

OCMS Team Update

A message from Anne Howard



****Cascade as appropriate to your teams****

Dear Senior Leaders,

Our way of working has transformed significantly over the past few weeks. As we all become accustomed to this new way of working, it is more important than ever to remain vigilant about cyber security.

Zoom should not be used at Metro.

As you may have seen in the media over the last few days, there are serious privacy and data security concerns around Zoom, a remote conferencing service. It is important for the protection of your personal information and Metro data that you **do not use Zoom**.

Use Microsoft Teams

Microsoft Teams is our secure platform for communicating with colleagues while working from home. Attached here is the Microsoft Teams guide that is also available on our employee coronavirus [website](#).



This guide covers:

- Installing Teams
- Starting text chats with individuals or group
- Scheduling meetings
- Video calling
- Screen sharing
- How to create meeting minutes within Teams.

If you are invited to a Zoom meeting

In the event you are invited to an external meeting using Zoom, here is a list of precautionary Do's and Don'ts:

DO's

- ✓ Update the Zoom mobile app and the Zoom desktop app to the latest version.
- ✓ Choose "Join a Meeting" as guest if you are using Zoom mobile app or "Join from your browser" by clicking the link in your desktop invitation.
- ✓ Generate a new Meeting ID for each meeting.
- ✓ Set a password for the meeting.
- ✓ Send the invitation link and password to the meeting participants only.
- ✓ Lock the meeting after the meeting has started if necessary.

DON'TS

- ✗ Don't sign in Zoom using personal accounts such as Google or Facebook.
- ✗ Don't share or present confidential documents and screens in Zoom.
- ✗ Don't click on links in Chat within Zoom from untrusted parties.

Thank you for your ongoing commitment and focus during what is a very challenging time.

Regards,
Anne

Anne Howard
General Manager OCMS