



Human Subjects Research Compliance Procedures

1. History of Human Subject Research Ethics	9
2. Legal Foundation for Review Requirements	10
3. The Institutional Review Board (IRB)	12
4. Scope of Western's IRB Review	12
5. What is Human Subject Research?	13
A. <i>What is Research?</i>	13
1. What is a systematic investigation?	13
2. What is generalizable knowledge?	14
3. Activities Deemed Not Research	15
B. <i>What constitutes human subjects?</i>	16
1. Definition: Intervention	16
2. Definition: Interaction	16
3. Definition: Private information	17
4. Definition: Identifiable	17
C. <i>Determining if Certain Projects Are Research</i>	17
1. Student Activities in the Classroom: Research or Not?	18

2.	Pilot Studies: Research or Not?	19
3.	Secondary Use of Data: Research or Not?	19
4.	Ethnographic Projects: Research or Not?	20
5.	Internet-Based Activities: Research or Not?	21
	a) Am I working with human subjects?	21
	b) What is considered public online?	21
	c) What is private identifiable information on the internet?	23
	d) What is intervention or interaction online?	24
6.	Who Submits for IRB Approval?	24
A.	<i>Faculty (tenure and non-tenure track) & Staff</i>	25
B.	<i>New Faculty Transferring Ongoing Research</i>	25
C.	<i>Students</i>	25
D.	<i>Non-Affiliated Researchers Collecting Data at WWU</i>	25
E.	<i>Collaborators</i>	26
7.	Levels of IRB Review	27
A.	<i>Exempt Research</i>	27
	Category 1: Normal Educational Practices & Settings	27
	Category 2: Educational Tests, Surveys, Interviews, or Observations	28
	Category 3: Benign Behavioral Interventions	29
	Category 4: Secondary Research	31
	Category 5: Public Benefits or Service Programs	32
	Category 6: Taste & Food Evaluation and Acceptance Studies	33
	Category 7: Broad Consent Storage or Maintenance	33
	Category 8: Broad Consent Secondary Research	33

WWU Category A: Benign Behavioral Interventions	34
WWU Category B: Benign Surveys or Interviews with Minors	34
<i>B. Expedited</i>	35
Category 1: Drugs & Medical Devices	35
Category 2: Blood Samples	35
Category 3: Non-invasive Biological Specimen Collection	35
Category 4: Non-invasive Procedures	36
Category 5: Secondary Data	36
Category 6: Voice, Video, Digital, or Image Recordings	37
Category 7: Survey, Interview, Focus Groups	37
Category 8: Continuing Review of Certain Research	38
Category 9: Continuing Review of Minimal Risk Investigational Drug or IDE Research	38
<i>C. Full Board</i>	39
8. Research Guidance by Project	39
<i>A. Student Conducted Research</i>	39
<i>B. Use of Student Education Records</i>	39
<i>C. Research in K-12 Schools</i>	40
<i>D. Research in University Classrooms</i>	41
1. Protection against possible coercion	41
a) Dual role researchers/faculty do not consent subjects	42
b) Consent after grades are submitted	42
c) Separate written consent forms from data	42
2. Incentives (Credit vs Extra Credit)	43

3.	The Family Educational Rights and Privacy Act (FERPA)	44
E.	<i>Ethnographic Research</i>	45
F.	<i>International Research</i>	45
G.	<i>Cross-cultural and International Research</i>	46
H.	<i>NIH Funded Clinical Trials</i>	47
9.	Vulnerable Populations	48
A.	<i>Minors</i>	48
1.	Parental/Guardian Permission	49
2.	Child Assent	49
3.	Protection of Pupil Rights Amendment (PPRA)	50
4.	Protection of Minors on Campus	50
B.	<i>Prisoners</i>	51
C.	<i>People with Diminished Capacity for Consent</i>	51
10.	Informed Consent	52
A.	<i>Requirements</i>	52
B.	<i>Best Practices for the Consent Process</i>	54
C.	<i>Best Practices for Consent Forms</i>	54
D.	<i>Methods of Consent</i>	55
1.	Written Consent	55
a)	When Read By the Subject	55
b)	When Read to the Subject	56
2.	Waiver of Documentation of Consent: IRB Approval Required	57
a)	Electronic consent	57
b)	Verbal consent	58

c) Implied Consent	59
3. Waiver of Consent: IRB Approval Required	59
4. Broad Consent	59
<i>E. Deception & Incomplete Disclosure</i>	<i>60</i>
1. What is deception?	60
2. What is incomplete disclosure?	61
3. When is it possible to use deception or incomplete disclosure?	61
4. What is debriefing and when is it necessary in a study?	62
5. How do you conduct a debriefing?	63

