Safeguarding Statement from THE CHURCH OF ENGLAND

ZOOM

You may be aware in the news of Zoom meetings being hijacked by an anonymous person(s) and then being able to share inappropriate content to the audience. We have reviewed the recommended changes to be made to our Zoom environment which we've applied with immediate effect. I've listed and highlighted these in yellow below. I've also pasted some guidelines on what best practices to follow.

- **Do not make meetings or classrooms public. In Zoom, there are two options to make a meeting private: require a meeting password or use the waiting room feature and control the admittance of guests. This has been switched on now and should come into effect immediately.**
- **Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post. Provide the link directly to specific people.**
- **Manage screensharing options. In Zoom, change screensharing to "Host Only."**
- **Ensure users are using the updated version of remote access/meeting applications. In January 2020, Zoom updated their software. In their security update, the teleconference software provider added passwords by default for meetings and disabled the ability to randomly scan for meetings to join. The latest app is being installed and reported by Zoom.**
- **Lastly, ensure that your organization's telework policy or guide addresses requirements for physical and information security.**

National Safeguarding Team
The Archbishops' Council, Church House
Great Smith Street, London SW1P 3AZ