Video Conferencing

Aim High, Learn Together, Feel Proud!

Ensure you have a complex password to access the system
This means having a mixture of numbers, letters, capitals and possibly special characters.

Avoid accessing video conferencing facilities on a mobile phone
As well as being impractical (as you may not be able to see all users on a mobile device), there have been instances of video conferencing software sharing data with social media channels (such as Facebook) without permission.

Do not record calls without prior permission.
We need consent to record users so permission should be sought at the beginning of a call. In any event video recordings should not be taken unless absolutely necessary and you should seek permission from your phase leader before doing so.

Check all the correct participants are present on the video call
Although unlikely, it can be possible for unauthorised individuals to jump on video calls. It may be best to start the call with a register if many users are involved on the call.

Ensure settings are fixed so that other users on the call cannot record the conversation covertly.
Check the system's settings to ensure that other users can't record calls. Also remind users at the beginning that the call should not be recorded.

External links shouldn't be shared
A lot of video conferencing software isn't encrypted and so can be prone to hacking. This can allow unauthorised users to join calls and send links to others (and these links when opened may expose user's account details and passwords). At the beginning of a call it may be beneficial to remind users not to open any external links sent over chat.

Sensitive documents shouldn't be shared over video call
Screen share facilities should be used rarely and should contain no personal data where possible. Other users can click "print screen" and then have a copy of documents they may not be entitled to. Additionally, unauthorised third parties external to the call may be able to access this data.

Do not send chat logs
If you send the chat log at the end of a call to users, you could be sending data they are not entitled to see. Some chat logs include private messages on them so beware sending chat logs to others.

Take control of the meeting
It is always best to have a facilitator to run the meeting, set the ground rules (such as making it clear there is to be no recording, etc) and also to set rules on chat etiquette (such as asking them to raise their hand before speaking).

Limit sending private or "side" messages to users
Content should be available to all.

Preparation/follow up
If you need to send documents or work in advance or following a chat session, do ensure that (1) all users are blind copied (BCC) into the email and (2) to avoid sending any sensitive data in those emails. If you need to send sensitive data (such as health data)

to a specific individual, do re-check the email address before sending to check it is being sent to the correct recipient.

Do not give out personal email addresses and numbers to users. Only school email addresses should be provided.
Providing personal details such as phone numbers, social media accounts or email addresses are forbidden in any circumstances. Please ensure you only provide them with official work communications only.

If you want to implement new software to interact with students please let your line manager know.
We need to conduct a data protection impact assessment before using them. Whilst there are lots of creative ways to communicate and interact with others during these times, some of those technologies are relatively untested so we as a company need to consider any security risks to data. Please do ask your line manager in the first instance.

Please refer to our acceptable use policy and procedure which can be found on the school website.

Approved: Oct 2021

Review: 2024