11. Research Subject Incentives 64

<i>A. How much can I give?</i>	<i>65</i>
<i>B. Requirements</i>	<i>65</i>
<i>C. Incentive Methods</i>	<i>66</i>
<i>D. Incentive Documentation</i>	<i>67</i>
<i>E. Incentive Tax Reporting</i>	<i>68</i>
1. Payments Requiring Reporting	69
2. Reporting Process	69
3. Payments made in other countries	70
4. Payments to Foreign Nationals	70
<i>F. Incentive Requests and Approval</i>	<i>71</i>
<i>G. Payment Process</i>	<i>71</i>
1. Electronic Gift Cards	71
2. Cash	72
3. Physical Gift Cards	72

12.Data & Security Protections	73
<i>A. How Does This Work?</i>	73
1. Identify your data sensitivity.	73
2. Identify the protections required for that data sensitivity level.	74
<i>B. Data Sensitivity</i>	74
1. Level 1 Data	74
2. Level 2 Data	75
3. Level 3 Data	75
4. Level 4 Data	75
<i>C. Data Protections</i>	76
1. Limit Access (Levels 2 – 4)	76
2. Passwords (Levels 2 – 4)	77
3. Data in Motion (Level 2 – 4)	78
4. Data at Rest (Level 2 – 4)	79
5. Data Storage Options	80
a) Network Storage	80
b) Cloud Storage	81
c) Commercial Services (MTurk, SurveyMonkey, etc.)	81
<i>D. Certificate of Confidentiality</i>	82
<i>E. Identifiable Information</i>	82
<i>F. De-identification</i>	83
<i>G. Protected Health Information</i>	84
<i>H. Health Insurance Portability and Accountability Act (HIPAA)</i>	84
<i>I. Anonymous vs Confidential: Describing Data Protections</i>	86

13. Protocol Submission Process	87
A. <i>Ethics Training</i>	87
B. <i>Complete an Application</i>	88
C. <i>Preliminary Review & Screening</i>	89
D. <i>Review & Determination</i>	90
1. Exempt Review	90
2. Exempt Limited Review	91
3. Expedited Review	91
4. Full Board Review	92
E. <i>Appeal of IRB Determination</i>	93
14. Open Research Applications	93
A. <i>Extending Your Research</i>	93
B. <i>Requesting Changes</i>	94
1. Changes Requiring Approval	94
2. How to request a modification	95
C. <i>Unanticipated Problems</i>	95
D. <i>Non-Compliance</i>	96
1. Levels of Non-Compliance	97
a) Minor Non-Compliance	97
b) Serious Non-Compliance	98
c) Continuing Non-Compliance	98
2. Reporting Non-Compliance	98
3. Investigations of Non-Compliance	99
E. <i>Data and Records Retention</i>	99

F.	<i>Study Closure</i>	101
G.	<i>Data Destruction</i>	101
15.	Research Misconduct	101
16.	Appendix A: How to Conduct Internet-Based Research	103
A.	<i>Internet Privacy</i>	103
B.	<i>Online Survey Considerations</i>	104
1.	Consent	104
2.	Eligibility requirements	105
3.	Optional Questions	105
C.	<i>Recommendations for Platforms</i>	105
1.	Qualtrics	105
2.	Sona	106
a)	Recruitment	106
b)	Consent	106
c)	Data Security	106
3.	Amazon Mechanical Turk Guidance	106
a)	Recruitment	107
b)	Consent	107
c)	Data Security	107
D.	<i>Chat Rooms & Support Groups</i>	108
E.	<i>Social Media Research (Twitter, Facebook, Etc.)</i>	108
F.	<i>Skype Research</i>	109
17.	Appendix B: Security: OneDrive vs. Google Drive	109
18.	Appendix C: Survey Monkey Security	116

1. History of Human Subject Research Ethics

Research with human subjects has a troubling history of abuse and ethics violations. We teach researchers about this history in order to provide the context for the laws that exist today.

