Institute for Social Research
University of Michigan

POLICY ON SAFEGUARDING RESPONDENT CONFIDENTIALITY

Policy:

The scientific mission of the Institute for Social Research (ISR) includes the planning and conduct of high quality social science research, and the dissemination of findings from this research. As part of this mission, ISR promises those who participate in its surveys and other studies that their responses will be kept completely confidential. In addition, certain research sponsors and/or federal laws and regulations require such assurance. ISR takes this obligation very seriously and requires that all ISR employees (faculty and staff) and affiliates read this Policy on Safeguarding Respondent Confidentiality (Policy) and sign the associated Pledge to Safeguard Respondent Confidentiality (Pledge) promising compliance with the Policy. Failure to comply with the Policy may result in discipline up to and including termination of employment for ISR employees, and severance of any relationship with ISR and/or the applicable research project for all other affiliates.

ISR widely disseminates anonymized datasets based on information provided by respondents. However, the utmost care is taken to ensure that no data are released which would permit any respondent to be identified, except in those rare cases in which the respondent specifically authorizes the identification. Thus, ISR requires that all ISR employees and affiliated non-employees read this Policy and sign a Pledge agreeing to safeguard respondent privacy, anonymity, and confidentiality. No individual or entity will be permitted to work with any ISR research data (other than unrestricted public release datasets) unless this Pledge has been formally signed by the individuals involved.

This Policy applies to all oral, written, electronic or other tangible forms of data, and to the management and application of data collection, storage, processing, analysis, retrieval and dissemination. It applies to all persons who have access to information about ISR respondents, regardless of whether that access has been specifically authorized. This Policy and Pledge explicitly require a commitment to safeguard respondent privacy as to past and future behaviors.

Definitions:

As used in this Policy and associated Pledge:

"Affiliate" means a non-employee of the ISR who has, or might have, access to information provided by ISR respondents. Affiliates include contractors and their employees, consultants, visiting scholars, students, informal visitors, teaching assistants, co-Investigators and project directors from other University of Michigan departments or other institutions, and custodial, maintenance, and security staff assigned to ISR.

"Anonymity" means that the name and other identifying information about a respondent, a proxy for a respondent, or about other persons on whom the respondent or proxy provides information, will not be revealed.

"Confidentiality" means that specified information provided by a respondent, or a proxy for a respondent, will not be disclosed without the permission of the respondent. Names and other identifying information regarding respondents, proxies, or other persons on whom the respondent or proxy provides information, are presumed to be confidential. Other information may be designated as confidential by specific agreement of the respondent and ISR staff.

"Employee" means an employee of ISR, including regular employees, temporary employees, contingent employees, Graduate Student Research Assistants, Research Fellows, and other employees.

"Privacy" means the ability of a respondent to control the dissemination of information about the respondent or a proxy, or provided by the respondent about others.

"Promise of confidentiality" means a promise to a respondent that the information the respondent provides will not be disseminated without the permission of the respondent; that the fact that the respondent participated in the study will not be disclosed; **and** that disseminated information will include no linkages to the identity of the respondent. Such a promise encompasses traditional notions of both confidentiality and anonymity.

“Protected information” means the information covered under anonymity and promise of confidentiality, as set forth in the definitions herein.

"Respondent" means a survey respondent or informant, experimental or observational subject, focus group participant, or any other person providing information to an ISR study or on whose behalf a proxy provides information.

Rationale:

To achieve its scientific mission, ISR seeks to advance the understanding of human behavior and social life through research designs which measure attributes of individuals, organizations, and their social contexts. These research designs are usually implemented by the collection, analysis, and publication of data from scientific samples of local, national, and international populations. Most ISR studies require interviewing respondents in order to obtain the necessary data.

ISR recognizes and appreciates that respondents should be given assurances that the information they provide will be confidential and the respondents remain anonymous. Further, it is also recognized that the loss of confidence by respondents in ISR's promises of confidentiality could significantly threaten ISR’s ability to conduct accurate scholarly research studies. ISR values each respondent's right to privacy, to decide voluntarily when to participate in ISR research, and to be informed about the purpose, scope, and importance of their participation. ISR study procedures are designed to ensure that individual respondents are protected at each stage of research.

The confidentiality and anonymity of information collected or held by ISR personnel must be assured through careful design and implementation of safeguards throughout all stages of the research process. All information obtained during the course of the research about respondents, their families, or the organizations they represent, is protected information, subject to the promises of confidentiality, regardless of whether that information is derived from the respondent or is otherwise learned by employees incidental to the performance of their work. ISR employees and others are obligated to respect as confidential and anonymous all such information, and never to discuss it for any reason not directly related to the project.

Some ISR research projects may use informed consent statements that make clear that certain types of information obtained from or about the respondent will **not** be subject to the promises of anonymity and confidentiality. Even as to information included in such exemptions, however, decisions about whether and under what circumstances the information will be disclosed may be made only by project directors and/or Center and ISR leadership, and not by any other employees or affiliates.

When confidentiality as to specified information has been promised to a respondent, the authority to give permission for release of the information belongs to the respondent, rather than to the respondent's proxy or to the persons on whom the respondent provided the information.

