Smarter Meetings with AI: Checklist Keeping Online Meetings Safe

Taking a Risk-Based Approach

Use the checklist below and any other relevant factors, to assess the overall risk to your organisation. Ensure that those running meetings are aware what the risk factors might be and know what steps they can take to increase security when appropriate to do so.

- **Cause.** We are all vulnerable, but some people are more likely to be attacked, such as our Jewish, Muslim and LGBTQI+ communities, and women's groups.
- **Communications.** If you have a significant profile online or in the media, you may be at higher risk.
- **Contributors.** The risk will be greater if there will be many people present or participants may be vulnerable, such as young people or.
- **Circulation.** If the meeting is open to anyone, particularly if it is being widely promoted.
- **Content.** The impact of a risk that occurs will be greater if the meeting content is sensitive.
- **Controls.** Not having adequate security is inherently dangerous but may also attract AI bots trained to seek out vulnerabilities.

Staying safe is not so much about detailed policies but creating and maintaining a safety culture.

Oversight & Meeting Management

- Choose secure platforms: Teams, Zoom or Google Meet with built-in safety features.
- Activate waiting rooms, meeting passwords, unique IDs—avoid public sharing.
- Assign a named individual or committee responsible for online safety.
- Provide host training in platform security settings and incident response.
- Require registration for webinars; for smaller meetings, share links only with confirmed participants.

Spotting Suspicious Registrations & Attendees

- Review registration details: look out for random characters or misspelled domains – mickeymouse@googgle.com.
- Encourage use of real names.
- Monitor for suspicious patterns: multiple registrations from similar names or emails, sudden spikes.

During the Meeting or Webinar

- Use waiting rooms to vet attendees.
- Only allow one approved AI note taker at a meeting.
- Restrict screen sharing to hosts/co-hosts only; disable annotations.
- Lock the meeting once all expected participants have joined.
- Assign co-hosts to monitor chat and participant behaviour.
- Watch for non-interactive attendees, disruptive comments, unusual audio/video patterns.
- Mute or remove participants showing suspicious disruption.

If the Meeting Is Compromised (Hacked)

- Remove offending participants immediately.
- Lock the meeting to block further entry.
- Mute all participants to regain control.
- Preserve evidence: note date, time, attendee names, chat logs, screenshots (avoid when illegal content is present).
- Do not screenshot extreme content that may be criminal in nature.

Afterwards: Incident Reporting & Review

- Report breach to platform provider (e.g. Teams support).
- Inform legitimate attendees of what happened and any protective steps taken.
- Conduct a security review: update settings and practices.
- Notify regulators if needed: ICO (personal data breach), Charity Commission, police or safeguarding bodies.

General Best Practice

- Keep all software up to date.
- Educate attendees not to share meeting links or passwords.
- Use strong, unique meeting passwords.

Help us to help everyone by sharing this with your network. Charity Excellence Learning: certificated, online AI courses that anyone can undertake.