There are several well-known examples of research abuse. During World War II the Nazis conducted experiments on concentration camp prisoners. From 1932 to 1972, the researchers from the U.S. Public Health Service at the Tuskegee Institute deceived and denied effective treatment to black males who suffered from syphilis. Stanley Milgram conducted research on authority and obedience by deceiving subjects into believing they were administering increasingly strong electric shocks to a second subject (who was actually a hired actor) every time that individual answered a question incorrectly. In many cases the subjects were led to believe they had seriously hurt or even killed the fellow participant.

The World War II criminal trials led to the creation of the Nuremberg Code, which outlines ten points for conducting ethical research. Three basic elements of this code included voluntary informed consent, favorable risk/benefit analysis, and the right to withdraw without repercussions.

In 1964, the World Medical Association established the Declaration of Helsinki, which is a set of ethical principles specifically regarding medical research.

Further research abuses led to the adoption of The Belmont Report in 1979. This report requires three essential principles in research: beneficence, justice, and autonomy. Under these principles, subjects must not be

subjects of convenience, they must be apprised of the risks and benefits of participation and they must have the right to decline to participate.

Ultimately, the National Institutes of Health (NIH) created the Common Rule (45 CFR § 46), regulations that establish the legal basis regulating human subject research.

[Skip to Next Section](#)

[Go to the Top](#)

2. Legal Foundation for Review Requirements

Review of human subject research takes into account all applicable laws, policies, procedures, and guidelines. These include:

- [The Belmont Report](#)
- [Code of Federal Regulations Title 46 Part 46 \(45 CFR 46\)](#) aka “[The Common Rule](#)”
- [Western Institutional policies and procedures](#), as applicable
- State policies
 - Abuse of Vulnerable Adults [RCW 74.34](#)
 - Abuse of Children [RCW 26.44](#)
 - Abuse of Patients [RCW 70.124](#)

- Confidentiality of Prescription Information [RCW 70.225.040](#) (section 4)
- Release of Records for Research [RCW 42.48](#)
- Medical Records Health Care Information Access and Disclosure [RCW 70.02](#)
- Newborn Screening - Privacy and Security [WAC 246-650-050](#)
- Notifiable Conditions [WAC 246-101](#)
- Protection of Human Research Subjects [WAC 388-04](#)
- Research with Vital Records:
 - Release of Records [RCW 70.58.082](#)
 - Disclosure for Research Purposes [RCW 70.58.104](#)
 - Requesting a listing or file with Personal Identifiers [WAC 246-490-030](#)
 - Requesting Records without Personal Identifiers [WAC 246-490-020](#)
- If applicable, tribal law passed by the official governing body of an American Indian or Alaska Native tribe
- Federal policies, as applicable
 - [FDA regulations](#), as applicable
 - [NIH regulations](#), as applicable
 - And more, depending on your particular research

3. The Institutional Review Board (IRB)

The Institutional Review Board (IRB) is a committee that reviews human subject research for compliance with federal regulations.

4. Scope of Western's IRB Review

WWU IRB approval is required prior to conducting any research involving human subjects when WWU is considered "engaged" in the research.

"Engaged" is a federal term that refers to whether or not the institution is involved in the research. Western is engaged in the research if any of the following are true:

1. WWU is receiving federal funding for the research (including salaries) through a grant, contract, or cooperative agreement directly from an agency.
2. WWU faculty, staff, or students:
 - Perform any research procedures with subjects (interacting with subjects, obtaining informed consent, manipulating the subject's environment for research purposes) or

- Obtain identifiable private information or biological specimens from any source even if there is no direct interaction.
3. The research satisfies a requirement imposed by the University for an honors or a graduate degree program

[Skip to Next Section](#)

[Go to the Top](#)

5. What is Human Subject Research?

The federal guidelines define what is considered “research” and a “human subject”.

A. What is Research?

Research is a **systematic investigation** – including research development, testing and evaluation – designed to develop or contribute to **generalizable knowledge**. This includes pilot research.

1. What is a systematic investigation?

A systematic investigation includes:

- An attempt to answer a research question,
- Methodologically driven activity (it collects data or information in a way that is organized and consistent),

- Analyzing data or information in some way (quantitative or qualitative), AND
- Drawing conclusions from the results.

