# Information on the Safe Use of Technology While Working Remotely

For Faculty and Instructors

April 2020

# Contents

# Introduction

To ensure the health and safety of our campus communities, align with government recommendations and to prevent the risk and spread of COVID-19, York moved to required services only on our campuses.

All buildings on our campuses are closed with limited access as needed for required services. Only staff who are required to be physically present on York campuses to deliver services remain on campus. All other staff are working remotely.

The following guidelines are designed to support those working remotely to help protect the privacy of employees and the university.

# Working Remotely

- All university employees are responsible for protecting and maintaining the confidentiality of any privileged and/or confidential University information while it is in their home/possession or being transported.
- All University policies, procedures, guidelines, and best practices related to information technology and information security apply including, but not limited to:
    1. Installation of operating system and software updates
    2. Use of anti-virus software
    3. Password protection
    4. Be cautious of using email/internet and email spam/ phishing
    5. Sending restricted data
    6. Not downloading or installing unsolicited files
    7. Avoiding peer to peer file sharing
    8. Turning on the computer's firewall

York's Cybersecurity awareness resources can be found at:

- Online course for staff and faculty
- Cybersecurity Best Practices for working remotely
- Follow Information Security on Facebook, Instagram, and Twitter
- Please refer to University Computing Policies for more information
- Please review Off Campus Computing

## Management of Confidential and Personal Information

These guidelines are intended to provide standard best practices relating to the management of confidential and personal information, whether paper or electronic while working remotely.

## FIPPA

York University's Policy on Access to Information and Protection of Privacy establishes the policy for access to university information while also protecting individual rights to privacy, and brings the University into compliance with *the Freedom of Information and Protection of Privacy Act* ("FIPPA") of Ontario. Consequently, all employees must comply with FIPPA whether working at York's physical facilities or working remotely.

## Special Considerations for Information Management and Privacy

Careful consideration should be given when accessing records containing personal information remotely. A "RECORD" means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise that can be recovered, reproduced and accessed.

Best practice when working with personal information:

1. Do not leave University-provided laptop or mobile device unattended.
2. Avoid storing University information on a personal computer. If using a personal computer, save all information to a shared workspace or personal workspace (One Drive) and dispose of all electronic copies, securely, from the personal computer, when done working.
3. Refrain from storing University information on unencrypted personal USB / flash drive devices.
4. Avoid printing work-related documents to consult remotely. If printing is essential, ensure records remain under your control, are not left unattended, and are securely destroyed when no longer needed.
5. Do not dispose of paper information of confidential nature or containing personal information in recycle bins at home or in a public area.
6. Avoid opening or viewing information in a venue were the information or the display panel of your portable device may be seen by unauthorized individuals.
7. Check the "downloads" folder to ensure that information automatically saved there is deleted such as from web browser and from download folder on personal computer hard drive.
8. Empty your personal computer recycle bin.

**Note:** The list above is not meant to be an exhaustive list but is meant to establish basic practices that someone can take/follow to protect records.

## Privacy Breaches

Suspected or confirmed Privacy Breaches should be immediately reported to your Chair/Director/Dean and to the Information, Privacy and Copyright Office (IPCO).

# Conducting and Participating in Online Meetings

The following guidelines pertain to online meetings both in Zoom and Microsoft Teams, unless specifically stated Zoom only.

## Zoom Security & Privacy

- Zoom users can log in securely with their Passport York credentials by visiting yorku.zoom.us. The Zoom @ York U service does not store any personal information beyond name, email address (which serves as the user account) and company name. Your Passport York credentials are never shared with the service.
- The meeting transmission data (audio, video, and content) and metadata are encrypted from end to end using the AES 256bit encryption algorithm and TLS tunneling as they connect to and travel through the Zoom cloud servers which are outside of the York network.
- Meeting hosts can record locally to their personal device and can grant other meeting participants the ability to record in meeting, though this feature is not available by default.
- Participants are audibly alerted to active recording in meetings, and visually by the red record icon in the top left of the Zoom window.
- Cloud Recording is now also available to Faculty. This feature will allow meeting hosts to opt for recording their meetings and having them automatically uploaded onto the Zoom cloud servers.

