Guideline for members on the protection of data and security for online meetings

Online communication platforms have become the norm for remote work meetings and conferences during the Covid-19 emergency. There are many platforms available with different levels of functionality, security measures and privacy statements. The following guidelines are provided to members who use online platforms for union activities. The key principles of; enhancing the protection of personal data and reducing security risks are the central concern. The guide also provides some general good practice measures that can be taken when using online platforms. The guide does not recommend any one particular software platform. There are also some links to useful information and resources provided at the end.

The online platform software

- Always use the Paid for version of the software as it has better security and privacy control, free versions usually require access to your private data for commercial use.
- Only download the software from a trusted website which has a security symbol and statement, remember using unknown sources settings on your device may allow viruses into your computer.
- Use the most up-to-date version of the software and regularly check for further updates, these enhance security and improve functionality.
- A platform that uses video streaming rather then video recording is better for data protection and privacy as images and audio are not stored on the server.
- Platforms that use encryption techniques can increase security and privacy levels.

Preparation before the online meeting

- To reduce the risk of unauthorised access to a meeting the following can be used.
  - Send an email with the invitation link and a separate email with the password to invite participants to a meeting
  - Use multi-factor authentication function where it is available
  - A meeting invite link and or passwords should not be sent via social media
- The following controls reduce the risk of privacy breaches
  - Turn off all chat functions
  - Turn off all animation and sharing functions
  - Turn off the recording function
  - Create a waiting room to check the person was invited and allow entry to the meeting
  - Lock the meeting once it commences
  - Do not share or open URL links during the meeting
- Remind participants of data protection and confidentiality requirements of the meeting

During the online meeting

- The Host should manage the meeting and control the main functions:
  - The screen share function
  - Enabling or turning off participants audio and video where needed
  - Eject a participant from the meeting if their behaviour is not acceptable
- The Host should close the meeting and delete any data including history

General points that should be considered for online meetings

- Send out agenda and documents in advance of the meeting
- Advise participants of the meeting duration
- Have a short agenda, with timelines for each agenda item.
- Health and safety factors should be considered such as appropriate eye to screen distance, reducing the brightness of the screen, correct sitting posture, avoid long periods of watching a screen.
- It is good practice to have short and regular breaks during the meeting (5-minute break every 50 minutes).
- Use an appropriate space at home to respect the privacy of the meeting.

Key tips for online meetings:

- Use trusted software which has a high security rating
- Use strong passwords for meetings
- Use encryption options where available
- Don't share meeting links on social media
- Don't share personal data during online meeting
- Never share personal passwords or account details during the meeting
- Normal dignity and respect practices should be adhered to during the meeting.

Useful information and resources relating to the protection of data and security for online meetings can be found at:

Data Protection Commissioner, Tips for video conferencing
https://dataprotection.ie/en/news-media/blogs/data-protection-tips-video-conferencing

Health and Safety Authority, Guide for home working
https://www.hsa.ie/eng/supports_for_business/faq's_in_relation_to_home-working_on_a_temporary_basis_covid-19_/

National Cyber Security Centre - 12 steps to Cyber security
https://www.ncsc.gov.ie/

Garda National Cyber Crime Bureau - Secure Online Conferencing - 4'P's
https://www.garda.ie/en/about-us/specialist-units/garda-national-cyber-crime-bureau-gnccb-/garda-national-cyber-crime-bureau-gnccb-.html

If you have any questions about Data Protection send them to the
TUI Data Protection Office at dpo@tui.ie