Guidelines for Using Zoom (REB section 4)

4.1.2 (Can be used verbatim)

Zoom ensures the security of the communication amongst all participants through encryption of data in transit and at rest, and meets industry and security organization standards (SOC 2; FedRAMP; GDPR,CCPA, COPPA, FERPA, and HIPAA; Privacy Shield Certified; and TrustArc Certified Privacy Practices and Statements). The University of Regina uses a Canadian-located data centre for its Zoom real-time meeting traffic.

4.1.3 (Can be used verbatim)

All University of Regina researchers have permission to use Zoom through the University’s license.

4.1.4 (Can be used verbatim)

Each Zoom participant, will be given a randomly generated unique meeting ID number and passcode. Participants will enter a waiting room where the principal investigator will admit them to the meeting. The meeting will be subsequently locked to prevent anyone else from joining the meeting once the interview begins. All recordings will be stored on the primary researcher’s host device which is password-protected (and not to a Zoom cloud server).

Suggested wording for the Consent form:

The online interviews will be held via Zoom, an online video / audio meeting software service. You do not need a Zoom account to join meetings as a participant. Access to the meeting space is secured using a unique meeting ID number and passcode. A link, containing the meeting ID and passcode, will be provided to you by the host. Following the link will open your web browser, or an installed version of the Zoom desktop or mobile client (see https://zoom.us/download), and take you to the virtual meeting. The meeting ID and passcode will also be sent to you, and you can enter that information directly into the Zoom web interface (at <https://zoom.us/join>) or the installed Zoom client. Note that some organizations restrict access to Zoom, in which case an alternative arrangement will be required.

Note to Researchers:

* Please see <https://support.zoom.us/hc/en-us/articles/4423182002317-Joining-a-Zoom-meeting-without-an-account>. The host must edit their settings to allow Show a "Join from your browser" link for a participant to do this. See <https://zoom.us/profile/setting>
* Please make sure to adhere to Zoom guidance as follows: <https://www.uregina.ca/is/security/advisories/security-advisory57.html>

Method considerations with Ethics Implications:

TCPS-2 Article 4.1: Inclusion

* Not everyone has access to technology or an adequate comfort level to use technology

TCPS-2 Article 3.12: Consent

* While, in some cases, it may be acceptable to provide the consent form to the participant over email; however, please note, there are inherent security issues when using email as a communication tool. By default, emails are not encrypted and are thus vulnerable to interception by outside sources. In order to avoid possible violations to the anonymity of the participant (e.g., if they leave their browser open and someone else sees), in the consent form please identify a phrase that does not reflect a research project (e.g., Zoom Guidance) that you will use in the subject line in all email communications. It is not recommended that the participant return a signed consent form via email. Alternatively, please consider obtaining oral consent during the scheduled Zoom meeting.
* We recommend language should be added to the recruitment material and/or consent form like: “There are inherent security issues when using email as a communication tool. By default, emails are not encrypted and are vulnerable to interception by outside sources or someone may see that you are involved in this research if you leave your browser open. We will use the term/phrase XXX in the subject-line of all email correspondence so you will know the email is from us and recommend you submit any email queries using the same term.”
* Be clear whether audio and/or video recording or both and obtain consent (see section below on Recording)
* Pre-registration for Zoom webinar/focus group including consent:
  + There is the possibility of presenting a consent form to participants for a focus group.
  + A secure webinar account is needed.
  + Choose pre-registration and you can input the text of your consent form in the pre-registration prompt area
  + When participants pre-register the consent form is visible and when they pre-register they provide consent.
  + NOTE: According to TCPS Article 3.1b (<https://ethics.gc.ca/eng/tcps2-eptc2_2018_chapter3-chapitre3.html>) participants are still entitled to their agreed upon one-time honorarium/gift card if they choose to withdraw their information after consenting to participate. So, if they don’t attend the focus group, they are still entitled to the compensation. It is recommended that the consent form state that consent will be revisited (orally) and final consent will be obtained at the actual focus group. If participants choose to withdraw during the actual focus group or after, compensation will still be provided.