These servers are external to the York network the viewing of these files is limited to those who are members of York's account and who have received a meeting link from the meeting host.
- Files cannot be downloaded unless the meeting host grants users the ability to do so. The files will by default be kept for 30 days before they are deleted and can be removed at any time before then by the meeting host.
- For more information, read York's Zoom Privacy and Security Guidance
- Read a message from Zoom CEO to users outlining what Zoom has done to actively and quickly address specific issues and questions that have been raised
- We encourage you to NOT post pictures of your virtual meeting on social media or elsewhere online without consent from all participants.

## Security Options when Scheduling a Meeting in Zoom

There are many settings and other protection options at your fingertips when scheduling a meeting and rather than change anything in front of your participants.

Here are a few of the most applicable:

- Require registration: This shows you every email address of everyone who signed up to join your meeting and can help you evaluate who is attending
- Use a random meeting ID: We recommend you generate a random meeting ID for your meeting, so it cannot be shared multiple times. This is the better alternative to using your Personal Meeting ID, which is not advised because it is basically an ongoing meeting that is always running
- Password-protect the meeting: Create a password and share with your participants via York email so only those intended to join can access a virtual meeting
- Allow only authenticated users to join: Checking this box means only members of your organization who are signed into their Zoom account can access that meeting
- Disable join before host: Participants cannot join meeting before the host or moderator joins and will see a pop-up that says, "The meeting is waiting for the host to join"
- Manage annotation: Hosts should disable participant annotation in the screen sharing controls to prevent participants from annotating on a shared screen and disrupting meeting

Additionally, hosts have a few in-meeting options to control your virtual meeting:

- Disable video: Turn off a participant's video to block distracting content or inappropriate gestures while meeting is in session
- Mute participants: Mute/unmute individual participants or all of them at once. Mute Upon Entry (in your settings) is also available to keep the noise/distractions as people enter
- Attendee on-hold: An alternative to removing a user, you can momentarily disable their audio/video connections. Click on the attendee's video thumbnail and select Start Attendee On-Hold to activate

## ZOOM Accessibility

Zoom follows the latest accessibility standards to ensure that the product is fully accessible by everyone. One of the options supported by Zoom is closed captioning. See full Accessibility Features in Zoom

Additional Accessibility information includes:

1. Be mindful that not everyone can participate equally in live video/audio meetings.
2. There is a Borrow-a-laptop program for people with older technology at home. Learn more on the Off Campus Computing page
3. Give people the option of calling in by telephone, contributing/asking questions with text messaging.
4. When showing images or charts, be sure to provide descriptive narratives of visuals to help those who may be visually impaired.
5. Avoid extra meeting features or complex functions as these could be difficult for those using screen readers.
6. Any information required to participate in the meeting should be shared directly with participants so that they can review it in the way they prefer—that is, where possible provide access to a document directly rather than screen sharing, this will allow people direct access to it so they can zoom in, etc.
7. Ensure that the meeting is captured in high-quality minutes made available in a document that people can review outside of the meeting.
8. Whenever possible, encourage meeting participants to confidentially let you know of any accessibility needs they have.

## Conducting a Meeting

To improve your meeting experience and that of the other participants in the meeting try to:

1. Find a quiet space, free from distractions, where possible.
2. Be mindful of your background adequate lighting.
3. Have a designated facilitator/monitor for the meeting.
4. Mute your microphone when not talking and, as a host or co-host, mute other participants' microphones if needed to improve the audio quality of the meeting by reducing background noise.
5. Use a headset microphone if you have one available—this reduces echo and greatly improves the audio quality of the meeting.
6. Be conscious of not speaking over other participants. If needed, use the chat or use the raise your hand (Zoom).
7. If you are hosting a meeting that is going to be a few hours or more, include scheduled breaks in your agenda.

## Setting Passwords

- The university recommends using passwords for meetings to ensure only the people you've invited are able to enter your meeting
- Check out Zoom's blog post about preventing party crashers in your meetings

## Lock Your Meetings

- You can lock a Zoom session that has already started, so that no one else can join. Give participants a few minutes to join and then click **Participants** at the bottom of your Zoom window. In the **Participants** pop-up, click the button that says **Lock Meeting**.

## Requiring Participants to Authenticate

- Zoom let's you specify that you'd like to have your participants authenticate or sign-in to Zoom before joining your meeting. This feature can be turned on when scheduling a new meeting by selecting "*only authenticated users can join*" in the meeting options.

