**Zoom User Security Guidance**

**Background - Security Concerns**

The current main concerns of Zoom usage have been identified as:

* If settings are not applied correctly then uninvited members of the public are accessing meetings and causing disruption which is known as ‘Zoombombing’. Users would not necessarily be made aware of any uninvited attendees that had accessed the meeting;
* According to technical experts, over 500,000 accounts have been hacked and account details have been sold on the dark web;
* The host of a Zoom call has the capacity to monitor the activities of attendees while screen-sharing;
* Zoom allows account/meeting administrators to see detailed dashboards of users' activity, including a ranking system of users based on total number of meeting minutes. They can also see the operating system, IP address, location data and device information of each participant;
* There is an apparent issue with email addresses in the same domain being added to a ‘company’ folder where users can see each other’s information;
* Captured data (including Voice recordings and meeting attendees email details) is held by Zoom in data repositories in China and USA. According to sources, it has proven incredibly difficult for anyone to obtain their data which contravenes the ‘Right of Access’ in the General Data Protection Regulation (2018). In a recent change Zoom have confirmed paid account members are able to choose the region their data is routed through;
* If any user records any calls via Zoom, account/meeting administrators can access the contents; and
* Local recording is available to free and paid subscribers (but is not supported on iOS and Android). Local recording allows users to record meeting video and audio locally to a computer. The recorded files can be uploaded to a file storage service like Dropbox, Google Drive, or a streaming service like YouTube or Vimeo. If a meeting is recorded, then a consent notice is supplied to the attendees on entry to the meeting.

**Guidance Arrangements:**

The following section sets out guidance on how to ensure Zoom is used appropriately, identifying where specific actions **must** be followed in order to ensure security and safeguarding arrangements around its use.

**Passwords**

There have been cases where hackers have obtained access to users’ passwords in order to sell account details on the ‘dark web’.

You **must** ensure a completely different password is used for logging into Zoom than you have used for logging into other accounts or services.

**Security Settings**

To assist in reducing the risk of security breaches, you must ensure that the right security settings are correctly applied.

**Hosting a Meeting**

When hosting a meeting you **must**:

* Not share the meeting ID on public forums under any circumstances.
* Not share your personal meeting ID with other individuals unless appropriate, as this allows access to your virtual area at any time. An example of an appropriate sharing of your personal meeting ID is with your personal assistant.
* Stop participants ‘**screen sharing**’ by:
	1. clicking on the arrow next to ‘Share Screen’ in the host controls at the bottom of the Zoom screen; then
	2. select ‘Advanced Sharing Options’ and make sure the option to ‘Who Can Share?’ is set to ‘Host Only’.
* Enable the ‘**waiting room**’ feature by:
	1. going to ‘Account Management’;
	2. select ‘Account Settings’;
	3. select ‘Meeting’; and then
	4. select ‘Waiting Room’. More information can be found here - <https://support.zoom.us/hc/en-us/articles/115000332726>
* Turn off ‘**file transferring**’ by:
	1. going to ‘Account Management’;
	2. select ‘Account Settings’;
	3. select ‘Meeting’; and then
	4. select ‘File Transfer’.

**Setting passwords for meetings and webinars**

Passwords can be set at the individual meeting level or can be enabled at the user, group, or account level for all meetings and webinars. Account Owners and Administrators can also lock password settings, to require passwords for all meetings and webinars on their account.

When setting up a meeting for discussing:

|  |  |
| --- | --- |
| * personal information:
 | * You **must** set a password for the meeting at the ‘meeting’ level.
* This password **must** be shared with those invited to attend via a separate email to the one sent containing the meeting link.
* Each meeting **must** have a different password to the one used on a previous meeting and must not be a sequential approach (e.g. ‘meeting1’ for the first meeting and then ‘meeting 2’ for the next and so on)
 |
| * business sensitive information:
 | * Same as for ‘personal information’ (see above).
 |
| * non-personal and non-business sensitive information:
 | * If a password is set, it should be shared with those invited to attend via a separate email to the one sent containing the meeting link.
 |

**Recording Meetings**

The ability to record to the cloud or locally is something an Account Administrator can control. If they have recording access, the host can decide to enable/disable a participant or all participants to record.

If a meeting is being recorded in Zoom, the host should have setup a pop-up notice to attendees informing them that a recording is taking place. There is also possibly a visual indicator that appears when recording is on if the host has enabled this function. Good practice and potential compliance with Data Protection legislation (depending on the purpose of the meeting and type of information being disclosed), should mean these things have been put in place but there is no guarantee.

**Further Information**

More information about ‘pre’ and ‘during’ meeting settings can be found via the following link:

[Privacy & Security for Zoom Video Communications](https://zoom.us/docs/en-us/privacy-and-securi-ty.html?zcid=3747&creative=431306240822&keyword=zoom%20security&matchtype=e&network=g&device=c&gclid=EAIaIQobChMIotnrzrfv6AIVQ7DtCh15zgENEAAYASAAEgIuxfD_BwE)