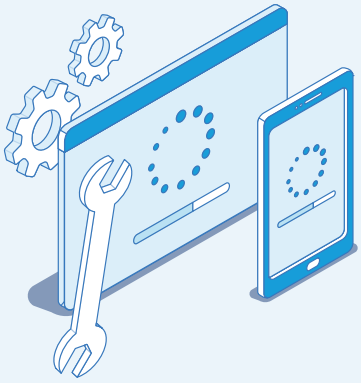
STAFF SECURITY TIPS FOR ZOOM

DEPARTMENT OF TECHNOLOGY ENHANCED LEARNING

With the increased use of systems like Zoom across the institute, it is more important than ever that these systems are deployed in a way that protects staff and student data while also preventing any unwanted uses of the system by internal or external parties. With this in mind, The Department of Technology Enhanced Learning has implemented a number of measures to safeguard your Zoom classes. Such measures include our enabling the Zoom waiting room as standard, default authentication settings, Canvas integration, and advanced permissions for staff and student user groups. While most classes run without issue, issues may arise for staff or students through, primarily, the use of an outdated version of the Zoom app, or by the way you and your students sign into the system.

To ensure the highest level of security staff are advised to make themselves aware of the following points and associated steps:



1 Keep your Zoom applications up to date

For important security updates and feature enhancements, please keep your Zoom applications (Desktop and Mobile) up to date. Zoom updates are released on a regular basis to address potential security issues, bugs, and to provide feature enhancements.

Check out our **Guide to updating Zoom**

2 Never use your Personal Meeting room to schedule a class

For security reasons, the Personal Meeting room option should never be used for live classes; your Personal Meeting Room **should only be used for one-off meetings** and typically sessions that are not recorded. Think of your personal meeting room like your office - where students may want to meet you privately one-on-one.

- **Always schedule your classes from Canvas**
  By scheduling classes in Canvas, students can clearly see upcoming classes in the Module Calendar, as well as accessing upcoming classes and recordings. Zoom also pulls enrolment data from the module which is updated daily.

3 Sign in via SSO

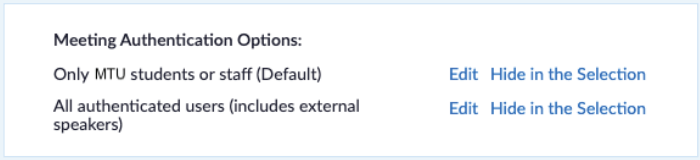
Ensure you are signed in to the Zoom desktop client or mobile app via SSO using your staff email and password to ensure you have full access to the features on our licensed MTU account.

Please also **advise your students** to log into Zoom using their @mycit.ie credentials

Follow the steps in this **Guide to signing in**

4 Authentication settings

Choose the relevant authentication option when scheduling a class.



"Only MTU students and staff" is the now the default option and will allow only authenticated users from within MTU (staff and students).

"All authenticated users (includes external speakers)" allows you to include users outside of MTU. This option should be selected if you want to include guest speakers in your zoom session and/ or students who may not yet have their mycit.ie account

Follow the steps in this **Guide to authentication options**

5 Use the Zoom In-Class Security Features

Use the Zoom In-Class Security features to easily access all the in-meeting security settings in one location. This includes Lock Meeting, Restricting Screen Sharing, Annotation, Chat and Removing Participants.

Check out our **Guide to in-class security features**

- **Inactivity Period:**
  If you have been inactive on the Zoom meeting client for a period of 10 minutes, you will be automatically signed out of Zoom.

In addition, this article on **Troubleshooting with Zoom** is highly recommended.