TCPS-2 Article 5.1: Privacy and confidentiality

* The technology adds identification of the individual (user name appears under the image). The host can change or delete this if it is a concern; though the participant can override the change.
* Ask participants to participate in a confidential space where their responses cannot be overheard
* As a researcher, conduct the interview in a confidential space where the participant’s responses cannot be overheard; consider wearing a headset so no one can inadvertently hear the interview
* Possibly scan the space around you to ensure the participant that no one else is in the room or could enter while conducting the interview
* Give participants the option not to turn on their camera or to use a background scene

Recording

* Please be clear on the consent form whether you are audio and video recording or just audio recording. Please note, local recordings will always create a video and an audio file. There is currently no way to allow audio only recording for local recordings (see https://zoom.us/profile/setting under “Recordings).
* The only way to assure someone that their image is not being recorded is to turn the cameras off so that the video file is only recording the black screen with the user’s name and their profile picture if they have one.
* If you are using the record feature on Zoom (with the participant’s permission), you should select “Record on this Computer” not “Record to the Cloud” or disable the Cloud recording (instructions below). See below for the rare circumstance where a researcher is allowed to save recordings to the Zoom cloud.
* Consider deleting locally-stored audio and/or video recordings once transcription is complete.

Disabling Cloud Recording

* Since it is not readily apparent how to do disable the Cloud recording option, the following instructions are provided.
* To disable Zoom cloud recording (<https://support.zoom.us/hc/en-us/articles/203741855-Cloud-recording>), please have each user:  
  1.Sign in to the Zoom web portal.  
  2.In the navigation panel, click Settings.  
  3.Navigate to the Recording tab and verify that the Cloud Recording setting is DISABLED.  
  Each user who is conducting interviews should configure this to disable cloud recording.
* Once this is done, local recording can be enabled using these instructions: https://support.zoom.us/hc/en-us/articles/201362473-Enabling-and-starting-local-recordings

Transcription

* If the interviews are to be transcribed, who will be doing this? If not the PI, is this clear on the consent form? If not the PI, how will the data be transported to the transcriptionist? Will transcripts be forwarded back to participants for review, and if so how will confidentiality be maintained through this process? Because email is not a secure mode for data transfer, it is recommended that you use a password protected file to communicate with the participants and/or transcriptionist. Please make sure to send the password in a second email or consider sharing a secure FILR folder. Also, ensure that no group emails are sent to the participants (use BCC) and that the emails will be securely stored separately from the data.
* Zoom software connects to IP attendees’ addresses and details might be shown. Please see : [https://support.zoom.us/hc/en-us/articles/360039017432-Dashboard-for-Meetings-and-Webinars#h\_40249173-6f00-4b05-ba09-03567d1b120f](https://support.zoom.us/hc/en-us/articles/360039017432-Dashboard-for-Meetings-and-Webinars" \l "h_40249173-6f00-4b05-ba09-03567d1b120f)

Producing an Automatic Transcription while Locally Recording

* To produce an automatic transcript of the Zoom session (this can be done regardless of whether the session is recorded locally or not; n.b., if “Record to the Cloud” is selected, an audio transcript is automatically created):

1. Under Settings on the Zoom website, (https://zoom.us/profile/setting), navigate to the Meeting tab. About ¾ down the page, under “In Meeting (Advanced)”:
   1. Enable “Automated captions”
   2. Enable “Full transcript”
   3. Enable “Save captions”

These settings will allow you to generate a live transcript that you can save to your local computer.

1. After starting the meeting, you can generate an automatic transcription of the interview (with the participant’s permission) by selecting “Live Transcript” from the in-meeting control panel, then “Enable” “Live Transcription”. Any participant can then hide or show subtitles, and view or close the full transcript.
2. You must select “Save Transcript” at the conclusion of the interview and before selecting the “End” meeting button. Do not end the meeting until you are certain the transcript has been saved. If in doubt, you can copy the full transcript and paste it in another document. If a meeting is ended before the transcript is save, the transcript cannot be recovered.
3. The automatic transcript can be used as the basis for preparing a corrected transcript with the aid of the recording.

