Sheffield Hallam University

Guidance on Using Zoom for Collecting Research Data

This guidance has been produced after consultation with DTS. Zoom can be used for research by staff and students as long as some sensible precautions are taken. These should be followed to ensure the most secure use of Zoom for collecting research data.

1. Ensure that data is not stored within Zoom. This is **crucial.** To do this :
   a. Turn off participant screen sharing so Zoom is not used to share or exchange files.
   b. Ensure that any meeting recording is **not s**aved to the cloud. To do this, the host researcher will need to make sure the recording file is saved to the researcher's local PC then treated securely as with any other piece of research data with respect to retention and deletion.
2. Do not show meeting ID numbers on the subject lines in e mails.
3. Do not share personal ID in any public forums including social media.
4. Use the dedicated security tab to change security settings for hosts and meeting attendees.
5. Password protect any meetings and require the password when scheduling meetings that participants have to use to join the meeting.
6. Do not allow others to join a meeting before the host arrives - this can be set in the account settings.
7. Use a waiting room feature to screen participants before they join the session
8. Lock down meetings by using the 'manage participants' tab to prevent others from joining without invitation.
9. There is a feature in settings to permanently remove nuisance participants.

Microsoft Teams
In future it is expected that Microsoft teams will be able to fulfil the needs for staff researchers but it is not ready just yet. It is unlikely to meet student researcher needs as although students have access to it, they cannot use it to set up meetings which will prevent them from using it to contact people outside the University.

UREC, October 2020.