microsoft Teams, or use it for chat and online meetings

2.2 Adherence to approved policy and regulations is fundamental to the effective operation of the university. This policy has been developed in alignment with sector best practice to promote consistency, accountability, and compliance with relevant standards. Observing the policy ensures that decisions and actions are informed, equitable, and aligned with institutional values.

3. Definitions

Term	Definition
Channel	A sub-location within a Team. There are three types of Channel: Public, Private, and Shared. By default, each Channel has two sections Posts and Shared Documents.
Channel Member	A user with access rights to a Channel. Channel Members generally have edit permissions within the Channel.
Channel Owner	A user with increased permissions to manage a Channel, this includes adding members to the Channel, and the ability to delete the Channel.

Term	Definition
Chat	This is an instant messaging function that can be 1:1, groups, or as part of a meeting.
Dataverse	A central cloud-based service that stores and organises information used by Microsoft Teams and other Microsoft 365 applications.
Folder	A designated space within a Channel (or within a Folder on a Channel) that enables files to be structured. Folders can be created within Folders.
General Channel	A sub-location within a Team; it is a special form of a Public Channel. General Channels are created by default and cannot be removed. General Channels should not be used to store data other than guidance about how to use the wider Team and its channels.
Guests	External users (without an @uea.ac.uk username) who can access approved UEA Microsoft 365 resources using their own organisational or personal email accounts. This is not the same as a Visitor.
Hidden Channels	Users can hide (and unhide) Channels within a Team. Infrequently used Channels within a Team will automatically be hidden
M365 Cloud	The location in which MS Team and other applications are retained.
Main Channels	This is a collection of your commonly used Channels within a given Team. Users can 'Hide' a Channel to move it into their Hidden Channels.
Microsoft Teams / MS Teams	The software for accessing Teams Chat, Teams and their channels, and other M365 Cloud applications.

Term	Definition
Microsoft Lists / MS Lists	An application for managing data in columns and rows.
Moderation / Moderators	Allows designated users to control who can create posts and manage conversations in a channel. By default, Team owners are the channel moderators.
Posts	This is a message board function that forms part of a Channel.
Private Channel	A sub-location within a Team that is restricted by default and can only be made accessible to all Owners and Members of the Team. Private Channels are marked with a padlock symbol to identify them
Public Channel	A sub-location within a Team that is accessible to all Owners and Members of the Team. It cannot be made accessible to those outside the Team.
Shared Documents	This is a sub-location of a Channel. It is where files and folders are stored.
Shared Channel	A sub-location within a Team with versatile permissions. It can be made accessible to Owners, Members, and those outside the Team. Shared Channels are marked with a loop symbol to identify them
Team	A location within MS Teams. A Team is made up of at least one Channel.
Team Member	A user with access rights to a Channel. Channel Members generally have edit permissions within the Team's Public Channels.
Team Owner	A user with increased permissions to manage a Team, this includes the granting of access rights to the Team, and the ability to delete the Team. See Section 4.1 for more details.
Visitor	A user issued with a V1 account. This is not the same as a Guest.

4. Roles and Responsibilities

4.1 Team Owners

Team Owners manage a Team and are responsible for:

i. Providing support/training to members of the Team they own

ii. raising ITCS support requests in relation to a Team they own

iii. managing permissions to the Team by adding and removing Team Members and Guests and changing member permissions (including notifying Guests of relevant IT usage and data protection policies)

iv. Ensuring data within the Team is managed according to all relevant University policies

v. Deleting a team when no longer needed

vi. Assigning a replacement Owner if leaving the Team or UEA

4.2 Team Members

Team Members have full use of the Team but cannot perform administrative actions for the Team, unless permissions have been given by Team Owner. See Microsoft's **comparison of Member's and Owner's capabilities**.

4.3 Guests

A Guest is someone who does not have an IT account with UEA who is granted access to a Team enabling them to collaborate on UEA's documents within UEA's M365 Cloud. This could include contractors, suppliers, or external researchers.

Guests can be added to the Team by the Team Owner. Team Owners should consider carefully whether all the data/information in the Team should be accessible to Guests.

Team Members can share individual files or folders with UEA users or non-UEA colleagues who are not in the Team by using the Teams appropriate sharing options.

Guests cannot be an Owner of a Team.

4.4 Users with additional responsibilities

4.4.1 Departmental Approvers

Departmental approvers are responsible for:

i. reviewing and approving, or rejecting, all requests for new Teams in their Department.

ii. nominating new owners for any Teams in their department which have one or fewer owners.

A list of Department Owners is maintained by the IT Service Desk. New approvers must be identified by the relevant Senior Information Asset Owner. A list of SIAOs is owned and maintained by the Information Compliance Team.

4.4.2 Information Asset Owners

The person who acts as the principal authority and has overall responsibility for an information asset and how it is managed.

