# **Virtual Research Guidelines**

While we have provided the following guidance and suggestions for how to approach virtual interactions, different approaches can still be used, provided the privacy and security details of the approach can be justified. If you have any questions about your virtual research plan, contact the IT Support Centre at (613) 533-6666 or by filling out the Online Help Form. For the most up to date information about Connecting and Collaborating Remotely visit Queen’s ITS.

**Jump to:** [Consent](#_Informed_Consent) [Virtual Platforms](#Virtual_Platforms) [Incentives](#_Sending_Incentives)

## **Informed Consent**

1. **Health Canada and/or US Regulated Research**

* It is Health Canada's recommendation that all efforts be made for the process of discussing and obtaining informed consent be done in person but if that is not possible, an alternate approached can be considered (e.g., over telephone/Zoom/Teams/telemedicine).
* The method used must be documented in the site's Informed Consent SOP, along with a valid rationale and justification for its use submitted to the appropriate REB.
* The new process must be cleared by the REB before implementing the new process.
* For regulated studies:
* A witness who signs the LOI/CF, should be present with the participant during the informed consent process, regardless of the method of communication.
* You must confirm research participant identity.
* At the first in-person visit, participants should bring the original signed LOI/CF that was previously discussed remotely. At this time, person who conducted the remote discussion should sign and date the original LOI/CF that was signed by the participant during first virtual (alternative) visit.
* A copy of the signed LOI/CF should then be given to the participant and the original should be filed as per record retention requirements.
* COVID-19 guidance documents can be referenced below for **Health Canada, FDA, and the Office for Human Research Protections (OHRP):**

1. [**Health Canada - Management of clinical trials during the COVID-19 pandemic: Notice to clinical trial sponsors**](https://www.canada.ca/en/health-canada/services/drugs-health-products/drug-products/announcements/management-clinical-trials-during-covid-19-pandemic.html)
2. [**FDA Guidance on Conduct of Clinical Trials of Medical Products during COVID-19 Public Health Emergency Guidance for Industry, Investigators, and Institutional Review Boards**](https://www.fda.gov/regulatory-information/search-fda-guidance-documents/fda-guidance-conduct-clinical-trials-medical-products-during-covid-19-public-health-emergency)
3. [**OHRP Guidance on Coronavirus | HHS.gov - Research Guidance on Coronavirus**](https://www.hhs.gov/ohrp/regulations-and-policy/guidance/ohrp-guidance-on-covid-19/index.html)

### **Standard Canada Post Mail or alternative secure mailing service (e.g., UPS)**

### **Email**

* Send a blank Letter of Information (LOI) to participants through email.
* You must include a statement within the email indicating that participants should **NOT** return a signed copy through email or email personal or sensitive information.
* You should use an institutional email address, not a personal email address.
* Use an alternative way to obtain informed consent (e.g., verbal, implied, survey response, waiver).
  + **We prefer that participants do not return signed consent forms through email** as this can be an added burden to participants due to the extra security steps required. One of the alternative options below is preferred.
  + If you plan to use this method, you must detail the secure file transfer process and directions that participants will be given
  + Participants must encrypt their signed consent form with a password.
  + The password to the encrypted document must be sent in a separate email, with a subject line that does not indicate that it contains the password.

### **Queen’s** [**OneDrive**](https://www.queensu.ca/its/microsoft-office-365/onedrive-business) **for Business**

* Create a folder where the LOI/CF is available for view/download/upload.
* If this is a secure private folder, the participant could enter their name and date indicating consent or upload their signed version to this secure location **OR** use an alternative way to obtain informed consent (e.g., verbal, implied, survey response, waiver).

### **Webpage**

* Create a secure webpage for the research study where participants can view and/or download a blank version of the LOI. You must find an alternative way to obtain informed consent (e.g., verbal, implied, survey response, waiver).

### **Survey using** [**Qualtrics**](https://www.queensu.ca/planningandbudget/surveytool) **(Queen’s preferred survey platform)**

* Provide a link to access the LOI online at the start of a survey.
* Obtain consent as the response to question #1 **OR** the LOI explains the completion of the survey implies consent.

### **Through your Recruitment Material**

* Participants can click on a link in the recruitment information (e.g., recruitment email, Facebook link, Twitter, etc.). You must find an alternative way to obtain informed consent (e.g., verbal, implied, survey response, waiver).

### **Verbal Consent**

* If you will be using verbal consent (e.g., through a telephone call or virtual meeting), ensure that you attach a [verbal consent LOI](https://www.queensu.ca/vpr/sites/vprwww/files/uploaded_files/Ethics/HSREB%20Verbal%20Letter%20of%20Information%20and%20Verbal%20Script%20Template%202020JUL28%20FINAL.docx) and [verbal consent log](https://www.queensu.ca/vpr/sites/vprwww/files/uploaded_files/Ethics/Verbal%20Consent%20Log%20Template%202020FEB06.docx) to your ethics application OR indicate how you will be capturing this information (e.g., use of audio/video recording).

