McMaster Research Ethics Board
Ethics Considerations for Conducting Online Research
Part I. Surveys and Experimental Tasks

1.Recruitment

Whether you are recruiting for your online study using the McMaster SONA system, social media, email, a crowdsourcing platform (e.g. Amazon MTurk, Crowdflower, Prolific) or some other means, the following is essential information about your study that should be provided at the recruitment stage:

- Names and affiliations of the researchers
- A brief statement outlining what participants will be asked to do (e.g. questionnaires, online tasks, watching videos, writing, playing games), what platform will be used (e.g. a website, an online survey tool), what type of tasks or questions will be asked -- e.g. will there be any sensitive or personal topics such as mental or physical health or income that might be probed in the course of the study?
- Any inclusion/exclusion criteria. State whether there is a pre-screening test to qualify for the study.
- Note any special software or computer requirements the participant must have to complete the study (e.g. javascript, audio, video camera)
- Clearly and accurately state how much time is required
- Incentive Payment: how much, in what form, and how will it be delivered.
- A statement of how participants can learn about the full details of the study, i.e. how will they receive the letter of information, and how they can have their questions answered if applicable.

2.Letter of information and study preamble

The letter of information (LOI) gives full details of the online study (link to LOI template). It is generally recommended that participants receive a copy of the LOI in advance so they have the time to read the details and consider any questions they may have. This may be required by MREB for studies with multiple parts or some risk.

During recruitment, the LOI can be included as an attachment to the recruitment email or via a link in a recruitment webpage/online posting.

The full LOI must be presented to participants immediately prior to taking part in the online study. The entire text of the LOI could be displayed on the landing page (the first page that appears in the online study) prior to asking consent questions. Alternatively, a shorter study preamble could be presented that includes a link to the full LOI. For online studies with higher risk, MREB may require the entire text of the LOI option.

In cases where a shorter preamble is linking to the full LOI, some basic information is still required in the preamble (link to template):

- Names and affiliations of the researchers
- A brief statement outlining the purpose of the study and what participants will be asked to do
- Any inclusion/exclusion criteria.
- Clearly and accurately state how much time is required
- Incentive payment: how much, in what form, and how will it be delivered.
- Any risks (e.g., privacy, becoming upset, etc.) and steps taken to mitigate risks (e.g., skip any questions that make them uncomfortable, list of supports available and list how it can be accessed)
- How they can withdraw from the study or skip questions.
- A statement informing participants they can view the LOI for full details, along with a link to the LOI.

3.Consent

Consent in online studies can be handled in a number of ways. Most commonly, online studies embed consent questions directly on the landing page of the online survey or study with clickable options such as "I agree" or "I do not agree".

Alternatively, if the participant is interacting with the researcher via phone or email prior to their participation, or there is a video component to the study, they could use other means such as:

- The participant downloads, prints, signs, scans and emails back the signed consent form to the researchers. This method places a rather large burden on participants.
- The participant emails you a simple statement confirming they have read the LOI, had their questions answered, and agree to participate
- Oral consent via a telephone, during which the participant could also have their questions answered. A record of this must be kept by the investigator including the time and date that consent was provided (this is typically done in an oral consent log—link to template)

Regardless of which of the above means is used, consent questions could include any of the following, as applicable:

- Agree to participate / do not agree to participate
- Agree to be contacted for future studies
- Agree to have data (state whether anonymized or not) retained for use in future studies
- Agree to have anonymized data uploaded to a public archive
- Agree to have direct quotes (state whether anonymized or not) used in publications or presentations
- Whether the participant wishes to receive summary of study results

  Agree to have responses video or audio recorded (specify which) Please see the MREB template for the preamble for online studies https://macrem.mcmaster.ca/Personalisation/DownloadTemplate/164.Risks

Data breach: The risk to your participant of a data breach is frequently higher when the study is conducted online versus in-person, especially when collecting data on sensitive topics such as health or income. Consider using the MREB-endorsed LimeSurvey platform (see https://research.mcmaster.ca/research-resources/limesurvey/) for collecting sensitive data, as it is locally hosted, data will be stored on a secure server, and it includes several MREB-approved survey templates. Limesurvey now has at-rest encryption of the LimeSurvey database, which

means everything that is in the database gets encrypted before being written to the server's disk and stays encrypted while it's not being used. Please be aware that this applies to data in the database only. Files that are uploaded using the LimeSurvey Upload question type are saved in the filesystem, not the database, so they are not encrypted when written to disk. RHPCS is working on finding a solution for that.

Best practice is to collect fully anonymized data, such that there is no way to connect the person to their data. Next best is to collect "de-identified" data on the online platform, i.e. only include the participant ID with the data collected, and keep these data in a separate place from participants' identifiable data collected for research or admin purposes as this reduces the risks to participants should data be breached.

