University of Wisconsin-Oshkosh
Institutional Review Board (IRB)

STANDARD OPERATING PROCEDURES (SOP)	
SOP Number: 18 Effective Date: 10/10/2022 Last IRB Review: 10/10/2022 Last Updated: 05/27/2022 Prepared By: A. Miron, K. Schill	**Title:** **Online and Internet-Based Research**

This SOP sets forth requirements and recommendations by which researchers can plan, develop, and implement computer and internet-based study protocols that provide equivalent levels of protection of human participants to those found in more traditional research methodologies (e.g., paper-based, or in-person studies).

This type of research presents its own unique set of issues and concerns during the IRB review process. Researchers may conduct research using electronic sources such as online survey software (e.g., Qualtrics, Survey Monkey, etc.), social networking sites (e.g., Facebook, Twitter, Instagram, etc.), online marketplaces (Craigslist, eBay, etc.) or crowdsourcing platforms (Mturk, Prolific, etc.) provided they observe the requirements outlined in this document.

In general, the Internet is an insecure medium as data in transit may be vulnerable. The potential source of risk is harm resulting from a breach of confidentiality. This risk is heightened if the research involves data that places subjects at risk of criminal or civil liability or could damage their financial standing, employability, insurability, reputation or could be stigmatizing.

1. Policy

Internet data collection via email, list servs, apps, electronic bulletin boards, text messaging, virtual chats, and web surveys falls under the purview of the Institutional Review Board. Researchers must adhere to the same ethical principles protecting human subjects as mandated in more traditional research situations (see SOP #1). These ethical principles are reflected in procedures that seek and obtain informed consent, protect privacy of participants, maintain confidentiality of data, minimize risks, and prevent coercion.

In general, email to inform and recruit participants is acceptable but should be avoided for the transmission of confidential data, unless encrypted. The IRB requires PIs to follow the procedures outlined below to ensure the adequate protection of research participants and guarantee the validity of the data collected.

The IRB must review all research activities involving the use of the Internet with the same considerations and standards for approval of research (45 CFR 46.111), for informed consent, and voluntary participation as all other research activities:

- The IRB must evaluate the appropriateness of the informed consent process.
- The IRB must take into consideration data collection and security.

- The IRB review must include a consideration for the delineation of boundaries (i.e., would the participant consider the access private or public space of the internet).
- The IRB must consider all additional requirements for the approval of research that involves a vulnerable population as all other studies recruiting those populations.
- As there is no standard for identifying distressed participants online, the IRB must take into consideration potential participant experiences (the sensitive nature of the research) that may be distressing when evaluating the risk/benefit ratio.
- Depending on the risk level and the specific circumstances of the study, the IRB may require researchers to provide an alternative means of collecting data.
- The IRB may require additional protections, such as technical separation of identifiers, data, consent forms and follow-up contact information, or a higher level of encryption.

2. Considerations Related to Online Studies

When posting a survey online, researchers will utilize third-party distributors that have been approved by the IRB (e.g., Qualtrics, Survey Monkey, Zoomerang, etc.). **The UWO IRB strongly encourages PIs to use Qualtrics for online studies:** https://oshkosh.qualtrics.com/**. To have an online study published in Qualtrics, the PI should email the IRB office for study activation. Please include the approved IRB protocol number in the correspondence. All online studies that constitute human subjects research must be approved by the IRB.**

A. Use of Internet for Subject Recruitment

- The IRB must review and approve all materials to be posted on the Internet (e.g., through a website, a banner advertisement, or an email solicitation). Computer-based and Internet-based procedures for advertising and recruiting potential study participants (e.g., internet advertising, e-mail solicitation, banner ads) must follow the IRB guidelines for recruitment that apply to any traditional media (e.g., newspapers and flyers).
- Investigators requesting to recruit through UWO's mass email system must follow the appropriate UWO policies and procedures for review and approval in addition to obtaining IRB approval for the recruitment procedure and message content.

