your own place

Presents

Safety Toolkit 2020

This Safety Toolkit has been designed to help you remain safe when using different Programmes and Apps during virtual delivery. This toolkit will include;

- Downloading Zoom
- Signing in to Zoom
- Inviting people to Zoom
- Staying safe on Zoom
- Additional Zoom Functions
- Screen-Share on Zoom
- Chatting on Zoom
- File-Sharing on Zoom
- Zoom Top-Tips

your own place

Presents

Zoom Safety Toolkit

Zoom is a video calling website that allows you to video call others around the world. It is hosted online so does not require you to create an account or download to use.

- Zoom can be downloaded to a PC or Laptop and there is also an App available on Apple Store and Google Play Store

If your trainee/participants decide to download Zoom just remind them they will need to set up a Zoom account. This will also mean they will need to enter personal details such as;

- Date of Birth
- Name
- Email Address

Whilst downloading the Zoom programme is preferable, any downloads must be the trainees/participants choice. We should also encourage online safety around sharing personal information.

Like most Apps and websites Zoom also offers the option to sign in using Facebook. Whilst this can be quick and easy it can also allow unknown and unwanted personal data to be collected by Facebook.

facebook

- When sending joining instructions to any trainee/participant ask them to sign in using an email address if they can. As this will potentially stop any personal information being shared from Zoom and limit the risk of further sharing

Good practice communication - During the sign-up process you will be asked to login using an email address or Facebook. We highly recommend that you sign in using an email address so no personal information from Zoom is shared with Facebook.

Bad practice communication - During the sign-up process you can choose to login using an email address or Facebook. Facebook is likely to take your personal information from Zoom.

This will also be a decision that the trainee/participant must make. It is our job to remind them of the risk of sharing data.

your own place

Presents

Zoom Safety Toolkit

When using Zoom there are things that we can do to keep ourselves and the trainees/participants safe.

- Each Zoom meeting that is created will be allocated a unique ID, Password and Link. This will help keep meetings safe for you and the participants. These details should be shared in a safe place to minimise risk

Good practice would be sending the link to trainees and participants directly along with safety instructions.

Bad practice would be posting it somewhere public for people to find such as social media or forums.

- When hosting a Zoom meeting with professionals always ask them to share their full name and organisation

- When hosting a Zoom meeting for trainees they must only share their first name. Only introduce the first letter of surnames if there are others with the same first name

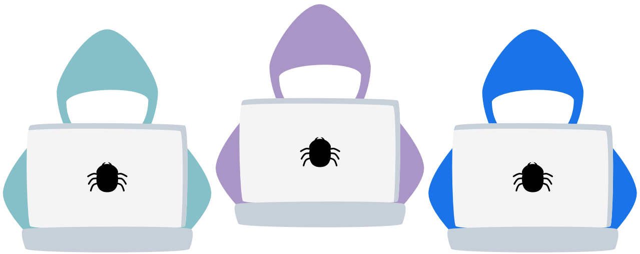
your own place

Presents

Zoom Safety Toolkit

- You can lock all meetings after a set amount of time or when all trainees/participants are present, this will stop unwanted guests (also known as 'Zoom Bombers') joining

A 'Zoom Bomber' is an individual who will join a Zoom meeting they have **NOT** been invited to with the intention of causing disruption or to hijack the session.



- You can also enable waiting rooms, so as a host you can decide who can enter the meeting. This will also help to deter and stop 'Zoom Bombers'

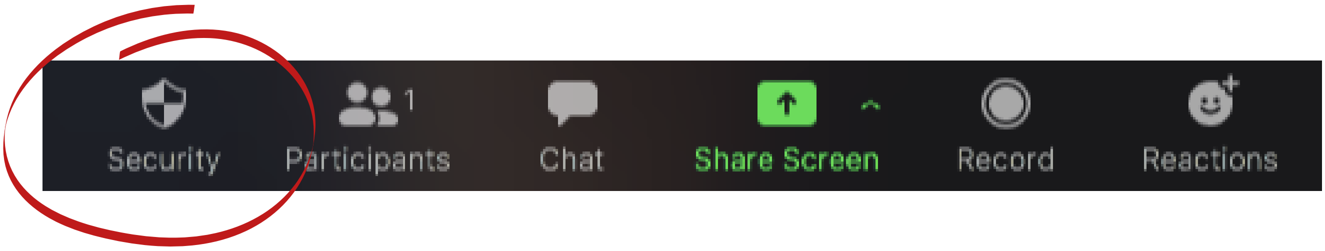
If using this feature make sure you know who you are expecting to the meeting.