2. What is generalizable knowledge?

Generalizable knowledge is when:

- The knowledge contributes to a theoretical framework of an established body of knowledge
- The results are expected to be generalized to a larger population beyond the site of data collection or population studied
- The results are intended to be replicated in other settings
- Publication, presentation, or other distribution of the results can be an indicator of generalizing knowledge, however it is possible to publish and present projects that are not considered research

Examples of activities that typically are not generalizable include:

- biographies
- service or course evaluations, unless they can be generalized to other individuals
- services, or concepts where it is not the intention to share the results beyond WWU or any agency supporting the research

- quality assurance activities designed to continuously improve the quality or performance of a department or program where it is not the intention to share the results beyond the WWU community.

3. Activities Deemed Not Research

Certain activities are deemed not to be research. These include:

- Scholarly and journalistic activities (oral history, journalism, biography, literary criticism, legal research, and historical scholarship) that focus directly on the specific individuals about whom the information is collected.
- Collection and testing of information or biospecimens, conducted, supported, requested, ordered, required, or authorized by a public health authority. These activities are limited to those necessary to allow a public health authority to identify, monitor, assess, or investigate potential public health signals, onsets of disease outbreaks, or conditions of public health importance.
- Collection and analysis of information, biospecimens, or records by or for a criminal justice agency for activities authorized by law or court order solely for criminal justice or criminal investigative purposes.
- Authorized operational activities (as determined by each agency) in support of intelligence, homeland security, defense, or other national security missions.

B. What constitutes human subjects?

A human subject is a living individual **about whom** an investigator conducting research either:

- obtains information or biospecimens through **intervention** or **interaction** with the individual, and uses, studies, or analyzes the information or biospecimens; or
- obtains, uses, studies, analyzes, or generates **identifiable private information or identifiable biospecimens**.

1. Definition: Intervention

Intervention includes both:

- procedures by which information or biospecimens are gathered (for example, collection of survey data, measurement of heart rate, or venipuncture) and
- manipulations of the subject or their environment that are performed for research purposes.

2. Definition: Interaction

Interaction includes communication or interpersonal contact between the investigator and subject (for example, surveying or interviewing), whether online or in-person.

3. Definition: Private information

Private information includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation is taking place, or information that has been provided for specific purposes by an individual and the individual can reasonably expect will not be made public (for example, a medical record).

4. Definition: Identifiable

Identifiable means that the identity of the subject is or may be readily ascertained by the investigator or associated with the information (e.g., by name, code number, pattern of answers, IP addresses, etc.). For a more detailed explanation please see the [Identifiable Information](#) section.

Data may also be considered identifiable if it is possible, through deduction, to identify subjects. For example, it may be possible in a smaller population to easily deduce who gave a particular quote. However, the IRB will need to take into account the likelihood of identification in each scenario. In the world of Big Data, it has been shown that cross-correlation between data sets can be used to re-identify subjects, though the likelihood of this occurring depends on the researcher and the data set.

C. Determining if Certain Projects Are Research

Some types of projects may or may not be considered human subjects research.

1. Student Activities in the Classroom: Research or Not?

Some classroom research projects do not require IRB review. A project is not considered "research" when:

- The exercise is solely to fulfill course requirements or to train students in the use of particular methods or devices AND
- The results will never be generalized and/or distributed outside the classroom and/or institutional setting AND
- The project involves minimal risk to subjects AND
- The project does not involve vulnerable populations.

Keep in mind that masters and honors theses are automatically published in CEDAR, an online public archive, which is considered generalizing knowledge.

In classroom projects, even though IRB review is not required, the ethical principles of [The Belmont Report](#) still apply. The instructor is responsible for informing students about these principles including the elements of informed consent.

Students can choose to submit classroom research projects for IRB review if they are interested in generalizing and/or publishing the results. This submission should be done prior to data collection. If a student does not obtain approval prior to data collection they cannot present at a conference even if the research was originally just performed as a classroom assignment.

2. Pilot Studies: Research or Not?

Pilot research that meets the definition of “human subjects research” must be reviewed by the IRB with the same scrutiny as a full-scale research project even though it may be conducted with a small number of subjects.

3. Secondary Use of Data: Research or Not?

Some activities involving using, studying, or analyzing secondary data are not considered human subjects research. These regulations can be read in full in Office of Human Research’s (OHRP’s) [Coded Private Information or Specimens Use in Research, Guidance](#).

