Grand Valley State University Institutional Review Board (IRB)	
Title: *Internet mediated research*	
Section: 740.	This policy and procedure supersedes those previously drafted
Approved by HRRC: 07/12/2011 Revised 11/04/2014 Reviewed 10/28/2014 Revised by HRRPPC: 04/24/2018 Revised by IRBPPC: 04/23/2019	Approved by RIO/HRPA: 04/12/2012 Revisions approved by AIO/RIO: 05/12/2018 Revisions approved by AIO/RIO: 5/23/2019
Effective Date: 5/27/2019	
Related Sections: *120: Compliance with applicable laws and regulations* *730: Collection, management and security of research information* *OP-8: OIA procedures for research involving GVSU student email* *G-16: Guidance on data management requirements for research data* *PC 11.7: Confidentiality, Data & Security Policy*	

Policy

Internet-mediated research is guided by the following principles:

- Research conducted using *public information* acquired through social media does not need explicit notification of or consent from persons participating in the social media.

- Research conducted using *private information* acquired through social media requires explicit notification of persons participating in the social media.

- Specific methods of notification of the intent to conduct research and subsequent securing of explicit affirmative consent from participants may be required at the discretion of the IRB.

- Consent, assent and permission requirements for research conducted using social media generally are the same as in other contexts and domains and as described in IRB policy.

- Any electronic research or communication with an individual within a country belonging to the European Economic Area must comply with the General Data Protection Regulation (GDPR). See *IRB Policy 120: Compliance with applicable laws and regulations* for more details.

Cloud computing is guided by the following principles:

- Use of cloud computing services is ***prohibited*** for research involving security levels 3 and 4 data *unless* specific contractual agreements are signed and approved by University legal counsel and an authorized representative of Information Technology prior to submission to the IRB [see IRB *Policy 730: Collection, management and security of research information*].

- The use of cloud computing services may be allowed, without prior approval of University legal counsel or Information Technology, for research that *does not* involve data security levels 1 and 2 as described in the IRB Policy 730. However, in such situations, the researcher(s) must *not* make guarantees of privacy or confidentiality to research participants.

- Cloud computing data storage must comply with the GDPR.

Cloud computing services may lack durable and verifiable data security and **their use could violate the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and the GDPR, or other privacy protections for which the researcher is responsible, and GVSU may be liable if breached.** Risks of storing data in cloud computing resources include potential loss of sensitive or confidential data and unauthorized access or use of the data by the host service provider or unknown third parties. For more information, see *G-16: Guidance on Data Management Requirements for Research Data*.

When evaluating research protocols that utilize the internet and/or electronic communication for conducting research, the IRB will consider all of the following components:

a. Sensitivity of the data collected
b. Identifiability of research participants
c. Personal privacy protections for participants
d. Terms of agreement from internet service providers including assurances of privacy protections, and comprehensive data security
e. Assurance that the research is compliant with GDPR
f. Accessibility of an individual within a country belonging to the European Economic Area to participate in the research

Procedures

1. Accessing Information for Research on Social Media Sites

    a. A researcher may not misrepresent him/herself to gain access to a social media site if it is against the policy of that site or is in violation of any law or regulation. Researchers who have ethical access to a site where membership or sharing of information is restricted to certain persons are considered to be in a "private" setting and, in order to conduct research, may need approval of the social media site owner/moderator and group members, as determined by the IRB.

    b. A researcher may not create a site that appears to be for the purposes of serving visitors to the site when the true purpose is to gather information for research, unless the site is an open forum that meets the requirements of "public" research as defined in this policy, or all of the following are true:

        i. Visitors to the site are clearly informed that information shared on the site will be collected for research purposes;
        ii. The site purpose and function does not violate any law, University, or host server policies;
        iii. Data is collected and stored in accordance with GDPR, and an appropriate, active consent process is used, in the event that any visitor is accessing the site from an European Economic Area country;
        iv. The site research project has been approved by the IRB.

2. Privacy Protections

a. If social media is used in the recruitment of research participants, researchers should describe all of the following:

    i. How participants' information will be gathered and used;
    ii. The potential privacy risks involved;
    iii. The planned data security;
    iv. How active, informed consent will be obtained in accordance with GDPR;
    v. Any risks associated with participating in the research, including but not limited to the following:

        1. Whether the information collected is duplicated, archived, sold or traded by or to other entities;
        2. The planned destruction of information collected for research purposes, including information on participants who withdraw participation prior to completion of the research.

b. Online names used on social media sites shall be treated as personally identifiable in the same manner as a person's legal name and may be used only with explicit consent from the participant.