Presents

Zoom Safety Toolkit

If you are the host of the session/meeting you have the option to turn on/off additional functions such screen-sharing and chat.

- When in a Zoom session/meeting you will need to click on the 'Security' button to turn these functions on/off



Always consider the meeting you are hosting to decide which functions you may need

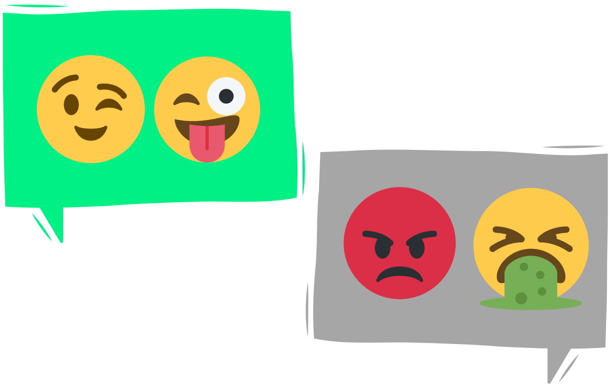
- Screen sharing will allow the host or a trainee/participant to show the rest of the group in the meeting what they are seeing and doing on their personal PC or Laptop

your own place

Presents

Zoom Safety Toolkit

- Chat allows participants to talk to each other by typing text into the chat box. This can be sent into a group chat or people can send personal messages to each other



- File-sharing is a great way to share documents and links quickly amongst the trainees/participants in the meeting

- The file-sharing function is accessed through using the chat function and means chat will need to be enabled in order to use it

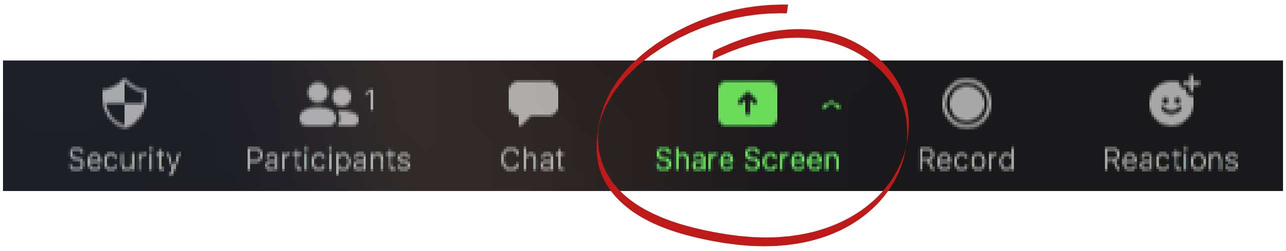
Always consider the meeting you are hosting to decide if these functions are needed for the delivery of the session/meeting.

your own place

Presents

Zoom Safety Toolkit

To share your screen with the participants/trainees in the room you will need to locate and click the 'Share Screen' button



- The 'Share Screen' function will show everyone else in the Zoom session/meeting what is on the screen of the person sharing. This could potentially risk someone showing something that is not appropriate for the session/meeting. It could also risk the trainee/participant sharing personal information that may be on their screen

Good practice would be turning this feature off for participants/trainees. Only enabling it, if it is vital for the delivery of the session/meeting.

Bad practice would be leaving this feature open, so any participant/trainee could potentially hijack the session/meeting.

Quick tips for the host/facilitator

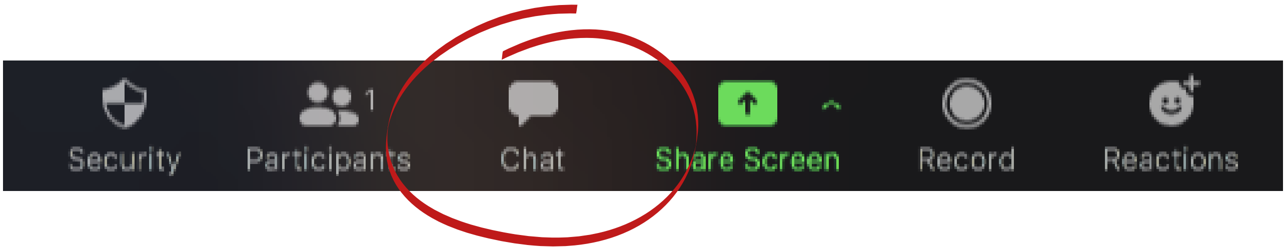
- Have a clean desktop with no personal information available
- Only pre-load the programmes and documents you need to deliver the session
- Enter your Zoom early to check all your settings and functions are working properly for screen sharing