OHRP does not consider research involving **only** coded private information or specimens to involve human subjects research if the following conditions are both met:

- the private information or specimens were not collected specifically for the currently proposed research project through an interaction or intervention with living individuals; **and**
- the investigator(s) cannot readily ascertain the identity of the individual(s) to whom the coded private information or specimens pertain because, for example:
 - o the investigators and the holder of the key (the link between data and identifiers) enter into an agreement prohibiting the release of the key to

the investigators under any circumstances, until the individuals are deceased

- there are IRB-approved written policies and operating procedures for a repository or data management center that prohibit the release of the key to the investigators under any circumstances, until the individuals are deceased; or
- there are other legal requirements prohibiting the release of the key to the investigators, until the individuals are deceased.

If the dataset intended for secondary use contains identifiers or can be linked back to identifiers, then that **would** be considered human subjects research. However, the project may be eligible for review under an exempt category.

4. Ethnographic Projects: Research or Not?

Ethnographic Research occurs when a researcher participates, overtly or covertly, in people's daily lives for an extended period of time. They may be watching what happens, listening to what is said, asking questions and/or collecting data to create a broader understanding of a particular environment, ethnic group, gender, etc. Ethnographic research **does** need to be reviewed by the IRB. See additional guidance on [Ethnographic Research](#).

5. Internet-Based Activities: Research or Not?

In some cases, it is easy to apply the federal definition of human subjects research to online data collection. In others, the line may not be so clear. In this section we discuss some situations where it may be tricky to apply the federal definition of human subjects research. For a more in-depth discussion of these issues you can refer to a document written by SACHRP in March 2013 titled "[Considerations and Recommendations Concerning Internet Research](#)".

a) *Am I working with human subjects?*

If you are working with avatars, they are considered human subjects if personally identifiable information about living individuals can be obtained by observing the actions of, or interacting with them. Computer-generated characters, on the other hand, would not be considered human subjects.

b) *What is considered public online?*

Collecting publicly available information online, as long as there is no interaction or intervention with participants, is not considered human subjects research. It can be difficult in some circumstances, however, to determine if information is publicly available.

The Secretary's Advisory Committee on Human Research Protections (SACHRP) suggests using the analogy of a public park when thinking about whether data online is public. If information is accessible by anyone online, without specific permission or authorization, this can likely be considered public and would not require IRB review to collect. However, just as eavesdropping may not be

considered appropriate in a public park, monitoring some internet-based activities for research may not be appropriate without IRB review. Researchers should consider the terms of service and the norms of the virtual space. When a group or space requires access logins or moderators, this may not be public information.

Public sites tend to fall into these categories:

- Sites containing information that is by law considered public. In most cases information from these sites is available without restriction, although access may require paying a fee. Many federal, state, and local government sites are in this category. This includes property tax records, birth and death records, real estate transactions, certain court records, voter registration, and voting history records.
- News, entertainment, classified, and other information-based sites where a login is not required and information is posted for the purpose of sharing with the public.
- Open access data repositories, where information has been legally obtained and is made available with minimal or no restriction.
- Discussion forums that are freely accessible to any individual with internet access and do not involve terms of access or terms of service that would restrict research use of the information.

If you are unsure about whether the data is public or private, continue reading the section below.

c) *What is private identifiable information on the internet?*

Please see our [definition of private identifiable information](#). Information that is not considered public according to the discussion above, should be considered private.

The researcher should take into account:

- the privacy policies and terms of service of the entity receiving or hosting the information posted by individuals. If the information/data online is freely accessible to anyone with internet access (without requiring user registration, login, password, etc) this is considered to be analogous to information that is observable in physical public spaces, so long as de-identification and aggregation practices are part of the research design.
- the subject's expectation of privacy. Generally, any venue that is moderated or whether membership or password is involved, should be considered private.
- the subject's expectation about whether the information will be made public. Sites where the purpose is to present participants' comments for public review (such as comments sections of articles or videos) are considered public.
- the norms of the virtual space. If the expressed norms of requests in a virtual space lean towards privacy, this

should be taken into account, though it may not be legally binding.