## Recording Meetings

- The use of Zoom technology facilitates online meetings in a manner that closely resembles the interactions that could occur in an in-person meeting. As is the case with in-person meetings, audio or video recordings of meetings are generally not advised. When necessary, assign one of the participants to take minutes. More information on Minute-Taking Tips and Techniques can be found on the Information and Privacy website.

## Control Screen Sharing

- Ensure you close any open documents or windows prior to the online meeting to avoid accidentally sharing unrelated or confidential information on your screen.
- We recommend sharing individual "windows" as opposed to "screens" to avoid others seeing email or other confidential information that may be open on your screen.
- To give meeting hosts more control over what participants are seeing and prevent them from sharing random content, Zoom recently updated the default screen-sharing. Sharing privileges are now set to "Host Only," so hosts by default are the only ones who can share content in class.
- However, if participants need to share their screen with the group, you can allow screen sharing in the host controls. Click the arrow next to **Share Screen** and then **Advanced Sharing Options**. Under "Who can share?" choose "Only Host" and close the window. You can also change the default sharing option to **All Participants** in your Zoom settings. Learn more about How to manage screen sharing.

## Use of Video During Meetings

- While use of video during meetings, especially team meetings, is a recommended practice to encourage social interaction during times of physical distancing, it is not a requirement. You may also consider adding a picture of yourself if you are not sharing video to help other participants put a face to a name, especially those you have not met in person.
- If you are using video, consider using a virtual background in Zoom to eliminate and separate your home/working space. Keep in mind that family members who come in view of your computer camera/webcam could be detected even with a virtual background. Use York Branded images when possible. Use the "Blur Background" during MS Team video calls.
- If you do not wish to use video the entire meeting, consider using it at beginning to say hello, build connection, then close it. This may also help to optimize performance of the technology during the meeting, especially in large MS team meetings.

## ZOOM Waiting Room

- The Waiting Room feature is one of the best ways to protect your Zoom meetings and keep out those who are not supposed to attend. When enabled, you have two options for who enters the Waiting Room before entering a meeting:
    1. All Participants will send everyone to the virtual waiting area, where you can admit them individually or all at once.
    2. Guest Participants Only allows known participants to skip the Waiting Room and join but sends anyone not signed in/part of your meeting into the virtual waiting area.
- The virtual Waiting Room can be enabled for every meeting (in your settings) or for individual meetings at the scheduling level. Visit the support page for more information on adjusting your Waiting Room settings. Learn more about How to enable the Waiting Room.

## Lock Down the Chat

Hosts can restrict the in-meeting chat so participants cannot privately message other participants in Zoom. You can control chat access in your in-meeting toolbar controls (rather than disabling it altogether) so participants can still interact with the host as needed. Learn more about How to control chat access.

## Removing a Participant

If someone manages to join your meeting, you can quickly remove them from the Participants menu. Hover over their name, and the **Remove** option (among other options) will appear. Click to remove them from your virtual meeting, and they won't be allowed back in. Learn more about How to remove a participant in Zoom

## Using Teams

It is also possible to hold meetings directly in Teams. Team benefits include:

1. Ease of holding a meeting with all members of any particular team
2. Initiate a voice call within a Chat session (click the Phone button)
3. Inviting others to your voice chat by adding them on the fly (add person icon at the top of the voice chat)
4. Creating meetings directly on your calendar within the Team client (utilizing the Calendar button)
5. Additional features in the Call menu

- You can also learn more about Office 365 on the yuoffice website: https://yuoffice.yorku.ca/

## Teams Instant Messaging

- In 2019, Microsoft announced: Skype for Business Online to Be Retired in 2021.
- For this reason, the University is recommending that you use Microsoft Teams Chat as your **Instant Messaging (IM)** platform.
- Microsoft Teams allows you to chat with either all Team members in a Team (**Posts** tab in a Team) or specific individuals or groups of users (**Chat** button in Teams).
- Instant messaging is great for quick exchanges with colleagues you work with frequently, and **Teams Chat** can now be your default IM app for Outlook, letting you start a chat directly from an email message.
- Learn more about how to use MS Teams Instant Messaging
- The following are some helpful tips for using Instant Messaging:

1. If you do not already use IM in your unit or with other colleagues, you should first have a conversation with your colleagues to discuss expectations of use – how you will use it, what is the expected response time, etc.
2. Generally, you should not start using IM with someone you do not know, or even with a colleague, unless you have discussed that as a preferred/alternate form of communication.
3. Use status indicators to see if colleagues are "available" to chat or "busy".
4. Treat your IM conversations as though they are happening in public spaces, and like email, do not say or share anything in an instant chat that you would not share publicly and openly.
5. Instant messages are not private. Anything you write in a chat can be forwarded to others who may not be your intended audience but who will see what you've written.