your own place

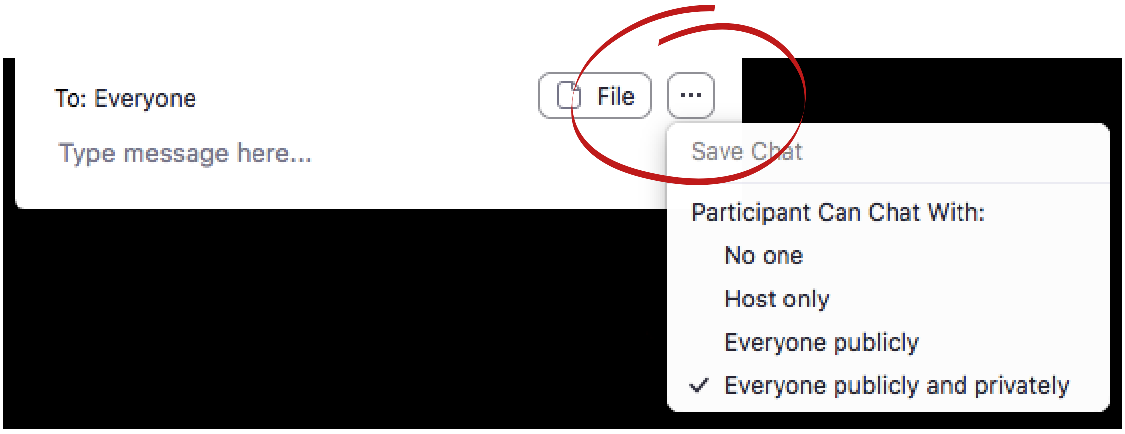
Presents

Zoom Safety Toolkit

To use the chat function you will need to click on the 'Chat' button.



- If using Chat function during delivery, it is essential that you decide before the session/meeting who will be able to communicate with who
- This can be done by opening up the chat window and clicking the '...'



Participant Can Chat With:
No one
Host only
Everyone publicly
✓ Everyone publicly and privately

- If the chat is not moderated in this way it could risk people privately messaging, sharing personal information as well as sending messages to each other that may not be suitable

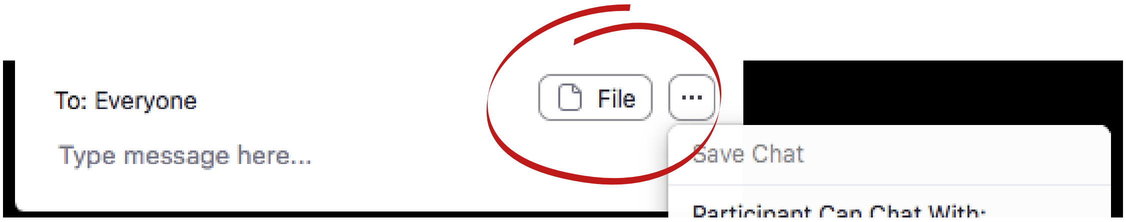
Good practice would be turning this function off until it is needed in the session/meeting.

Bad practice would be leaving this feature open, so any participant/trainee could privately chat to each other.

Presents

Zoom Safety Toolkit

When the chat function is enabled it will offer the function to share folders at the click of the button.


To: Everyone
Type message here...

- File-sharing will allow you to share large sized documents quickly to everyone in the meeting/session, which otherwise would take a large amount of time to send individually over email

- Unknowingly this means unstable/corrupted documents could be shared by anyone in the meeting/session
- This could infect the participants/trainees device with viruses which could stop it from working
- It could also infect the device with Spyware and Malware which will infiltrate your computer and steal sensitive personal information (account details, bank details, passwords, email address accounts) to be used by others

The only person who should have access to share files should be the host/facilitator. This will minimise any type of digital risk to participant, trainess and you!

your own place

Presents

Zoom Safety Toolkit

Some top tips on managing and keeping yourself participants and trainees safe are;

- Enter your Zoom room 15 minutes early to make sure all functions are working correctly to avoid any technical difficulties during delivery
- Use your 'Security' settings to enable/disable functions that may/may not be needed for delivery
- When Screen Sharing make sure your desktop is clean and no personal information can be seen
- Pre-Load anything you may need during delivery to minimise any disruption to the meeting/session
- Make sure if using the 'Chat' function you set who can talk to who, so this can be monitored for safeguarding reasons
- If any unwanted messages are sent in the chat (personal information, explicit language) these are deleted with urgency and addressed with the group
- File sharing should be disabled and only enabled by the host/facilitator if needed
- Take time to share with participants/trainees about how to keep themselves safe from online risk