scottishathletics

When using online video platforms such as Zoom, we recommend clubs use the increased security measures outlined below.

These measures are in addition to **scottish**athletics separate guidance on social media and digital communication practice available in the welfare section of our website.

Things to avoid:

1. Never publish your meeting password on a public forum/website
2. Don't click on any links that appear from a chat video (send them separately via email)
3. You should not accept any files via messenger or meeting forum tools
4. Don't assume that all Zoom meeting invites/links are safe. Verify this with the person that has sent you the invite
5. Never go to a meeting that doesn't have a password
6. Never go to a meeting on Zoom without a waiting room
7. Never give control of your screen to a third party
8. Don't accept any files from chat forums

Good practice:

1. Update the app when prompted
2. Always set up the meeting with a nine character password
3. Treat Zoom/Zoom Chat like a work tool and maintain professionalism at all times
4. When hosting a meeting always lock the meeting room once all known participants have arrived
5. Remove unwanted participants and prevent them from re-joining the meeting
6. Mute participants on entry of meetings
7. Disable video on entry of meetings
8. Enable waiting rooms to verify participants where possible
9. Encourage the use of; "Allow only signed-in users to join"

We hope you find this guidance useful and it enables you to stay safe online.