B. Informed Consent Process

- Internet-based surveys need to initially present an IRB approved consent form on which participants would either choose "I agree" or "I do not agree" buttons thus indicating their active choice of whether or not they consent to participate.
    - Should participants not want to participate by choosing the "I do not agree" button, the researcher should immediately direct the participant to a next and final screen that thanks the participant for their consideration and ends the involvement in the study.
    - Should the participants want to participate by choosing the "I agree" button and the data collected is anonymous, the researcher should immediately direct the participant to a next and separate screen from the consent form that will begin the data collection. For online studies with consent forms that require a participant to type their name, the consent form and data collection will be

housed separately. **In order to utilize this consent procedure, the investigator must request a waiver of documentation of consent signature (see UWO Application Consent Section: https://uwosh.edu/sponsoredprograms/irb/forms/**

- For surveys sent to and returned by participants via email, investigators should include an IRB approved consent form and inform participants that submitting the completed consent document indicates their consent. Participants must be informed that, due to unintentional breaches of the data, this method of data collection cannot ensure confidentiality.
- For surveys sent to and returned by participants via email without a signature, investigators must include a consent document and inform participants that submitting the completed survey indicates their consent. This constitutes unsigned consent. **In order to utilize this consent procedure, the investigator must request a waiver of documentation of consent signature (see UWO Application Consent Section: https://uwosh.edu/sponsoredprograms/irb/forms/**
- When using an online data collection site (e.g., Amazon Mechanical Turk, Survey Monkey, etc.), investigators should carefully review the site's data security policy. If the site stores identifiable information and/or links survey responses to Individual participants, this must be made clear in the investigator's IRB submission and in the corresponding consent document(s).
- Researchers conducting any form of web-based research convey that they will endeavor to provide confidentiality or anonymity but should be careful not to make guarantees of confidentiality or anonymity, as the security of online transmissions cannot be guaranteed.
- Researchers should instruct subjects to close their browser window after participation and suggest that they clear their cache to protect their confidentiality, especially if the participant uses a shared computer.
- After receiving consent from each participant in an online synchronous or asynchronous discussion board between two or more individuals, and when research includes observing a chat room that is not open to the public, researchers must inform participants that observation is taking place, and that any information exchanged may be used for research purposes. Researchers remain vigilant to remove any unintended individual joining the established group after the researcher has gained consent.

C. Risks

Collecting data over the Internet can increase potential risks to confidentiality because of the frequent involvement of third-party sites and the risk of third-party interception when transmitting data across a network.

All studies, including those using computer and internet technologies, must:

- Ensure that the procedures fulfill the principles of voluntary participation and consent
- Have appropriate safeguards to protect the privacy or confidentiality of information obtained from or about human participants
- Adequately address possible risks to participants and ensure that risks such as psychosocial stress, violation of privacy, and legal risks, etc. are minimized.

- Participants should be informed of these potential risks in the informed consent document. For example:
    i. "Although every reasonable effort has been taken, confidentiality during actual Internet communication procedures cannot be guaranteed."
    ii. "Your confidentiality will be kept to the degree permitted by the technology being used. No guarantees can be made regarding the interception of data sent via the Internet by any third parties" (Pennsylvania State University);
    iii. From UWO IRB website MTurk Consent Template (Updated 2021): "**Privacy & Confidentiality of your Information:** Researchers will have access to your MTurk worker ID which may be able to link to your personal information on your Amazon public profile page, depending on your settings you have on your Amazon profile. Amazon will have access to your MTurk ID and personal information (social security number, IP address, bank account information, etc.) and would be able to link it to your survey responses if the survey is created using MTurk internal software. MTurk worker IDs will not be shared with anyone outside the study team and will be used solely for the purposes of distributing compensation and will not be stored with your (survey responses/data). We will not be accessing any personally identifying information about you that you may have put on your Amazon public profile page. Worker IDs will be removed from the dataset (describe when). Data will be retained on the Amazon (and Qualtrics if applicable) servers for (length of time) and will be deleted by the research staff after this time. However, data may exist on backups or server logs beyond the timeframe of this research project. Data transferred from the survey site will be saved on a password protected computer for (length of time data will be retained). Any reports and presentations about the findings from this study will not include your name or any other information that could identify you.
    iv. "Data may exist on backups or server logs beyond the timeframe of this research project."

