Your guide to safely using collaborative tools

As many of us are now working from home, we have turned to digital solutions to stay in touch and conduct our business operations.

And while we appreciate the benefits of online collaborative tools, we must also understand the risks associated with them and apply some essential safety rules.

We must use these tools safely to protect ourselves, the information we handle and the organisations we work for.

Only use tools supported by your organisation

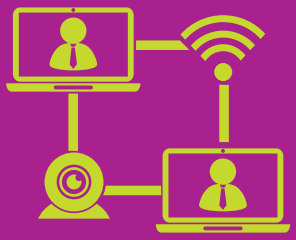
Before using any collaborative tool, such as instant messaging, secure file transfer or video conferencing, check it has been audited, has the appropriate level of security and is approved for use.

Using approved tools will enable you to remain connected and productive while working from home, without putting the organisation or yourself at risk.

Video conferencing tools

There are many video conferencing tools available, such as Microsoft Teams, Zoom, Google Meet, Skype and Slack. While these video conferencing tools can provide a forum to stay connected while working from home, we must make sure we are using them in a secure way.

Zoom, for example, has come under fire recently after privacy and security concerns, including 'Zoom bombings'. Attackers have been entering meetings to share pornographic content, racist language and violent threats.



But there are ways to protect information and secure meetings against unauthorised or disruptive participants.

Before the meeting:

- Only use approved video or telephone conferencing tools.
- Familiarise yourself with the tool's settings and features.
- Generate random meeting IDs and password-protect all meetings.
- Only allow invited people who are authorised and have a 'need-to-know' to attend.
- Do not share links on social media or public forums.
- Turn off file transfer to prevent participants from sharing unsolicited images, GIFs or other content.
- Turn off annotations to prevent others being able to write on the screen.
- Check the classification level and details contained in any documents or information you will share in the meeting.
- Choose a location where you will not be overheard or where your screen could be seen by unauthorised people.

During the meeting:

- Use a secure internet connection, such as your work VPN. Never use a public WiFi connection.
- Confirm all participant's identities and that they are authorised to know what will be discussed.
- Lock the meeting once all authorised participants have joined.
- Ensure attendees understand the sensitivity of the material being shown or discussed
- Limit desktop sharing to the specific application that is needed.
- Never leave a workstation that is in desktop-sharing mode unattended.
- Prevent participants from screen sharing and disable private chat.
- Remove unwanted or disruptive participants, put them on hold, disable their video, or mute them.
- End the meeting and log off when you are finished.

Remember, each tool will have its own settings and functionality, so make sure you are familiar with the tool before hosting a meeting.

Consequences

Using unapproved tools or failing to secure a meeting could put you, the information you handle and the organisation you work for at risk.

Tools which have not been approved may contain vulnerabilities which could expose networks to attackers or malware.

Failing to properly secure a meeting could expose participants to social engineering attacks.

And exposing information to participants who do not have a 'need-to-know' or allowing uninvited participants into a meeting where confidential information is discussed are both examples of data protection breaches.

So, please only use approved tools, and use them safely to protect yourself, your information and your organisation.