

There has been much debate here about Zoom and other technologies. I am a school governor and receive a regular safeguarding briefing, this week's contained some excellent advice which follows:

Safeguarding Briefing - 6th April 2020

Live Meetings with Zoom

One of my favourite programmes was Spooks. Seemingly capable of logging into anything, it was done speedily and without much thought. Hacking Zoom is the new reality. But it doesn't involve hacking. It just involves knowing slightly more than someone else. Like the cabinet office press releasing screenshots of a Zoom call clearly showing the meeting ID.

Zoombombing

Schools Week reports that an online conference of headteachers was 'zoombombed' last week and that shocking pornography was unleashed on the viewing leaders. This has been happening a lot.

I think that when we hastily set stuff up, we don't always think about the potential negative consequences. This is especially true of anything internet-related. If you have never live-streamed, there is a lot to think about. It's not like Spooks, or picking up a telephone.

Zoom is the market leader and like any market leader will attract more 'bad actors' than other products. In March, Zoom added 2.22 million users worldwide; in the whole of 2019, it grew by 2 million. In other words, more people joined over the last month than in the whole of 2019. I suspect many of those had never used a remote platform before.

Safer use of Zoom

From today (5th April 2020), Zoom are forcing users to password protect their meeting room. This is an important first step. Other things to do to protect your Zoom space are:

- Use a new meeting room each time (ie. don't use the personal meeting ID)
- Don't allow attendees to join before host
- Mute attendees on joining
- Turn screen sharing off
- Set up a 'waiting room'
- Lock your meeting room after you have started
- Don't publicise your meeting's link on social media
- Don't share the screenshot of everyone, especially when it shows the meeting ID
- Try to have someone whose job it is to 'manage the room' and focus just on doing that.
- Tell people what the Plan B is (ie. if you do have to abort the meeting where will the meeting move to and how can people rejoin)

Additionally,

- Avoid sharing personal information
- Turn off your video and microphone, unless it's needed.

Take time to learn about new tech

I'm quite tech-savvy, but it has taken a while for me to get to know the online tech tools, so I can do more work online. It takes trial and error, and rehearsal to get it right. It's not Spooks!

Above all, remember just because it can be done, doesn't mean it should be.

Where to find out more about using Zoom and other online technologies

My favourite online tech guy, Steve Dotto from [dottotech](http://dottotech.com), has some great videos about setting up and using Zoom.

In this video, Steve works with his wife, a teacher, to look at the main features of Zoom: <https://www.youtube.com/channel/UC9BqPtCcSyHvQsbl2rumM4w>

Do you already have tried and tested tech tools?

Head of Learning Technologies at Concero, Alan Foster, got in touch last week to remind me that many schools already have access to the technology they need.

Alan says, 'Teams and hangouts Chat are a great way for teachers to communicate with each other they can chat, share files, editable at the same time, do video conferencing or audio calls and all for free with Office 365 Education.

Welcome to Microsoft Teams

<https://support.office.com/en-gb/article/video-welcome-to-microsoft-teams-b98d533f-118e-4bae-bf44-3df2470c2b12>

Learn about the new Hangouts Chat (GSuite)

<https://www.youtube.com/watch?v=DvFZaljVpic>

There are lots of videos and articles on the web that can give you more information, above is just a very quick insight into Teams and Hangouts Chat. I hope this helps. If you require any further information let me know

The Concero Website is here: <https://www.concerouk.com/>

Andrew Hall

Specialist Safeguarding Consultant

Success In Schools Ltd.