## **Virtual Platforms**

### **Queen’s Microsoft Teams**

[Microsoft Teams](https://www.queensu.ca/its/microsoft-office-365/teams) is Queen’s preferred platform. Indicating in your ethics application or amendment that you will be using Microsoft Teams as your platform provides sufficient information on the privacy and security of this platform for the REB. If you will be recording the session, ensure that you inform the participants in the LOI/CF and at the beginning of the virtual session.

Queen’s ITS recommends these best practices to protect your Teams meetings:

* [Be prepared](https://www.queensu.ca/its/microsoft-office-365/teams/tutorials/meetings-teams#beprepared) – know the meeting options and settings prior to your virtual meeting
* [Keep meeting join information private](https://www.queensu.ca/its/microsoft-office-365/teams/tutorials/meetings-teams#privatejoin) - do not share on social media or public websites
* [Control access](https://www.queensu.ca/its/microsoft-office-365/teams/tutorials/meetings-teams#controlaccess) – learn to manage the meeting lobby to prevent uninvited guests from attending
* [Prevent users from taking control of the meeting](https://www.queensu.ca/its/microsoft-office-365/teams/tutorials/meetings-teams#preventcontrol)
* [Limit screen sharing](https://www.queensu.ca/its/microsoft-office-365/teams/tutorials/meetings-teams#limitscreenshare)
* [Restrict chat](https://www.queensu.ca/its/microsoft-office-365/teams/tutorials/meetings-teams#restrictchat) to members of your Team
* Visit Queen’s ITS [Meetings in Teams page](https://www.queensu.ca/its/microsoft-office-365/teams/tutorials/meetings-teams#protectmeetings) for an overview of best practices and detailed tutorials for how to protect your Teams meetings.

### **Queen’s Zoom Education Account**

Queen’s University students, staff, teaching assistants, and faculty with an active NetID@queensu.ca email address are eligible for [licensed Zoom Education accounts.](https://www.queensu.ca/its/zoom) If you will be recording the session, ensure that you inform the participants in the LOI/CF and at the beginning of the virtual session.

Queen’s ITS has released the following recommendations when using Zoom:

* Avoid sharing meeting links on social media or public outlets
* Avoid using Personal Meetings ID (PMI) to host public events- Your PMI is a persistent meeting room and people can pop in and out all the time
* Manage Screen Sharing - To prevent random people from taking over sharing, restrict sharing to the host
* Manage Participants
* Lock the meeting - By locking the meeting after the meeting has started, no new participants can join
* Remove unwanted or disruptive participants
* Disable video – Hosts can block unwanted, distracting, or inappropriate gestures on video
* Mute participants – Hosts can block unwanted, distracting, or inappropriate noise from other participants
* Introduce a Waiting Room – The Waiting Room is a virtual staging area that stops your guests from joining until you are ready for them
* For more information about protecting your Zoom meetings, visit the [Zoom security website](https://zoom.us/security)

### **Alternative Platforms**

Virtual interactions that are proposed on an alternative platform (e.g., Skype, DocuSign®, FaceTime, GoToMeeting, Zoho, etc.) must include information about the privacy and security details of the chosen platform. If you will be recording the session you must inform participants in the LOI/CF and at the beginning of the virtual session.

* These questions can be used to help assess and mitigate the risk based on the specific virtual platform derived from Queen’s ITS [Authorization to Operate](https://www.queensu.ca/its/security/security-services/authorization-operate) page under ‘What should you consider?:
  + What type of data will be collected, used, stored, and processed by you and by the vendor and [How sensitive is it](https://www.queensu.ca/its/security/policies-and-procedures/data-classification-standard)?
  + Who will have access to the data, and how can we confirm this?
  + Does the vendor claim the right to use the information for its own, secondary purposes?
  + Where does the vendor operate and/or store the data and what laws govern data in that jurisdiction? Are those laws comparable to Canadian privacy laws?/GDPR/US Regulations?
  + Is access to personal information limited and restricted to authorized individuals?
  + What controls does the vendor have in place for intrusion detection, perimeter security, physical security, application of security patches, and data-leak prevention, among other safety measures?
  + What policies and procedures are in place to detect, prevent, and mitigate identity theft?
  + How are incidents and breaches reported?
  + Will we receive notification if a breach to our data occurs?
  + Can the data be retrieved and/or permanently deleted from the vendor’s systems and servers?

## **Sending Incentives/Confirming Receipt of Incentives**

1. **Standard Canada Post Mail or alternative secure mailing service (e.g., UPS)**
2. **Cellular Text Message/Automatic Notification**
3. [**Qualtrics**](https://www.queensu.ca/planningandbudget/surveytool)
   * Link at end of survey will take participants to a second survey where participants can enter their information for compensation (e.g., email, student information for credit).
4. [**OneDrive**](https://www.queensu.ca/its/microsoft-office-365/onedrive-business)
   * Participants are provided with the link to a secure private folder with the receipt document. Participants can edit the document to insert their initials indicating they have received incentive.
5. **Email Confirmation with secure file transfer as applicable**

### **Documenting Incentives**

Documentation of payments to research participants is mandatory as per Queen’s [Payments to Research Study Participants](https://www.queensu.ca/secretariat/policies/finance/payments-research-study-participants/) policy.