

Using Zoom safely

To ensure that your governing body meeting is not restricted by the 40-minute time limit, Zoom has temporarily lifted the restriction on free Basic accounts for schools affected by the Covid-19 – go to

<https://bit.ly/2YtUgV0>

1. To avoid unwanted intrusion (Zoombombing) and to ensure that you have the best possible security, **always password protect** your invitation to the meeting which will then be required by all your attendees to be able to access the meeting
2. When setting up the meeting, tick the box where it says that you **do not allow others to join the meeting before you as the host**; this will then ensure that only those who are authorised attendees may join from the Waiting Room; this is a particularly useful option if you are using Zoom, for example, for interviews as you then have greater control of who and when attendees join the meeting.
3. If you are really concerned about security, **you can 'lock' your meeting** by heading over to 'Manage Participants' once you are confident everyone has arrived, click 'More' and choose 'lock' and this will prevent anyone else from joining the meeting
4. Screen sharing is an excellent tool but it also could allow a Zoom bomber to share inappropriate information. If you consider this a concern, **you can disable the screen share option** for attendees to share their screens via the Security tab.
5. Always ensure that you do not use your personal meeting ID but choose the option for a **randomly generated ID**
6. Should your meeting be disrupted by an unexpected and uninvited attendee, you can essentially kick them out by going to the Participants' tab, click on 'More' and remove them – if this is serious Zoombombing, you can ensure that they cannot return by disabling 'Allow Removed Participants to Rejoin' under 'Settings: Meetings – Basic' tab
7. Regularly check for **updates** – these should usually happen when you log in for a meeting