It is the responsibility of ISR, through its employees and affiliates, to protect the anonymity of respondents and the confidentiality of its research documents and data at each stage of the research process: data collection, storage, processing, analysis, retrieval and dissemination.

The potential sanctions for violations of this Policy do not apply to releases of data pursuant to a valid court order, provided the release is made with the approval of the appropriate project, Center, ISR, and University of Michigan officials.

Stages of Research Process:

(1) *Data Collection*: All employees and affiliates associated with data collection must endeavor to conduct interviews or other data collection activities in situations that do not compromise the respondent's privacy. Data and documents in which individuals, families, or organizations are identified must be maintained so that access by unauthorized persons is prevented. Data should not be collected from persons the employee or affiliate knows personally, except with prior approval of the research project directors.

(2) *Data Storage, Processing, Analysis and Retrieval:* All information, in paper, electronic or other tangible form, that identifies an individual respondent -- such as name, address, telephone number, or other identifying information available to persons outside ISR -- must be separated from the substantive information collected, and placed in secured files as soon as possible after data collection from the respondent is completed. Research documents that identify respondents or organizations must be kept in areas with restricted access. When such documents are being handled and used, they must never be left unattended, and they should be locked away when not in immediate use. Access to identifiable survey data should be limited to appropriate personnel who have signed the Pledge associated with this Policy.

Affiliates of ISR who process information with respondent identifiers, such as for data entry or respondent location services, must comply with the same rules as ISR employees. It is the responsibility of ISR project directors to secure signed Pledges from such affiliates attesting that they will comply with this Policy, and that they will return all originals and copies of any ISR data provided to them. The relevant ISR employees assigned to a project have the responsibility to monitor the compliance with this Policy of affiliates. Affiliates have the same responsibility to secure signed Pledges from all outside contractors they use related to the ISR project or data and to provide such signed Pledges to the applicable ISR project director.

Research documents such as completed questionnaires, coversheets, data tapes, printouts, photocopies, electronic files, or any other documents, specimens or electronic media with respondents' names or other identifying information must be stored securely, used exclusively in a manner for which they were intended, and disposed of in a secure manner. Computers containing respondent information should at a minimum be kept in locked offices and password protected. Respondent information contained on computers should be labeled and segregated for ease of retrieval and for assurance that the required confidentiality of the information is known. Encryption of confidential data is good practice when such information must be transferred over the internet or any public network. Employees should consult with ISR computing staff to ensure the appropriate disposal of confidential information maintained electronically.

All employees and affiliates are responsible for the security of any associated user ID (log in) and password for all applications to which they are granted access. Employees and affiliates must maintain security of all accounts, passwords and other information; unattended documents or workstations must be secured and user IDs and passwords must not be shared with others.

(3) *Data Dissemination:* The utmost care must be taken to prevent the dissemination of research datasets containing information that would permit any respondent to be identified. Research results must be presented only in summary form without names or other identifying information. Unrestricted public use data sets must be anonymized, and every effort must be made to prevent deductive identification of respondents. Where such deductive identification seems a realistic possibility, special restrictions must be placed on access to the data to protect anonymity and confidentiality of respondents.

ISR staff must treat all information linked to identifiable respondents as protected information, except in those cases where respondents or organizations waive anonymity or confidentiality for specified uses. In such cases, respondent information will only be released for those specified uses. Sponsoring agencies will be provided with respondent names or other identifying data only if such release is clearly specified in the research proposal, and is specifically authorized in writing by respondents.

Procedures:

All employees and affiliates of ISR are required to read this Policy and sign the associated Pledge as a condition of their employment and affiliation.

All newly hired or appointed employees in ISR are required to sign the Pledge, as a condition of their employment, at the time of hiring. All hiring supervisors and primary research recruitment committees are required to communicate this Policy and the need for a signed Pledge during the recruitment process, so that all candidates are fully advised of this requirement early in the interviewing process.

All new affiliates are required to sign the Pledge as a condition of their affiliation with ISR, at the time of their affiliation. For contractors and their employees, the signing must be done at the time of the agreement to be affiliated with the ISR project which can occur in conjunction with the signing of the formal contract for their services, if such a contract will exist.

A special case exists where an ISR project director is supervising an ISR-funded project, the data or subjects of which are being utilized by University employees in another campus unit. Before those non-ISR employees can handle the data collected under ISR auspices, they must sign the ISR Pledge. An "equivalent" pledge provided by the campus unit is not sufficient.

The relevant Center Directors' offices (and the ISR Director's office for employees and affiliates not associated with any Center) are responsible for ensuring that all employees and affiliates renew the Pledge annually, and for keeping centrally copies of signed paper Pledges and access to electronically signed Pledges for those employees and affiliates (and any affiliate contractors) of their respective Center. The respective Center must retain paper copies and logs of electronically signed Pledges for at least the applicable year and thereafter must have a tracking method for verifying employee and affiliate attestations for past years.

Project directors and other relevant ISR employees are responsible for identifying affiliates (and affiliate contractors if applicable) in their areas subject to this Policy, reporting the names of those individuals to the relevant Center Director's office, and for forwarding all signed Pledges to those offices.