Confidentiality: There is also a risk, if the participant is using a computer in a public space or at home, that someone in their vicinity could see their responses on the screen, hear their responses if using audio, or someone in the household who shares the computer could access their responses. These risks are particularly important to be mindful of in studies that ask about sensitive information, and in studies with vulnerable participants where simply knowing that someone participated in a study could place them at risk. Ways to mitigate these risks include advising the participant, in advance, to complete the study in a private place and clearing their web browser history upon completion. As always, risks must be identified in the main application form directed to reviewers, as well as in the Letter of Information directed to participants.

Demographic questions: Compared to in-person studies, online studies have the potential to reach a much broader range of international participants. With that broader reach, greater care must be taken to design demographics questionnaires that are inclusive and will not offend or pose risks to a participant given their cultural context. Researchers sometimes design questionnaires that conflate ethnicity, race, geography, and language into a mix of questions that can be confusing for participants or leave some out unintentionally. For example, the US race/ethnic categories often use the term American Indian which isn't considered acceptable in Canada. Moreover, some questions could place the participant at excess risk in the case of a data breach. For example, there are countries where disclosing one's non-conforming gender identity or sexuality could result in the

participant being the target of harassment, violence or imprisonment. Some of the ways in which these risks can be minimized include: allowing open-ended or fill-in-the blanks responses, allowing the participant to select all options that apply, and including as response options "other (please specify)" and "prefer not to answer".

5.Withdrawing from the Study, and Skipping Questions

Article 3.1 of the TCPS2 states that consent shall be voluntary, consent can be withdrawn at any time, and that if consent is withdrawn the participant can also request the withdrawal of their data.

Therefore, the following best practices should be adhered to, unless there is a strong justification by the research not to do so:

- Participants can choose not to answer questions or not to complete components of a study that make them feel uncomfortable.
    - In practice, this means questionnaires should not include mandatory questions and/or should have response options such as "prefer not to answer". Very long multi-part studies should include options to skip a given part.

- If a participant withdraws from an online study, the default should be that the data submitted to that point is discarded.
    - However, researchers could include, in the withdrawal process, a question asking participants if data submitted to that point can be kept for use in the research.
    - In a low-risk, anonymous, online study, it may be permissible to keep participant data upon withdrawal by default – if this is clearly communicated in the informed consent process.

- Participants can change their mind about being in a study at any time, without negative consequences. The application section of Article 3.1 states "The participant should not suffer any disadvantage or reprisal for withdrawing, nor should any payment due prior to the point of withdrawal be withheld. If the research project used a lump-sum incentive for participation, the participant is entitled to the entire amount. If a payment schedule is used, participants shall be paid in proportion to their participation."

- In keeping with the above, best practice is to provide the incentive payment to the participant, either full or partial, upon withdrawal, particularly if they have already spent a lot of time providing their data. The details of how withdrawal affects incentive payment must be included in the informed consent process.
- Some platforms make full or partial payment challenging but not necessarily impossible to implement. For example,
    - In the MREB-approved installation of LimeSurvey, all the templates provide each survey page with a link to "Exit and clear survey" that simply exits the survey, without proceeding to debriefing or compensation (this route does NOT allow partial compensation). However, the MREB-approved Limesurvey template called "McMaster" has been adapted so researchers have the option of adding custom texts and links to the screen shown to participants when clicking "Exit and clear survey". Here researchers can add information about options after exiting the survey, including a link to an "exit survey" where they can ask any necessary exit questions, as well as take care of payment/draw entry.Break the study into multiple modules, each one linking to the next, with exit options at the end of each.
        - E.g. in LimeSurvey, the researcher can include in the "end page" of a survey a link to another survey that has multiple links e.g. a "withdraw from the study" link to an exit survey if further questions will be asked, and a "continue to the next module/questionnaire" link which could take the participant to another survey or anything else. Combining a participant's data across multiple surveys can be done by passing the participant ID between surveys using URL variables, which are dynamically inserted into the "end message" URLs and then read into the next survey. See https://manual.limesurvey.org/URL_fields
        - E.g. using MTurk, to break up a long study into modules, a study can be divided into a main "HIT"

that must be completed to receive payment (e.g. a brief pre-screening survey), and a series of "bonus" tasks or questionnaires that can be completed for varying levels of additional payment. (Note that the main HIT and bonus scheme within Mturk is also sometimes used by researchers as a way of rewarding participants who perform at a minimally acceptable level to earn the bonus payment.)

- Combining a participant's data across multiple tasks, surveys or other online modules: Regardless of the platform, one way to handle this is to have the participant generate their own unique code that they enter at the start of each module; see the document "Anonymous coding questions for Linking Surveys" in the Tips and Samples page (type surveys into the searchbox) https://macrem.mcmaster.ca/Personalisation/DisplayPage/50

6.Incentive

Inform participants on both the recruitment materials and LOI how much payment will be given, in what form, and whether they will be paid automatically upon completion or after a specified delay (e.g. if paying the participant requires experimenter intervention). As with any other type of study, it is important that incentive or remuneration offered in online studies is commensurate with the time that the participant spent providing data. Researchers should be aware that some online platforms (e.g. Mturk) allow their participants to provide feedback on the researcher's study, and unfair payment frequently comes up as a complaint in these reviews.