# File Storage, Sharing & Collaboration

## Security

- Every time we share information, whether through email, USB stick, fax, or other transmission services, there is a risk that it will be intercepted by unauthorized parties.
- Faculty and staff who access York systems or share York data have a responsibility to protect this information, especially when it is confidential or sensitive. The following are university approved file storage and sharing methods:

1. We strongly recommend copying all your personal work folders and files into OneDrive. OneDrive is the easiest way to access and update your documents remotely. Click here to learn more about OneDrive.
2. Microsoft Teams or network shared drives using VPN are both acceptable places to save documents that need to be accessible by entire teams/departments. It's highly recommended to students, faculty, and staff to use VPN when performing York related work off-campus and when using non-secure wireless.
3. Microsoft OneDrive and Teams are approved for storing confidential files, except:
    - Payment Card Industry data
    - Personal Health Information

Learn more about Privacy and Security in 0ffice 365

## yuoffice and Office 365 Tools Overview

- **yuoffice** provides valuable tools that can help you collaborate with community members remotely. Functionality includes:

| Function | Office 365 Product |
|---|---|
| Store, share and collaborate on Documents | OneDrive and Teams |
| Instant Messaging, online meetings and voice chat | Teams |
| Project and Task planning and sharing | Planner |
| Video hosting and sharing | Stream |
| Note taking, organizing and sharing | OneNote |
| Create simple and effective Communication | Sway |
| Create forms, surveys, quizzes and polls | Forms |
| Task management and sharing | To Do |

- You can learn more about Office 365 on the yuoffice website: https://yuoffice.yorku.ca/

## File Sharing and Collaboration

The following are some recommended guidelines for Office 365 File Sharing in OneDrive or Teams:

1. Always share files with specific individuals as opposed to "anyone" in the organization.
2. For multiple file shares, share a whole folder of files as opposed to setting permissions on each individual file.
3. Limit access to only what is required (i.e. view vs edit).
4. Once the sharing is no longer required, remember to remove the shared access. You can see all your shared files by selecting Shared --> Shared by You in OneDrive.
5. Alternately, you can store files in a Team of which you are a member for use by all other Team members.
6. Use Teams when sharing files/folders with a group.
7. Share folders rather than many individual files.
8. Maintain one copy where feasible and share the copy via a share link.
9. If using Microsoft Office, you can edit files directly on your cloud OneDrive storage as opposed to downloading and uploading each time.
10. Version history capabilities are available for the last 500 revisions however for major changes you can rename your file and provide versioning (i.e. filename v1.doc, filename v2.doc).
11. Sync files between your computer and the cloud so you can access files from anywhere. More information on using OneDrive Sync

## Inclusivity and Working Remotely

"In an inclusive meeting, everyone gets a chance to contribute and all voices have equal weight". Read more about How to counteract 3 types of bias and run inclusive meetings.

**Land Acknowledgement**

"The land acknowledgement is an important part of reconciliation following the findings of the 2015 Truth & Reconciliation Commission of Canada and its calls to action. It is an acknowledgement and a moment of pause". Please visit **here for more information**. Land Acknowledgements can be said at the start of a remote meeting with any number of participants.

**Religious Observances**

Be mindful of religious observances and when they might be taking place and how this may impact remote participation in meetings, lunch & learns, remote coffee chats etc.

**Safe Space**

We cannot assume that the home is a safe space for all meeting participants, free of bias, conflict or potentially threatening situations. It is important to check in with your colleagues and be open to being flexible and provide assistance, if needed. Please feel free to contact Health, Safety & Employee Well-Being. or Employee and Family Assistance Program (EFAP) for further information.

# Technical Support

For additional support or technical issues, please contact the IT Service Desk at askit@yorku.ca and/or contact your local IT support.

# Additional Learning Resources for Working Remotely

- Learn more about using Zoom for online meetings using the Zoom Resources Guide
- Learn more about MS Teams and O365: https://yuoffice.info.yorku.ca/training/
- Teaching Commons: https://bold.info.yorku.ca/