Title: Guideline - Use of Online Data Collection Tools for Research with Human Participants

1.0 PURPOSE

TCPS 2 (2022) builds its guidelines on three core principles – one being Concern for Welfare. A contributing factor to participant welfare is ensuring the privacy and control of participant information, which includes participant data housed by online companies, such as survey platforms like Qualtrics, REDCap, SurveyMonkey, recruitment sites like Prolific and Amazon Mechanical Turk (Amazon MTurk), and video conferencing tools like Zoom and Webex. Researchers and REBs must ensure that participants are not exposed to unnecessary risks, and, if risks are present, that participants are made aware of these risks (i.e., collecting and housing online data).

The use of online surveys and video conferencing tools have become popular methods for data collection from research involving human participants.

Online Surveys allow researchers to gather information from participants through web-based questionnaires. This approach can facilitate the collection of large amounts of data. Participation typically requires internet access and a basic level of computer literacy.

Video conferencing tools are online communication platforms that support audio and video interaction. This method allows researchers to interview participants remotely while collecting qualitative data through verbal responses and observable non-verbal cues. Participation typically requires internet access and a basic level of computer literacy.

Many video conferencing tools now offer **AI transcription** built directly into their recording features. When a session is recorded to the cloud, the platform can automatically generate a transcript using AI. There are important considerations that arise regarding the platform's terms of service. Since the company's systems process the data (i.e., the recorded interview), it can be used to train AI models. Researchers must be aware of these data usage policies and ensure participants are appropriately informed about how their audio and visual content will be stored, processed, and potentially used.

For a list of software available to Lakehead University faculty, staff, and students, please click here. Further, if you want to learn about AI tools and data leakage, please visit our cybersecurity webpage.

This Guideline outlines the precautions that must be taken when using companies for recruitment and data collection to ensure that participants are aware of privacy risks and agree to the survey and/or video conferencing company terms.

2.0 DEFINITIONS

- **Research Ethics Board (REB)**: The body of researchers, community members, and others with specific expertise established by Lakehead University to review the ethical acceptability of all research involving humans conducted within Lakehead University's jurisdiction or under its auspices.
- **Online Survey Tool**: A survey designed for completion and submission on a computer or any electronic device connected to the internet (e.g., Google Forms or Qualtrics).
- **Recruitment Platform**: A website or service that connects researchers with potential study participants, making it easier to find people who fit specific research criteria (e.g., Amazon Mechanical Turk). These work in collaboration with an online survey tool.
- **Video Conferencing Tools**: A software platform designed to conduct synchronous interviews/focus groups with participants remotely, allowing for real-time audio and video interaction over the internet (e.g., Zoom, Microsoft Teams).
- **AI Transcription Service**: An online tool, sometimes integrated within a video conferencing platform, that uses artificial intelligence to automatically convert audio or video files into written text (e.g., Zoom's AI transcription service).

3.0 RESPONSIBILITIES

Data anonymity and confidentiality can be vulnerable when collected and stored via the internet. Researchers planning to use online services must acquaint themselves with the relevant laws, for example, PIPEDA or where health information is involved, Ontario's PHIPA. While the physical location of the servers where data is stored is important, our institutional preferences prioritize services governed by specific, protective institutional agreements.

Any data collected and stored electronically is subject to some risk. Researchers and participants must understand that while institutional contracts and enhanced security features help minimize the risk, **absolute confidentiality cannot be guaranteed**.

Governments, regardless of location, can potentially access data housed within their jurisdiction under applicable privacy and national security laws. The most important aspect of the consent process is ensuring participants are fully informed about this potential risk of disclosure under legal authority.

To leverage the security and privacy protections afforded by our institutional agreements, LakeheadU researchers must use their university-provided accounts (accessed via their institutional email) when collecting data.

The tools below provide enhanced security features rather than a personal account or platform that lacks an institutional agreement with LakeheadU.

4.0 RECOMMENDATIONS/INSTITUTIONAL APPROVED BEST PRACTICES FOR ONLINE DATA COLLECTION TOOLS

To promote the protection of participant privacy and the integrity of research data, this section outlines the use of Lakehead University's institutional platforms, along with the specific technical and procedural safeguards to mitigate digital risks such as unauthorized access and fraudulent bot activity.

Where possible, use Canadian-owned and operated online tools, with servers hosted in Canada.

Enhanced security features are recommended for identifiable and/or sensitive data. If you have questions about how your data is classified, please refer to our Data Classification Cheat Sheet, or meet with the Research Security and Data Management Specialist (security.research@lakeheadu.ca | rdm.research@lakeheadu.ca; (807) 343-8010 ext. 8190).

4.1 Institutional Recommended Tools

For Survey Tools: Researchers should use Google Forms through their Lakehead University Google Workspace as their survey collection tool.

For Video Conferencing: Researchers should always use their Lakehead University Zoom account for video conferencing data collection. Saving the video conference instance to the cloud will allow researchers to use Zoom's AI-generated transcription option. Under Lakehead's institutional agreement with Zoom, the data (the recording) will not be used to train Zoom's AI models. Find more information about Zoom's privacy measures by clicking here.