In choosing the form of incentive, consider whether you will need to collect personal information such as emails or mailing addresses (if so, this will need to be discussed in the Confidentiality and Data Security section of the form), and whether this information can realistically be kept separate from sensitive data within your data collection platform (if it can't be separate, then you cannot claim that data collection is anonymous). Collecting personal information in order to facilitate incentive payment means that

participation in the study is not anonymous (even if the data itself is anonymous due to personal information being collected separately and without any link to data).

Potential ways to issue compensation in an online study include:

- Physically mailing a cheque or gift card
- emailing an online gift card
- E-transferring money
- using the crowdsourcing or research panel (e.g. MTurk) platform's payment system
- Issuing a token or identifier based on how much of the survey or study was completed, and asking the participant to contact you and provide this token to obtain partial compensation
- Entering participants in a draw, which involves being able to send the payment/prize to the winners (e.g. collecting email addresses)

7.Confidentiality and Data Security

Below are some of the data security considerations around online data collection. These issues, if applicable, should be discussed in the confidentiality and data security section and also in the risks section of both the main form and the LOI.

Confidentiality: It is important that participants understand that anonymity cannot be guaranteed in any online environment where data is being collected. In the specific case of Amazon MTurk, it has been found that MTurk worker IDs can easily be linked to individuals' Amazon profiles. Thus the default should be that participants' MTurk worker IDs are not collected, or if it is necessary to do so, worker IDs should be kept confidential and secure, not linked back to survey data, and deleted after use.

Anonymization versus de-identification of data: Data that is coded by a participant ID rather than by their name or email can be considered de-identified even if you retain in another location the link between their data and their name or contact information. However, a participant's data cannot be considered as "fully anonymized", even if their name or email is not stored explicitly with the data, if they could potentially be re-identified, e.g. from audio or video or other personal details, because their data is associated with their unique IP address or MTurk worker ID or similar, or

because you are retaining the link between their participant ID and their data. In the case of data collected online, it is not always straightforward to determine whether identifiers such as their IP address are associated with the data. In the McMaster instance of LimeSurvey the default is not to collect IP addresses. This setting should be left as is unless there is a compelling justification why the collection of IP addresses is essential for the research. Researchers should confirm that other online platforms they use for research do not collect IP addresses (or if there is an option, ensure it is set to not collect the IP addresses). In the case of Mturk, note that Mturk worker ID's are stored as part of the study on Mturk. Therefore, researchers should always explain that they are keeping the Mturk IDs separate/confidential from the data (since they always have access to the IDs). And for all studies, whether on Mturk or not, researchers should explain what they are doing with the IDs and how long participants have to withdraw their data.

Cloud vs local storage: Will the data collection platform allow you to store data directly on your local server or will it be stored on the cloud and then transferred? There is additional risk of a data breach with the latter. Best practice is to directly store the data to a secure password-protected McMaster-hosted server, or transfer the data from the cloud to such a server and delete from the cloud as soon as possible. Note that archived or backup copies may still be present in the cloud. Researchers should be familiar with the data retention/deletion policies of the online platforms they are using, and my be requested by MREB to provide this information in the ethics application.

Data encryption: Best practice is to encrypt all data at the point of data collection. NOTE: The TCPS2 strongly recommends encryption of identifiable research data and MREB generally requires encryption of identifiable data, including audio and video recordings.

Video and audio platforms: If the online data collection includes collecting video data using a video conferencing tool (e.g. Skype, Zoom, MS Teams, Google hangouts), there are a number of additional risks, including the risk of a data breach where participants are easily identifiable, and the risk of participants illicitly recording the video session and sharing confidential information. For an in-depth consideration of these and related issues, please see the document "Zoom video conferencing: Best practices for

privacy and security" https://cto.mcmaster.ca/zoom-video-conferencing-best-practices-for-privacy-and-security/

and also the document "Using Video Conferencing Platforms for collecting data from Human Participants"
https://research.mcmaster.ca/videoconferencing/

Use of participants' data by third parties: Carefully consider the Terms of Service (TOS) of any non-locally-hosted online platform you are using (e.g. MTurk, qualtrics, survey monkey, google forms, survey gizmo, zoho survey, Pavlovia) especially regarding the collection of participants' online behavior and history through cookies or other tracking systems), selling of participants' data to third parties, and any protocol the platform has for dealing with a data breach. Any additional risks posed by the above should be stated on the ethics application and participants should be informed of these on the LOI.