3. Identification of and intent to use a cloud computing service must be included in the initial research proposal or any change in protocol that adds such use after initial approval has been granted. Other approval(s) may be required in addition to that of the IRB. Use of third-party commercial survey tools is not permitted for research that involves sensitive data as described in categories 3 and 4 in IRB *Policy 730: Collection, management and security of research information.* See guidance *OP-8: OIA procedures for research involving GV student email*).

4. Researchers should be aware of the risk of data loss or corruption when using cloud computing services and should consider backing up the data by some other IRB-approved method. Any data breach occurring on a project involving GDPR-covered research must be reported **within 24 hours** upon identification of the breach to the appropriate university GDPR compliance official (Vice Provost for Research Administration) and the Office of Research Compliance and Integrity. The breach must also be reported to the IRB as an Unanticipated Adverse Event within 7 calendar days.

5. Researchers should not make guarantees of confidentiality of data or anonymity of participants when using internet mediated methods of conducting research.

6. Low-risk, anonymous or de-identified surveys and questionnaires may be exempt from the federal regulations and generally do not require documentation of informed consent agreements. However, study participants must be informed of potential risks of discovery of the participant's identity or the identity of the computer used when participating in the research.

7. Internet-based surveys should include disclaimer statements about all relevant risks of participating including risks related to internet data security. Participant response buttons "I agree" or "I do not agree" are a common method of indicating the participant has been informed of potential risks described and consent to participate in the research. An active consent process utilizing a clear affirmative action indicating consent **must** be used for all internet-based research, so as to comply with the GDPR. Pre-ticked boxes and/or inactivity are not considered active

consent and cannot be used.

8. If a survey or questionnaire uses GVSU e-mail as a communication link, the researcher must receive approval from the Office of Institutional Analysis (OIA). See Policy *OP-8: OIA procedures for research involving GVSU student email.*

9. For internet mediated research in which ***documentation*** of informed consent is required, the researcher should describe the method by which the documentation will be provided from each participant. One possible option is to have ink signed consent forms faxed or scanned and electronically submitted. In some cases an original ink signed consent form must subsequently be mailed to the researcher for the research file.

10. All participants in internet mediated research must be asked to affirm their current age. Surveys and internet based interviews involving persons under the age of majority require either documented parental/guardian permission or a waiver from the IRB. Data may not be gathered or used from persons who have not reached the appropriate age of majority. For most locations in the USA the age of majority is generally eighteen (18) years, but in some states and territories it is older and in some it is younger. For Member States of the European Union, the age of consent to comply with the GDPR is sixteen (16), unless the Member State law provides for a younger age of consent. See IRB *Policy 120: Compliance with applicable local laws and regulations* and IRB *Policy 911: Exemption determinations and research ethics standards.*

11. When applicable, researchers must clearly indicate whether narrative responses to open-ended questions or other comments may be quoted and reproduced by the researcher.

Background

1. Social Media: For purposes of this policy, social media is understood to include web-based and mobile technologies used to turn communication into interactive dialogue such as web sites, RSS feeds, pod casts, text messaging systems such as Twitter accounts, and comparable communication systems.

2. Public Information: Information collected from or about living human persons for research purposes and acquired through social media is considered *public* if:
    a. It can be accessed freely without requirement of membership, subscription or fee payment, or
    b. Access requires membership, subscription and/or fee payment but is readily available to anyone and initial membership is routinely granted.

3. Private Information: Information collected from or about living human persons for research purposes and acquired through social media is considered *private* if:
    a. A gatekeeper has the authority to deny access to the social medium (such as a moderator who approves/denies memberships, regardless of whether that authority is exercised), or
    b. The information can be accessed only through affirmative permission(s) of a gatekeeper, or
    c. Membership is restricted to persons with certain eligibility characteristics such as having specific medical conditions or providing care to persons with specific medical conditions.

4. User Group Compliance: Researchers collecting information in social media networks where there is an explicit set of eligibility requirements, policies, standards, procedures, or other expectations of all users, must comply with those expectations and requirements. Examples include the avoidance of certain types of language, posting of prohibited material, etc.

5. Research studies that involve surveys, discussion groups, and some versions of audio and visual based experiments increasingly utilize internet based forums. Several difficult ethical issues have been identified when considering how best to provide protections to research study participants. These include:

    a. Restricted versus open access to the internet sites
    b. Personal privacy protections
    c. Security of information provided by research participants including:
        i. Potential for data corruption or loss
        ii. Data re-use by other researchers or commercial vendors
        iii. Data archiving and assured destruction
        iv. Distributing by the service provider or other persons with technical access to it