4.2 General Security Practices:

- **Enable Encryption**: For surveys, you can enhance security by enabling the SSL (Secure Sockets Layer) feature within the survey tool. For video conferencing and storage, ensure that end-to-end encryption is active.
- **Use Strong Passwords**: Protect the account used to access any online research tool with a strong, unique password.
- **Enable Multi-Factor Authentication (MFA)**: Whenever possible, add an extra layer of security to your accounts by enabling MFA.

4.3 How to Make Your Video Call More Secure:

When conducting interviews or focus groups via video conference, researchers should follow these steps to protect the session:

- **Use an Institutional Account:** Always use the university-provided license (e.g., Zoom), which has enhanced security features, rather than a personal account.
- **Generate a Unique Meeting ID**: Create a new, unique meeting ID for each interview or focus group. Do not use your Personal Meeting ID, as it is a recurring link that could be compromised.
- **Use a Password**: Protect every meeting with a unique and strong password.
- **Enable the Waiting Room:** Always use the waiting room feature. This allows you, as the host, to control who enters the meeting and verify participants before they join.
- **Lock the Meeting:** Once all expected participants have arrived, lock the meeting to prevent anyone else from joining.
- **Control Screen Sharing:** Set screen sharing permissions to "Host Only" by default. You can grant permission to a participant temporarily if needed.

4.4 How to Make Your Surveys Secure and Accessible

Due to the increase in phishing attacks and fraudulent bot responses, we recommend the following protections. These measures (Babicheva 2023) prioritize "passive" security—detecting bots in the background—to ensure the survey remains accessible to users relying on screen readers or other assistive technologies.

- **Invisible Bot Detection (reCAPTCHA v3):** Instead of visual puzzles (e.g., "Select all traffic lights"), which are difficult for visually impaired users, use **invisible background detection**. This technology analyzes behavior (such as mouse movement and navigation speed) to assign a "bot score" without requiring user interaction.
    - *Note:* In Qualtrics, this is found under Survey Options > Security > "Bot Detection."
- **Accessible Honeypots:** These are hidden questions invisible to human users but visible to bots scanning the code. If a response is recorded for a honeypot question, it indicates a bot submission.
    - *Crucial Accessibility Step:* To prevent screen readers from announcing this hidden field to blind users (causing them to answer it and be rejected), you must ensure the field is coded correctly or labeled with instructions such as: *"If you are a human, leave this field blank."*
- **Instructional Logic Questions (Replacing Math):** Avoid mathematical challenges (e.g., "What is 2+2?"), which can be barriers for those with dyscalculia or cognitive impairments. Instead, use **Instructional Compliance** questions.

    - *Example:* "To verify you are human, please type the word 'Purple' in the box below."
    - *Why this works:* Simple bots look for data patterns (like names or emails) and struggle to follow specific, random instructions.
- **Time-to-Completion Analysis:** Humans need time to read and process questions; bots fill fields instantaneously. Configure your platform to flag or reject responses submitted faster than a human could physically read the survey.
- **AI "Hallucination" Traps:** To catch sophisticated AI bots, ask a question about a fictional event or object.
    - *Example:* "What did you think of the [Fake Name] event last year?"
    - *Result:* Humans will answer "I don't know" or "N/A." AI bots, attempting to be helpful, may invent a detailed, positive description of the event, revealing themselves as artificial.
- **Response Limiter:** Set a limit on the total number of survey responses to prevent an unexpected and costly wave of submissions if a bot attack occurs.

5.0 PROCEDURES AND INFORMED CONSENT REQUIREMENTS

When using institutionally approved online tools/services, the information/consent letter for participants must contain the following statement:

> **Because this study uses online tools, there is a small risk that your data could be accessed by third parties, including government authorities, under applicable privacy and national-security laws. While all reasonable efforts will be made to protect your confidentiality and anonymity, absolute confidentiality cannot be guaranteed when data is transmitted or stored online. With your consent to participate in this study, you acknowledge this potential risk.**

Following this statement, the Information Letter must contain the steps the researchers *will* take to protect confidentiality (as described in the REB Informed Consent Checklist) i.e., methods for secure storage of data, who has access to the data, that participants will not be named in publication of results, etc.

6.0 REFERENCES

- Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans 2022
- Babicheva, Viktoriya. "Avoiding and Detecting Bots and Fraud in REDCap Surveys." Paper presented at REDCapCon 2023, Vanderbilt University, 2023.

7.0 ACKNOWLEDGEMENT

- This revised guideline was developed with the assistance of AI tools (Google Gemini and Grammarly) to support clarity, consistency, and alignment with current best practices.
- We consulted with the Lakehead University Technology Services Centre regarding the material in this document.

Author: _REB Coordinator; Research Ethics Facilitator, and Research Security and Data Management Specialist

REB Chair: _____L. Chambers, Monica Flegel_____

Date of approval: November 29, 2016

Revised: January 28, 2022; February 27, 2026