**Guidance on Zoom based Research**

The use of Zoom, a virtually cloud-based platform to conduct research has become rampant. This online tool is popular with researchers who use it to collect data primary through interviews and other types of virtual communications. There are risks to privacy and confidentiality and this guidance document will provide steps to mitigate those risks.

Privacy and Security:

* Create an account through UCM and register your profile and access the platform through Single Sign-on.
* Consult UCM IT for additional security and privacy measures.
* Limit research interactions that collect highly sensitive data as the portal may have access to any audio or video collected on Zoom.
* Disable screen-sharing. To avoid by default, anyone entering a meeting and automatically sharing their screen with the group.
* Zoom’s encryption policy information. Although others will not be able to access any audio or video content created from your encrypted meeting, this information is not private from Zoom itself. Please make sure your participants understand this.
* Use a meeting password. By using a password, only those with the password can enter your meeting. Although the password function can be turned off, all researchers are expected to use this feature.
* Turn on waiting rooms. For smaller meetings, turn on waiting rooms in the settings. The host must approve each new attendee prior to them having access to the meeting room.
* Please use UCM approved method of transferring files between the research team and research participants and not Zoom. Disable this function in settings. This is highly recommended, so participants do not accidentally share confidential information.
* Lock meetings. Once all participants have entered the meeting, the host can lock the meeting which will not allow anyone else to join.
* Limit research interactions that collect highly sensitive data as Zoom may have access to any audio or video collected on Zoom.
* Limit the use of the Record function. Recording sessions presents additional security and privacy risks when not handled properly. Only use this function when necessary and explicitly state that to your participants when sessions will be recorded.
* When using the Record function, always record to the computer. Please refrain from recording to the cloud. All recorded meetings should be saved to the computer and then promptly transferred to secure storage (e.g., UCM Box) and immediately deleted from the computer.
* When using Record function, please be sure that all participants consent. The meeting room should require permission and/or alert participants that they are being recorded, and researchers should verbally consent participants prior to recording any session. No participants should be recorded that have indicated they do not want this function used.

Including details in the Protocol –

* + - * Provide details on the Zoom procedures such as who will have access to the meeting password. A new link and a new password should be generated for each participant.
      * Describe the way participants will be provided the opportunity to consent to the creation and use of Zoom recordings.

Additional considerations for Informed consent –

* Privacy and Confidentiality – State how long recordings will be stored, and how recordings will be protected.
* A statement that the recordings are subject to [Zoom’s privacy policy](https://explore.zoom.us/en/privacy/). Participants should be linked to the policy.