When in doubt, please consult with a Research Compliance Officer.

d) *What is intervention or interaction online?*

Online intervention or interaction with subjects takes the form of anything mimicking real-world intervention/interaction. Interventions online include testing website interfaces, recording internet-based activities, using the internet as a reminder or interface for some activity. Interactions online include communication through email, text, in virtual worlds, social media, chat rooms, newsgroups, and mobile platforms. Surveys are considered interaction even though there is no live individual receiving responses in real time, but data are collected for later access by the investigator.

[Skip to Next Section](#)

[Go to the Top](#)

6. Who Submits for IRB Approval?

When WWU is engaged in human subjects research, an IRB application must be submitted. Those submitting applications can include:

A. Faculty (tenure and non-tenure track) & Staff

Please see the section included in this handbook on the extra protections that must be in place for faculty utilizing students as subjects in research.

B. New Faculty Transferring Ongoing Research

A copy of the original research protocol and approval from their previous institution must be provided to the IRB. The WWU IRB will review and determine whether it will require an independent review of the research requiring a new protocol submission.

C. Students

Undergraduate and graduate students are encouraged to conduct research at Western. Students may be listed as Principal Investigators on the application, but a Faculty Advisor is required.

Faculty are expected to take an active role in educating students in the review process and maintaining study integrity for the entire research experience.

D. Non-Affiliated Researchers Collecting Data at WWU

Researchers must submit an application to the WWU IRB to collect data at WWU.

E. Collaborators

Researchers often collaborate with other institutions on research projects.

If Western is not considered engaged in the research, the WWU IRB does not require review and approval. For example, if a WWU faculty member is only receiving de-identified data (where there is no link back to identifiable information), this would not meet the definition of human subjects research and as such would not require review.

If the lead PI between research collaborators is a Western faculty, staff, or student member the WWU IRB will prefer to conduct their own review of the research.

If the Western faculty, staff, or student member is not the lead PI between the research collaborators, the WWU IRB may be able to defer to the review and approval of another institution's IRB. In order to submit a request for a deferral, please email compliance@wwu.edu with a description of the study and the institution that would be providing review. If you have already received approval from a separate IRB, attach the complete approval packet. The WWU IRB will consider each situation individually.

[Skip to Next Section](#)

[Go to the Top](#)

7. Levels of IRB Review

There are three levels of IRB protocol review, assigned based on the tasks involved, the subject population, and level of risk. The IRB will determine the level of review upon receipt of the application.

A. Exempt Research

Six categories of research may qualify for exempt status under the federal regulations. Western has additional exemption categories that are applicable to non-federally funded research.

At WWU an exemption means that the research does not need to meet certain Common Rule regulations and requires minimal continuing oversight by the IRB. Please see our [information about open applications](#) below for more information.

Only the IRB has the authority to determine whether research involving human subjects is exempt from full review. Exemptions are not guaranteed and may be denied by the IRB.

Research involving the Food and Drug Administration or prisoners are not eligible for exemption.

The categories of exempt research include:

Category 1: Normal Educational Practices & Settings

Research conducted in established or commonly accepted educational settings that specifically involves **normal educational practices** that are not likely to adversely impact students' opportunity to learn required education content or the assessment of educators who

provide instruction. This includes (i) most research on regular and special education instructional strategies, or (ii) research on the effectiveness of or the comparison among instructional techniques, curricula, or classroom management methods.

Category 2: Educational Tests, Surveys, Interviews, or Observations

Research that **only** includes interactions involving educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures or observation of public behavior (including visual or auditory recording), if one of the following is met:

Criteria 1:

Information obtained is recorded by the investigator in such a manner that the identity of the human subjects cannot be readily ascertained, directly or through identifiers linked to the subjects.

Criteria 2:

- Any disclosure of the human subjects' responses outside the research **would not** reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, educational advancement, or reputation. **OR**
- In the event that disclosure may reasonably place the subjects at risk, and the information obtained is identifiable, the IRB conducts a [limited review](#).

Research with [minors](#) may only be considered for this category if the investigator is observing public behavior and not participating in the activities being observed. This type of research with minors may be eligible under [WWU's Exempt Category B](#).

Not all interviews require IRB review. For example, if a historian is interviewing a holocaust survivor about her memories and how it impacted her life it is not research because it is not generalizable knowledge and hence not "human subject research". However, if the researcher is researching several holocaust survivors regarding their experience and how it impacted their subsequent relationships, it would probably be categorized as generalizable knowledge thus requiring IRB review and approval.

