1.0 POLICY

1.1 Background.

1.1.1 Online research is proliferating because of the opportunity to contact many people rapidly, to reach people with certain characteristics (diseases, political views, etc.), and, often, to collect highly personal information free of the constraints and expense of face-to-face interaction. This upsurge has led to evaluations of if and how conventional research ethics guidelines can be applied to research in cyberspace.

1.1.2 “Online research/internet research” is defined very broadly to include research involving e-mail, homepages, weblogs, Listservs, USENETs, IM (text-based), CUSeeMe (and other audio-video exchanges), chatrooms, MUDs/MOOs, gaming, images and other forms of multi-media presentation (webcams, etc.), social media (Facebook, MySpace, Twitter), and other venues that emerge as part of cyberspace.

1.2 Policy Statement.

1.2.1 It is the policy of the University of Alabama Institutional Review Board (IRB) to review all research using 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 under the jurisdiction of the UA IRBs.

1.2.2 The informed consent process and documentation of such must include all relevant elements of informed consent as listed in the Federal regulations.

1.2.3 The Office for Human Research Protection (OHRP) does not recognize electronic signatures as evidence of consent. If the UA IRB requires that written informed consent must be obtained, prospective participants must write or FAX their agreement to the investigator.

1.2.4 Investigators may not use internet survey contacts for any purpose other than the explained and approved research.

1.2.5 The IRB application and review must include a consideration for the delineation of boundaries (i.e., would participants consider the access to be private or public space of the internet).

1.2.6 The IRB review must consider the risks to the participants and must assure that there is an appropriate level of protection:
1.2.6.1 Each communication carries the risk of a breach of confidentiality. Even when data are collected without names, websites or email programs may still be capable of collecting identifiers.

1.2.6.2 The IRB must consider that admonishing participants that they must be at least 19 years of age to participate does not guarantee compliance.

1.2.6.3 The protection of vulnerable populations must be considered in internet research as in other research.

1.2.6.4 Because there is no standard for identifying distressed participants online, the IRB must consider potential participants’ experiences (the sensitive nature of the research) that may be distressing when evaluating the risk-benefit ratio.

1.2.6.5 Research involving online surveys with multiple data collections (cohort research) must describe mechanisms for participant withdrawal and how to retrieve and discard data from participants who decide to withdraw.

1.2.6.6 The IRB must receive, review, and approve all materials used for posting recruitment materials on the internet, e.g. through a website, a banner advertisement, or an e-mail solicitation.

1.2.6.7 Investigators requesting to recruit through the mass communication systems of the University of Alabama (e-mail, the UA Student News, the student research subject pools, etc.) must discuss their communication plans with the persons in charge of these systems and append a letter of agreement to assist, pending IRB approval, from those persons.

1.2.6.8 The IRB must approve all plans for data collection and security for each step of the communication pathway (e.g., from the participant to the server, from the server to the investigator). All databases storing identifiable information or data must be protected regardless of the source creating the data (e.g., encryption of the database, de-identifying the data). Information regarding transmission and storage of the data must be provided. If a separate server will be used for data collection or storage, the IRB must approve its administration.

1.2.6.9 The UA IRBs may seek external consultation about proposals for internet research as needed.

1.2.6.10 Any changes to an approved protocol—e.g., plans to add internet recruitment to an approved protocol, to add internet venues different from those previously approved, to reach a different population, to change the content of advertisements or other solicitations—must be submitted to the IRB using FORM: Modification of An Approved Protocol.

1.2.7 Objective

1.2.7.1 Implementation of this policy will ensure that the rights and welfare of participants in internet research conducted by UA affiliates will be adequately protected.
1.3 Responsibility.

1.3.1 This Vice President for Research is ultimately responsible for this policy. Enabling parties include the Director of Research Compliance and Research Compliance Specialists, the IRB Chairs and Members, the Associate Deans for Research, investigators, faculty supervisors of student research, and the Director of Security and Compliance from the Office of Information Technology.

2.0 PROCEDURE

2.1 Investigators will prepare initial, continuing, or modified applications for IRB that address the special considerations of internet research described under I.2 and enable the IRB to assess the adequacy of human subjects protection.

2.2 Investigators should consult other IRB policies and guidance documents that relate to their proposals, such as policies on specific vulnerable populations or appropriate and legal incentives.

2.3 Include descriptions of all security measures in place regarding data collection and storage and any software used to protect confidentiality and privacy of persons and data. Note that the protection of participants’ identity from other participants or the investigator is often a key factor in whether the research can qualify for exempt status.

2.3.1 Describe any software/survey package features used to protect persons’ privacy and confidentiality of data.

2.3.2 When appropriate, the data should be transmitted in an encrypted format.

2.3.3 Encryption is also required when a server will be used for data storage.

2.3.3.1 This server must be in a secure location, accessible only by the principal investigator and key study personnel.

2.3.3.2 The server must be maintained by a professionally trained person with expertise in computer and internet security.

2.3.3.3 Back-ups of the data should be made as appropriate and stored in a secure location.

2.3.3.4 A plan for destruction of the data must be included in the IRB application.

2.4 Investigators must describe the methods for obtaining and documenting informed consent from each participant (this may be as simple as stating that submission of responses will serve as evidence of informed consent, allowing “no response” as an option for questions, or the IRB may require separate written signed consent).
2.4.1 If appropriate, request a waiver of consent or a waiver of written documentation of consent, using those forms.

2.5 Describe the mechanism(s) for assuring that participants are of the legal age to consent.

2.6 Describe efforts to assess potential participants’ comprehension of the consent information. Possibilities include incorporating short questionnaires into the consent process to assess understanding or asking participants to contact the investigator to discuss the information presented before beginning the study.

2.7 If the research involves gathering of sensitive information, describe a mechanism for identifying serious distress and providing assistance to participants who may be distressed by the questions asked. Possible methods include providing contact information for the investigator, identification of reactions or symptoms that indicate a need for counseling, identification of a trained counselor, or listing websites providing useful information or support.

2.8 For use of the campus-wide communication systems for recruitment, identify the person in charge of the desired system and describe your plans/needs to that person. Note that these persons may give you valuable advice about the process of using their systems and the format or content of your communication, thus saving you the need to revise an application later to fit system circumstances. Append a letter of agreement to assist from that person, pending IRB approval of the application.

2.9 Use FORM: Template for Study Presentations for Web Surveys to guide development of email messages to prospects or on a study website. The eight elements of consent must be addressed.

2.10 The IRB will follow its policies and procedures for the review of exempt, expedited, or full board review appropriate to the application, while considering that all communication carries the risk of a breach of confidentiality, and for communication of decisions to the investigator.

3.0 REFERENCES


4.0 RELATED SECTIONS

4.1 GUIDANCE: IRB Application Guide

4.2 FORM: IRB Checklist for Reviewers and Investigators

4.3 FORM: IRB Renewal Application
4.4 **FORM:** Modification of an Approved Protocol

4.5 **GUIDANCE:** Template for Study Presentations for Web Surveys