Video Conferencing Policy

Introduction

With video conferencing now being used by the college to deliver teaching sessions and conduct meetings it is important that staff understand the risks and best practices involved. This document will give you guidelines on how keep yourself and your students safe as well as tips for making video conferencing less daunting.

Currently Supported Platforms

At this time the college recommends the use of only two video conferencing platforms for College business.

- Zoom
- Microsoft Teams

Though these offer similar features, Zoom is a lot easier to use and is therefore suggested for classroom use. MS Teams offers more business based features and is more complicated to get set up.

General Rules

When setting up for a video conference there are a few things you should consider.

- **Internet Connection**
  - Is it fast enough for video or should you only use audio? Typically, you need a minimum or 3mbps upload and download for a video conference, Wi-Fi will introduce extra lag so make sure you have the best connection possible.
  - Is it shared, could someone else suddenly start using a large amount of bandwidth?
  - Is it reliable, could it stop working part way through your call? This mostly applies to Wi-Fi connections.
- **Location**
  - With the camera on what can be seen behind me?
  - Is the light too bright / in my face / over my shoulder? All of these can make it hard for others to see you clearly
  - What is the sound like, is there background noise, does the area echo?
- **Others**
  - Confirm the nature of the video conference, if it is confidential, ask all attendees to confirm that they have taken steps to ensure confidentiality.

- Are other people in the house, kids, pets that could make an unscheduled appearance. You should make them aware you are on video conference and if possible have the room to yourself.

Best Practices - General

Thanks to the similar features in both Zoom and MS Teams the below suggestions are possible on each platform, Network Support can offer guidance on how to enable these if users are unsure.

- **Background filters** – It is recommended if you are video conferencing in a busy area or from home you use a static background image from the inbuilt libraries of each app. This will reduce distractions for others in the video chat, block out any unwanted cameos and protect the privacy of your home.
- **Headsets** – Though not always necessary these are recommended as they limit the exposure of the conversation taking place. Others at your location cannot hear what is being said to you, and having a mic closer to your mouth means it is less likely to pick up background noise.
- **Screen sharing** – If you need to share something on your screen with others in the video conference it is recommended you only share the application window you need to show. This means that members of the conference can only see that application and nothing else on your computer. If you need to share multiple applications it may be necessary to share your entire screen, in this case make sure your desktop is appropriate, you may not want others to see what applications you have installed or the picture of your family on your desktop wallpaper.
- **Framing** – Try and sit center frame when in a chat and be aware of your movements it is easy to forget that the camera, unlike a person, cannot follow you if you move out of its field of view.

Best Practices - Zoom

Due to the recent issues around the Zoom platform it is recommended the following practices are followed at all times.

- Password protecting your meetings will prevent most “Zoombombing” – Make the password secure (i.e. not 1234, password or anything else easily guessable)
- Use the lobby feature and manually allow lobby members into the meetings, this also prevents “Zoombombing” as a secondary layer of protection.
- Once all attendees are present, lock the meeting preventing anyone else from joining. This may not always be practical but is the best way of protecting your meeting.

- Use the “Hands Up” feature rather than allowing attendees to just post constantly in the chat, this can be distracting for others and will also prevent anyone posting something they shouldn’t.

*****Zoombombing, Zoom-bombing or Zoom raiding is the unwanted intrusion into a video conference call by an individual or individuals, which causes disruption often maliciously and offensively.

Recording Video Conferences

Although both supported platforms have this feature it does come with considerations. The College’s position is that recording should only be used where there is a clear and justifiable reason to do so, in most cases it is recommended you check with a member of the SLT before deciding to record a session. Additional points of note are:

- Recorded sessions are covered by GDPR and College Retention Policies, as well as taking up costly storage space. Therefore, should be deleted as soon as they are no longer needed.
- You must have permission from everyone attending the session for them to be recorded. Preferably in writing (email counts). Anyone objecting to being recorded should be asked to leave the session. This includes audio only participation.
- Before recording, you should plan what you are going to do with the recording afterwards, where will it be stored and for how long? Recordings must be deleted as soon as they are no longer needed.
- Make the attendees aware of your / the College’s plans for the recording. Make sure this is done prior to commencing recording and is acknowledged in the written consent.

Safeguarding Requirements

When in a 1:1 video conference with any student, especially young or vulnerable students a third party should be present but where this is not possible the session will be recorded (with the student’s permission). This provides you with evidence in the event of any allegation, misconstrued comments or incidental disclosures. These recordings must not be kept longer than is necessary under safeguarding rules and should be deleted as soon as they are no longer needed.