Note that if a task is involved in addition to the survey or interview, this makes a study ineligible for Category 2, though it may be eligible under Category 3. Activities that are simply part of answering the survey or interview, such as writing responses, will not be considered tasks.

Category 3: Benign Behavioral Interventions

Research involving benign behavioral interventions in conjunction with the collection of information from an **adult subject** through **verbal or written responses (including data entry) or audiovisual recording** if the subject **prospectively agrees** to the intervention and information collection as long as:

- The intervention is brief in duration, harmless, painless, not physically invasive, not likely to have a significant adverse lasting impact on subjects, and the investigator has no reason to think the subjects will find the interventions offensive or embarrassing;

- The research procedures cannot involve collection of biological specimens, exercise procedures, or the physical assessment of subject's physical characteristics;
- If the research involves deceiving the subjects regarding the nature or purposes of the research, the subject must authorize the deception (that they will be unaware of or misled regarding the nature or purposes of the research) through a prospective agreement; AND
- One of the following is criteria is met:

Criteria 1:

Information obtained is recorded by the investigator in such a manner that the identity of the human subjects cannot be readily ascertained, directly or through identifiers linked to the subjects.

Criteria 2:

If the subjects are identifiable, any disclosure of the human subjects' responses outside the research **would not** reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, educational advancement, or reputation.

Criteria 3:

If subjects are identifiable, and the questions are sensitive, the IRB conducts a [limited review](#).

If the research involves anthropometric measurement, collection of vital signs, or deception without prospective agreement, it may still be eligible for exemption under [WWU Exempt Category A](#).

Category 4: Secondary Research

Secondary research uses of identifiable private information or identifiable biospecimens, if at least one of the following criteria is met:

- these sources are publicly available;
- the information is recorded by the investigator in such a manner that the identity of subjects cannot readily be ascertained directly or through identifiers linked to the subjects, the investigator does not contact the subjects, and the investigator will not re-identify subjects;
- The research involves only information collection and analysis involving the investigator's use of identifiable health information is for the purpose of "health care operations" or "public health activities and purposes"; OR
- The research is conducted by, or on behalf of, a Federal department or agency using government-generated or government-collected information obtained for nonresearch activities, if the research generates identifiable private information that is or will be maintained on information technology that is subject to and in compliance with the E-Government Act of 2002, if all of the identifiable private information collected, used, or generated as part of the activity will be maintained in systems of records subject to the Privacy Act of 1974, and, if applicable, the information used in the research was collected subject to the Paperwork Reduction Act of 1995.

Please see the Use of Secondary Data section if the dataset being obtained/used does not contain or is in no way linked to identifiable private information.

If the researcher records coded data, with a number that links back to identifying information, this would not be eligible for this exemption category, but may be eligible for Expedited Category 5.

Category 5: Public Benefits or Service Programs

Research and demonstration projects that are conducted or supported by a Federal department or agency, or otherwise subject to the approval of department or agency heads (or the approval of the heads of bureaus or other subordinate agencies that have been delegated authority to conduct the research and demonstration projects), and that are designed to study, evaluate, improve, or otherwise examine: (i) Public benefit or service programs; (ii) procedures for obtaining benefits or services under those programs; (iii) possible changes in or alternatives to those programs or procedures; or (iv) possible changes in methods or levels of payment for benefits or services under those programs. Such projects include, but are not limited to, internal studies by Federal employees, and studies under contracts or consulting arrangements, cooperative agreements, or grants.

Each Federal department or agency conducting or supporting the research and demonstration projects must establish, on a publicly accessible Federal website or in such other manner as the department or agency head may determine, a list of the research and demonstration projects that the Federal department or agency conducts or supports under this provision. The research or demonstration project must be published on this list prior to commencing the research involving human subjects.

Category 6: Taste & Food Evaluation and Acceptance Studies

Taste and food quality evaluation and consumer acceptance studies, (i) if wholesome foods without additives are consumed or (ii) if a food is consumed that contains a food ingredient at or below the level for a use found to be safe, or agricultural chemical or environmental contaminant at or below the level found to be safe, by the Food and Drug Administration or approved by the Environmental Protection Agency or the Food Safety and Inspection Service of the U.S. Department of Agriculture.

Category 7: Broad Consent Storage or Maintenance

Storage or maintenance of identifiable private information or identifiable biospecimens for secondary research for which broad consent is required. The IRB must conduct a "[Limited Review](#)".

