Videoconferencing in Schools
Data protection and safeguarding considerations when using Teams and Zoom

Internal staff and governor meetings should be delivered over **Microsoft Teams**. There is no reason to use Zoom or other conferencing tools for internal meetings when all staff and governors have access to Office 365 and Teams.

Any meetings with **non-school / non-SCC staff (e.g. parents)** that may include **sensitive personal information** (such as **Team Around the Child** meetings) should be conducted using Teams.

In order to ensure personal details about participants in the Teams meeting are not shared with each other, schools should invite participants by emailing a link to the meeting **using BCC:**

- To access the link to a meeting, create the meeting, adding **only your own** email address to the list of required attendees. You will then receive an email containing the meeting link:

  Join Microsoft Teams Meeting

  This link can be copied and pasted into an email to all participants **using BCC**. Participants will not see each other's details in the email and will only be able to see each other's names during the meeting. No other details will be shared.

- In the invitation email, we would recommend including a phrase such as 'This link must not be forwarded to anyone else without the permission of the meeting host'.

- To use the lobby and ensure only hosts can present, set meeting options as below:

(Meeting options can be accessed by double clicking the meeting in your Teams calendar, then clicking the Meeting options icon at the top of the window.)

When participants follow the link to the Teams meeting, they will be placed into a lobby, where only the meeting host(s) can allow them to join.

Videoconferencing in Schools
Data protection and safeguarding considerations when using Teams and Zoom

When holding meetings that will **not** include the sharing of sensitive personal data or lessons with students or families who do not have access to Office 365 and Teams, schools **may** be considering Zoom. There are **procedural, safeguarding and data security** issues that must be addressed.

Procedures:

- Every Zoom meeting should be **documented** – keep a spreadsheet of the meetings that were held, with whom, for how long, and for what purpose.
- Follow this advice on safely setting up a Zoom meeting here https://www.theverge.com/2020/4/17/21196104/how-to-keep-your-zoom-meetings-safe-security-privacy
- Have a **very specific focus** e.g. annual reviews or music therapy. Staff can't set up Zoom meetings without SLT authorisation – this exposes them to higher levels of risk and must not be allowed.
- When you've got the focus, then **communicate with parents** about it, and explain that you will be using Zoom for a specific activity, at this time, on this day. Give them the option to include their child if they wish, by sending the school their email address (do all of this communication **through a school email account**). This is securing their consent.
- In the communication to parents, explain that the staff member, as host, will consider **safety features** e.g. muting webcams and microphones if there are any concerns about what pupils are discussing, and **locking the meeting five minutes after the scheduled start time** (to avoid zoombombing!). The **parent should be in the same room** as their child during the Zoom session. Pupils must be presented as if they are in the classroom, and if the teacher thinks the pupil is inappropriately dressed, they should remove them from the session.

Safeguarding:

- Remind staff that there should be **no direct communication between the teacher and pupils** outside of the Zoom meeting - all communication is between the parent and teacher. Secondary settings may consider adapting this based on the maturity of their learners, but all communication must be open and transparent.
- The Zoom session should be delivered on a Somerset County Council laptop (**avoiding personal devices**) and the staff member should set up a new Zoom account using an SCC email address. – not their personal email address.
- In the invitation to the meeting, we would recommend including a phrase such as 'This link must not be forwarded to anyone else without the permission of the meeting host'.
- No Zoom sessions with pupils should be recorded by staff **unless the school considers there is a safeguarding risk** or concerns about content/conduct – this **must** be discussed

with SLT.

- All staff undertaking such lessons are expected to be **appropriately dressed** and in a room which doesn't have continuous distractions.

- The staff member should be aware that **any safeguarding concerns or disclosures** should be responded to and reported in the same way as they would if they had occurred in the school.

Data security:

- After the session, staff should **delete their session cookies** to avoid any data mining from Zoom.

Important note:

A parent or child may record a Zoom videoconferencing meeting, without the knowledge of the meeting host. If they do record the meeting, this is not considered a data protection breach as they are acting in a *'personal and domestic'* capacity and are exempt from the General Data Protection Regulation.

However, if they redistribute the recording e.g. by uploading it to YouTube, this may be considered a risk to the safety of pupils or staff. If you become aware that a parent has redistributed the Zoom meeting, contact the Professionals Online Safety Helpline **0344 381 4772** https://www.saferinternet.org.uk/helpline/professionals-online-safety-helpline