



GREB SOCIAL MEDIA GUIDELINES

Purpose

The purpose of this guideline is to:

1. Provide researchers with standardized information and guidance related to research involving social media platforms
2. Promote and facilitate best ethical practices when using social media in research

Background

Conducting research-related activities involving social media has become increasingly common among researchers. Social media platforms, such as Facebook, Twitter, Instagram, Snapchat, etc. provide researchers with new methods and opportunities to recruit participants, collect and analyze data, and disseminate their research.

Social Media Competencies

Researchers who wish to conduct research activities using social media platforms should demonstrate to the Research Ethics Board (REB) that they are aware of the subtleties of using social media.

Researchers need to be aware of the privacy issues, relevant user settings, privacy settings and terms of service on the social media platform as well as their effects on the privacy, confidentiality and rights of potential research participants and participants alike.

Recruiting Participants Using Social Media

Recruiting research participants using social media platforms must be conducted in accordance with the core principles laid out in the Tri-Council Policy Statement (TCPS 2):

- Respect for Persons
- Concern for Welfare
- Justice

Just as other non-social media recruitment documents such email scripts, printed posters, in-person scripts, etc. require GREB review and approval, so too do social media recruitment documents.

This includes, but is not limited to:

- tweets,
- Instagram posters/pictures,
- Facebook advertisements, posts, videos, and messages.

Respecting the Privacy and Confidentiality of Research Participants

Respecting the privacy and confidentiality of participants typically entails that potential research participants can find out more information about a given study, and are able to participate in a particular study, without having such information made known to individuals outside of the research team. To this end, social media platforms should be examined to understand any suggested limits in participant privacy and confidentiality. It is imperative that privacy and confidentiality is protected unless participants consent to waive such protections. It is also important to understand that as the risk(s) of participation in research increase, privacy and confidentiality become critical requirements.

Facebook

As of January 2022, Facebook has four types of privacy settings for events:

- Private – only people who are invited
 - Guests can invite friends, (Yes and No) If this is set to “Yes,” this would be considered snowball sampling and would need to be clearly mentioned and detailed in the recruitment section of the GREB Standard Application Form
- Public – Anyone on or off Facebook can view the event
- Friends – Only your friends on Facebook can view the event
- Groups – Only Members of a group you are in can view the event

GREB advises researchers not to communicate directly with participants through Facebook, nor should Facebook users be able to post on the event’s feed. Rather, potential participants should be encouraged to contact the research team directly outside of the particular social media platform.

To protect the privacy of individuals you can invite Facebook users to an event, however, the “Show guest list” option would need to be turned off so that other guests cannot see who else was invited.

Protecting the Privacy and Confidentiality of Researchers

The use of personal social media accounts for conducting online recruitment poses unique challenges.

Personal social media accounts tend to include private details about individuals (such as addresses, places of work, religious and political affiliations/ideologies, etc.) as well as details about third parties (such as friends, family members, colleagues, acquaintances, etc.).

Using a personal social media account for research purposes can be problematic because such accounts typically not only share personal information about the researcher, but also share details about the researcher’s friends, family, and colleagues, who may not want such details revealed to potential research participants. Thus, out of respect for those individuals who may indirectly feature in the researcher’s social media account, personal social media accounts are discouraged from being used in research-related activities.

GREB encourages researchers to develop a research-specific Facebook profiles, groups, or other social media profiles.

Avoid using your personal Facebook account, create a separate account for your research.

If you are a part of a research group or lab, create a separate Facebook account for your research group.

Recommended Settings for Facebook Events

If you use Facebook Events to invite people to participate in your research study, we suggest you use the following settings for your event to ensure the integrity and security of the Facebook Event.

1. Set Event Options-> Show guest list = Off
2. Set Event Options-> Only admins can post in event = On
3. Set Event Options -> Posts must be approved by a host or co-host = ON

Collecting and Analyzing Social Media Data

One of the major misconceptions many researchers have when conducting social media research is that just because social media data (e.g., Instagram posts, Facebook pictures, tweets, etc.) exists on a seemingly “public” social media platform, that researchers are free to use such data as they wish, for their own research purposes. This is not necessarily correct.

There are two things that researchers should do when conducting and analyzing social media data: (i) respect the privacy restrictions, user settings, and legal requirements of the particular social media platform they intend to use; and (ii) take seriously the potential risks associated with collecting and analyzing social media data.

Respecting Privacy Restrictions, User Settings, and Legal Requirements

Researchers collecting and analyzing social media data must familiarize themselves and abide by the privacy restrictions, user settings, and legal requirements of the social media platforms they intend to use. These policies vary across different social media platforms and evolve over time. Let us look at one example.

Presently, according to Facebook’s Terms and Services, individuals own the rights to the information that they themselves have produced and posted on Facebook. This includes pictures, comments, notes, videos, and so on. In cases where researchers wish to collect and analyze social media data that does not belong to them – regardless of how easily available the data may be – they must obtain consent from the owner before using the data for research-related activities. Individuals who share data on Facebook have an intellectual property right over their data and respecting the rights of research participants necessarily entails receiving their consent before using their data for research-related purposes.

For example, if a researcher is seeking to conduct a photovoice project using someone else’s photos that appear on Facebook, even if such pictures are shared widely, they must nonetheless obtain consent from the owner of the photos to use them in their project. The important thing to note is that just because social media data may be widely accessible does not mean that consent is not required to use such data for research-related purposes.

Potential Risks Related to Research Involving Social Media Data

Individuals conducting research-related activities involving social media data must be cognizant of the potential risks associated with such activities. Even in cases where social media data is widely shared, there may be significant risks to research participants. For example, it is not uncommon for individuals to upload and share information on a social media platform that (i) does not belong to them, (ii) that they have no right to share, and that (iii) may cause significant harm.

GREB Social Media Guidelines

For instance, individuals may create and operate a fake social media account that in no way represents the actual user or create and operate a social media account with the intent of bullying, harassing, or exploiting others. Unfortunately, such social media accounts exist, and it is important for researchers to be aware of the precarious nature of social media data, and to think carefully about how using social media data may affect the rights of research participants.