

# Guidance Document for Staff – MS Teams

Version – v1 – November 2023

**Procedure Author** – IT Security and Customer Support Manager

**Procedure Owner** – Vice Principal (Finance & Infrastructure)

**Parent Policy Statement** – Information Services Policy Statement

**Public Access or Staff Only Access** – Public

**Version** – Version 1 – November 2023

**Changes and Reason for Changes** – new Guidance.



## Purpose

The purpose of this document is to enhance the security posture for all service users at UWS. Please take the time to read these guidance notes and familiarise yourself with best practices around Team management. Note that if guidance is not followed Teams may be deleted without notice where there is a perceived risk identified.

### Do

- Give Teams appropriate names to make them identifiable. Teams labelled as 'Test' or without a descriptive title will be deleted.
- Be vigilant for suspicious 'guests' in meetings. Is there anyone on the meeting call you wouldn't expect?
- Ensure a Team has more than 1 'Owner' role. Where there are not at least 2 owners assigned the role of 'owner' a member of the Team will be automatically elevated to this role.
- Have a portrait photograph as your Teams profile picture (rather than the Teams icon).
- Regularly (suggested monthly) review Team membership to ensure appropriate removal of members when they no longer require access and that the site is deleted at the appropriate time.
- Only add Team members who are permitted access to content (Files/conversations etc.)
- Delete Teams as soon as they are no longer required. Owners of Teams not used for 12 months will be emailed to advise that it is intended to delete the Team and given the option to justify the extension of use.
- Take care when adding files to Team Groups as the entire Team membership will see.
- Ensure created Teams are marked as 'Private'.
- When creating a team, check whether it is appropriate to re-use an existing Team to avoid duplication.
- Keep Team content clearly labeled, current and well structured.
- Refer to the [Data Handling and Classification Protocol](#) if you are unsure on what should be shared with a Team.

### Don't

- Create a Team name which uses offensive language or terms. These Teams will be deleted without warning and disciplinary action may be taken.
- Add external members to Teams without approval (Dean or Director and IT).
- Download Teams content to a 3<sup>rd</sup> party app/storage location.
- Change setting for a team from 'Private' to 'Public' without approval (Dean or Director and IT).
- Rename a Team without informing membership.
- Add files/attachments to Teams chats. This makes them difficult to find and risks data loss and creation of multiple copies of the same document which is poor practice. Save them under Files in the Team.
- Download copies of files from Teams, this creates duplicate and potentially outdated copies.
- Use Teams as a medium to deliver learning and teaching.