Ideally, IAOs should be Team Owners for any sites for which they are responsible for the information within the site. However, an IAO does not need to be a Team Owner; nor does a Team Owner need to be an IAO.

4.4.3 Head of Infrastructure Services

The Head of Infrastructure Services is responsible for:

i. co-authoring and reviewing this Policy

ii. leading the ITCS Infrastructure Team

4.4.4 ITCS Service Desk

The ITCS Service Desk are responsible for:

i. managing the Departmental Approvers List

ii. providing initial customer support and escalate as necessary to the appropriate ITCS support area.

4.4.5 The ITCS Infrastructure Team

The Infrastructure Services Team are responsible for:

i. logging tickets with Microsoft and liaising with Microsoft to resolve a fault

ii. implementing and maintaining governance policies within the M365 cloud at the direction of the Senior Information Risk Owner, IT Leadership Team, or Data Protection Officer.

4.4.6 Associate Director for Information Compliance

The Associate Director for Information Compliance is responsible for:

i. co-authoring and reviewing this Policy

ii. devising and monitoring M365 information management policies including Data Loss Prevention, Record Retention, and Data Classification

5. Policy Statement

5.1 Instant Messaging and Online Meetings

Within MS Teams there are multiple instant messaging functions including Chat and Posts.

5.1.1 Chat

Chat is an instant messaging service. Chats are created outside of a Team, and can be '1 to 1', within Meetings and 'group chats'.

Chat is intended for work-based communications in real time. Chat should not be used to capture decisions or evidence activity; where such activity occurs in a Chat it must be exported.

The use of Chat for personal use is permitted.

All Chat messages are searchable to ITCS and Information Compliance; Chat may be searched in relation to statutory information requests, disciplinary investigations, or incident investigations.

All Teams Chats expire after 90 days.

5.1.2 Meeting Recordings

UEA permits the recording of Meetings; however, wherever possible, meeting organisers should ensure that attendees are agreeable to the recording taking place. The use of automated recordings is not encouraged, but nor is it prohibited.

Teams meeting recordings will expire:

- After **60** days if the meeting was created by **staff** or **students**
- After **30** days if the meeting was created by a **Visitor or Guest**

Users can change an expiry date by following the instructions to Manage the expiration of a meeting recording.

When a recording is deleted, the meeting owners will be notified via email. The recording can then be retrieved by the user from their recycle bin for up to 90 days. Once recovered, the recording will no longer expire automatically.

5.1.3 Posts

Posts are a messaging function within a Teams Channel.

Posts are intended for work-based communications with Channel members in relation to activity on the specific Channel.

The use of Posts for personal use is prohibited.

Posts will be retained for one year and will then be automatically deleted.

5.2 Team Management

5.2.1 Team Creation

Before requesting a new site, users should ensure that there is no existing Team that would be appropriate for their use.

A new Team can be requested at: https://office365.uea.ac.uk/requestteams

Each Department has designated Departmental Approver who reviews the request and approves, or rejects, the creation of the Team. Each Team must have at least two (2) Team Owners and these must be designated as part of the request.

5.2.2 Access Management

MS Teams should be used to manage access controls for the content stored on a Team or Channel.

Whilst Microsoft enables access to be managed within SharePoint, this functionality is prohibited.

Where access to content needs to be restricted either a Private or Shared Channel should be used.

5.2.2.1 Access Management - Public Channels

Public Channels – including the General Channel - inherit their permissions from the Team they are under. The content of such Channels is available to all Team Owners and Team Members of that Team.

5.2.2.2 Access Management - Private Channels

Private Channels exist within a Team but are restricted to a sub-set of that Team's Owners and Members. If we imagine a Team to be a building, a Private Channel is like a locked room within that building; the room (the Private Channel) has restricted access that depends on users first being able to enter the wider building (the Team).

When establishing a new Private Channel, or adopting a new Team Owner, all Team Owners should be granted access to all Private Channels under the site(s) they own.

5.2.2.3 Access Management - Shared Channels

Shared Channels are for making files available to those who are not members of the Team. It is a useful tool for communicating elements of a project or work-area to those outside the project or organisational team.

5.2.2.4 Access Management – Folder and File Level

Microsoft enables the use of file-level and folder-level permissions; however, UEA discourages this.

ITCS and the Information Compliance Team do not support File or Folder Level access management; they do not provide assistance on implementing this, nor in resolving issues arising from this. In the event of an issue arising, permissions will be reset to the default Teams/Channel Owners and Members; any File or Folder Level permissions will be lost.

The use of such permissions is done at the users own risk; users should consult with the relevant Team Owner and/or Information Asset Owner before utilising Folder or File Level permissions.

5.2.3 Retention and Disposal of inactive Teams

To prevent stale Teams from being retained indefinitely, the University applies automated retention and disposal rules to delete a Team after 365 days of inactivity.