- Online consent may not be suitable for high-risk studies where the research involves data that places participants at risk of criminal or civil liability, or could damage their financial standing, employability, insurability, reputation, or could be stigmatizing. Thus, researchers may be required to:
    - gather consent through direct contact with participants (i.e., not online), or
    - request a waiver of documentation of consent (meaning the researcher will provide potential participants with all of the required elements of consent, but not collect signatures from participants)

NOTE: Research is subject to the Children's Online Privacy Protection Act. Therefore, researchers are prohibited from collecting personal information from a child without posting notices about how the information will be used and without getting verifiable, written parental permission.

- For minimal risk research, both assent forms from the child participant and consent forms from the parent or guardian must be secured before any data can be collected. If

the research is more than minimal risk, the scope, child participation and potential risks of the study must be discussed virtually with the parent or guardian before assent and consent forms are secured and any data can be collected.

- For research that excludes minor participants, in order to authenticate that the participant is not a minor posing as an adult, the IRB may ask the researcher to describe the procedures to be employed to authenticate that the participants are adults. Some options are using internet monitoring software or using adult check systems that can screen out minors.

D. <u>Collecting Data from Social Media Sites</u>

When a researcher plans to observe comments posted on blogs or other social media websites, the researcher must:

1. Do so in accordance with the site's privacy policy, and;
2. Identify him/herself as a person conducting research who will be gathering information from the site for a specified period of time (for instance, when using Twitter API process: https://help.twitter.com/en/rules-and-policies/twitter-api or;
3. If, due to the nature of the study, it is not possible for the researcher to identify him/herself, this must be justified on the IRB application along with a description of appropriate opt-out and debriefing procedures.
4. **IRB review is not needed for data that are public (see below).**

<u>Distinction between Public versus Private Online Data</u>

- Using data from public sites is akin to observing public behavior which does not meet the definition of research using human subjects. Private information is considered identifiable under the Common Rule if the identity of the subject is or may readily be ascertained by the investigator or associated with the information. [45 CFR 46.102(f)].
- When a website has a privacy policy, the IRB will assume that the users of the site have a presumption of privacy, unless the site policy specifies which data are public and which are private. **Using data that are deemed private by the site privacy policy or by the researcher meets the definition of research using human subjects.**
- When a website has a privacy policy and the researcher plans to use private data, the researcher must attach a recent copy of the site's privacy policy (printed within thirty days of protocol submission) to their IRB application.
- When a researcher plans to collect private data from a website that has a privacy policy, the research design must conform to all requirements of the site's privacy policy.
- If the researcher is unable to find a copy of the site's privacy policy, the researcher must contact the site to determine if a policy is available.
- If after contacting the site the researcher learns a privacy policy is not available and the researcher plans to use private data, the researcher must state this on the IRB application.
- Researchers using public data such as tweets or other public posts are encouraged to paraphrase tweets to protect the identity of participants. If researchers plan to use data harvesting tools such as Tweet Catcher that track and collect participants' tweets or posts across time, researchers should submit an IRB application to get approval for the

use of those data and allow participants to opt out of the study if direct quotes of tweets are used.

This resource was developed in part using material from:

- Northeastern Illinois University: NEIU Online Research/Online Consent: https://www.neiu.edu/sites/neiu.edu/files/documents/2021/02/04/Online%20research%20SOP.pdf
- University of North Carolina Wilmington: Online Research (#6.2): https://uncw.edu/sparc/integrity/documents/uncw_irb_sop6.2_online_research.pdf
- University of Missouri Kansas City: Research Data Security https://ors.umkc.edu/services/compliance/irb/irb-docs/21-research-data-security-february-2019.pdf
- Johns Hopkins IRB Guidelines for Research Involving Apps and Software: https://www.hopkinsmedicine.org/institutional_review_board/guidelines_policies/guidelines/research_involving_apps_software.html
- University of Wisconsin IRB Guidance for Technology and New Media Research: https://kb.wisc.edu/sbsedirbs/page.php?id=42376
- Cornell University: Use of Social Networking Sites or Mobile Devices https://researchservices.cornell.edu/sites/default/files/2019-05/IRB%20Policy%2020.pdf
- SACHRP Recommendations Concerning Internet Research and Human Subjects Research Regulations https://www.hhs.gov/ohrp/sites/default/files/ohrp/sachrp/mtgings/2013%20March%20Mtg/internet_research.pdf