TCPS-2 Article 6.12: Risk

* Be cognizant of potential for “Zoom fatigue” if participant is in an occupation that spends a lot of time during the day on Zoom.

Saving to the Cloud

* In rare circumstances, researchers are allowed to “Record to the Cloud”.
* In these situations, researchers are instructed to download all files (video, audio, and audio transcript) from Zoom onto a secured device (e.g., personal password-protected computer, UofR Filr storage) and immediately delete the recordings from the Cloud.
* However, the deleted recording remains in the Trash for 30 days (see Figure 1).

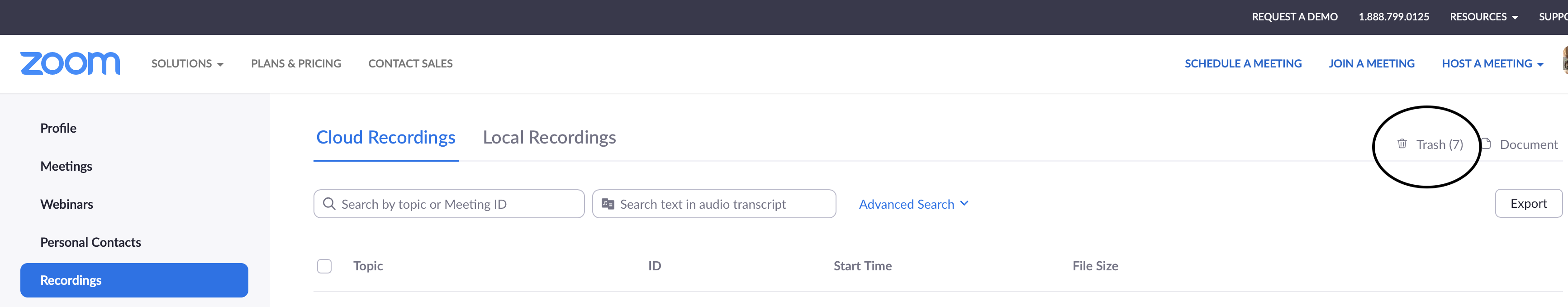


Figure 1.

* Please ensure that you click on the Trash icon, and empty the trash from that folder (see Figure 2)

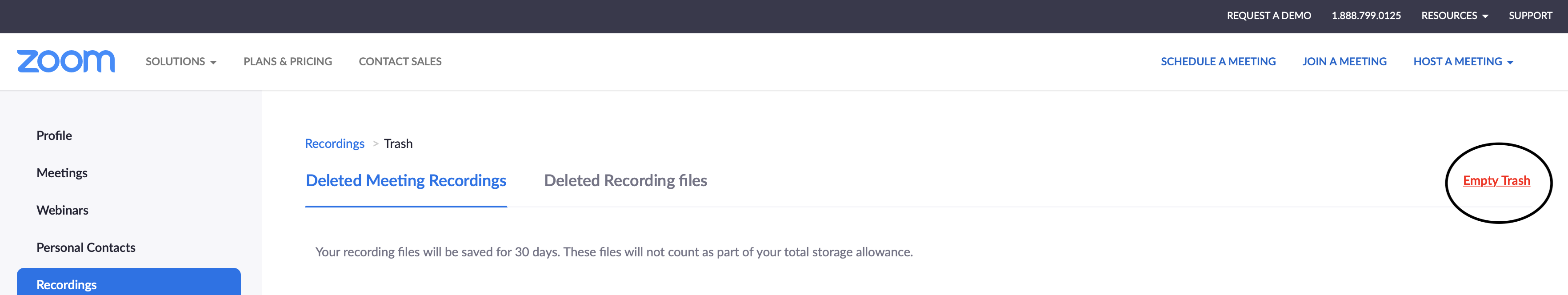


Figure 2