Team owners will be notified before deletion so they can renew the Team if still required. If no action is taken, the Team and its content are disposed of.

5.3 OneDrive File Storage

The University has Digital Storage Guidance that sets out the appropriate use cases for different digital storage locations.

OneDrive is an appropriate document storage location for:

- your personal documents that no-one else needs access to; such as files relating to your employment
- local line management files

When a user leaves UEA, their OneDrive, and all of its content, is deleted. Therefore, it should not be used as a storage location for University data.

The University has limits on the volume of data that can be stored in a user's OneDrive; if this limit is breached by a user, they must take steps to reduce this to within quota. When a OneDrive is over quota, it will become read-only. A user will not be able to add further records to it or edit documents until records no longer required are deleted.

5.4 MS Teams File Storage

5.4.1 When to use MS Teams to store files

The University has Digital Storage Guidance that sets out the appropriate use cases for different digital storage locations.

MS Teams is the appropriate document storage location for information that is intended for use either within, or across, organisational structures - including with select external parties.

5.4.2 Appropriate use

Where MS Teams is the appropriate location, the below guidance should be followed:

i. no files, MS Lists, or Teams Applications should be created in the General Channel; the only exception is any local guidance on how to navigate and use that Team and its Channels.

ii. no personal (non-work) data should be stored on a Team

5.4.3 Retention and disposal of files in MS Teams

There is no automated retention and disposal of files stored in a Team.

The content of Team should be managed by its Owners and Members in line with the University's Record Retention and Disposal guidance.

Should a Team become inactive for a period of 365 days it, and all of the files within it, will be deleted. See section 5.2.3 for further information.

5.5 Feature Management (Apps)

5.5.1 Approved Applications

Within MS Teams, Microsoft by default makes some Teams Applications available for use to all users. These Apps – such as Whiteboard and Planner - can be added to a Team to provide additional functionality.

All Microsoft published Teams Applications are available for use by default and are approved for use.

However, ITCS do not provide assistance on implementing these Applications, nor in resolving issues arising from their use. Functionality issues arising from the use of Teams Applications will not be resolved by ITCS.

The use of such Teams Applications is done at the users own risk; users should consult with the relevant Team Owner and/or Information Asset Owner before adding such an App to a Team.

5.5.2 Unapproved Applications

Prior to adding a third-party app to a Team, Team Owners must seek approval via IT Service Desk to ensure that the appropriate data protection measures/agreements are in place with the app supplier in order to safeguard University data. Once this is done the third-party app can be made available in the App library.

If you wish to use a 3rd-party app in a Team, a Team Owner must seek approval via the IT Service Desk to ensure the appropriate data protection and security measures/agreements are in place with the app vender in order to safeguard University data and services.

If you have questions about data protection at UEA, contact the Information Compliance team at dataprotection@uea.ac.uk.

5.5.3 Prohibited Applications

The University prohibits the use Teams Applications and Teams Add-ins for other third-party storage providers including, but not limited to: Dropbox, Google Drive, and WeTransfer.

6. Compliance and Monitoring

6.1 UEA undertakes regular and routine monitoring of compliance with this Policy.

6.2 In addition to the standard review cycle, this policy will be reviewed sooner where:

- there is a significant incident or trend that changes UEA's risk exposure
- there are material changes to law, regulation, or sector expectations
- there are significant technology changes; or
- audit/assurance findings require policy amendment.

6.3 Significant or substantive changes to this Policy will only be approved by the Approving Body. However, the Policy Owner is authorised to make minor amendments to the Policy for the purpose of formatting, updating links, or correcting errors.

6.4 Activities that deviate from this Policy – without a prior approved Exemption from the SIRO – must be reported to the CISO and, where personal data is affected, the DPO. Failure to report such activities also constitutes failure to adhere to this Policy.

6.5 Where actual or suspected deviation from this Policy is identified the SIRO, CISO, DPO, or their deputies, are authorised to instruct Users to cease further activities and/or take remedial action(s) to ensure compliance with this Policy. Failure to adhere to such directions constitutes failure to adhere to this Policy.

7. Related Documents

This Policy is supported by the documents below; these should be read in conjunction with this Policy.

<u>Associated UEA Policies</u>

- Acceptable Use Policy
- Information Risk Management Policy
- Records Management Policy

8. Revision History

Version number	Approval date	Approval mechanism	Details of change
1.0		Project Team	
2.0	19/11/2026	SIRO	Major revision. • Format change from MyUEA accordion to Internal Policy Template. Adopting templates resulted in new sections on Definitions, Roles and Responsibilities, Compliance & Monitoring, Related Docs, & Revision History • Owners and Approvers clarified. • New Polic Statement content on Chat, Posts, File storage, OneDrive