Category 8: Broad Consent Secondary Research

Research involving the use of identifiable private information or identifiable biospecimens for secondary research use if the following criteria are met:

- Broad consent is obtained and documented;
- An IRB [Limited Review](#) is conducted to determine that the research is within the scope of the broad consent; AND
- The investigator does not include returning individual research results to subjects as part of the study plan. This provision does not prevent an investigator from abiding by any legal requirements to return individual research results.

WWU Category A: Benign Behavioral Interventions

Non-federally funded research that would otherwise meet the requirements for Exempt Category 3, except:

- The study includes anthropometric data collection or vital signs. **AND/OR**
- If the research involves deceiving the subjects regarding the nature or purposes of the research, and the researcher is able to demonstrate that the integrity of the research will be affected in a material, negative way by informing the subject prospectively that they will be will be unaware of or misled regarding the nature or purposes of the research.

WWU Category B: Benign Surveys or Interviews with Minors

Non-federally funded research with minors, which would otherwise be eligible under Exempt Category 2 with an adult population, involving survey or interview procedures on benign topics. In order to be considered for this category, the following should be true:

- Parental permission and child assent must be obtained. An exception is made for students under 18 years old enrolled at Western Washington University unless FERPA or PPRA applies to the research.
- Survey topics **cannot include**: political affiliations or beliefs of the minor, mental or psychological problems, sex behavior or attitudes, sexual orientation, illegal, antisocial, self-incriminating, or demeaning behavior.

B. Expedited

To qualify for expedited review, a research procedure must be limited to the activities that are federally approved for expedited review and incur no more than minimal risk for subjects.

Minimal risk is defined as “the probability and magnitude of harm or discomfort anticipated to be experienced by the participant are not greater in and of themselves than those ordinarily encountered in daily life or during the performance of routine physical or psychological examination or tests”.

There are nine categories for expedited review. These categories are:

Category 1: Drugs & Medical Devices

Clinical studies of drugs and medical devices under limited circumstances.

Category 2: Blood Samples

Collection of blood samples by finger stick, heel stick, ear stick, or venipuncture under certain circumstances.

Category 3: Non-invasive Biological Specimen Collection

Prospective collection of biological specimens for research purposes by noninvasive means, like hair and nail clippings or saliva.

Category 4: Non-invasive Procedures

Collection of data through noninvasive procedures (not involving general anesthesia or sedation) routinely employed in clinical practice, excluding procedures involving x-rays or microwaves. For example:

- a researcher utilizing physical sensors that are applied either to the surface of the body or at a distance and do not involve input of significant amounts of energy into the subject or an invasion of the subject's privacy, such as in Kinesiology research
- weighing or testing sensory acuity
- magnetic resonance imaging (MRI)
- electrocardiograph (EKG), electroencephalography (EEG), thermography, ultrasound,
- moderate exercise, muscular strength testing, body composition assessment, and flexibility testing where appropriate given the age, weight, and health of the individual

While this category is appropriate for research involving moderate exercise of normal, healthy subjects, an application would rise to the level of full review if the subjects were infirm and/or subjected to an intense or dangerous exercise.

Category 5: Secondary Data

Research involving materials (data, documents, records, or specimens) that have been collected, or will be collected solely for non-research purposes (such as medical treatment or diagnosis).

This expedited category differs from Exempt Category 4 in that it allows for the use of specimens that may not currently exist. All data used under Exempt Category 4 must be existing or already “on the shelf” before the research begins. This expedited category also allows researchers to record and keep identifiers.

Examples of the types of secondary data that might be used under this category include data from previous research studies or health records.

Category 6: Voice, Video, Digital, or Image Recordings

Collection of data from voice, video, digital, or image recordings made for research purposes.

These data collection types are allowable under certain exemption categories, so this expedited category is rarely utilized.

Category 7: Survey, Interview, Focus Groups

Research on individual or group characteristics or behavior (including, but not limited to: research on perception, cognition, motivation, identity, language, communication, cultural beliefs or practices, and social behavior) or research employing survey, interview, focus group, program evaluation, human factors evaluation, or quality assurance methodologies.

Category 7 can include research that is not eligible for Exempt Category 2 due to a link between identifiers and data as well as possible risk to a participant’s reputation, employability, etc.

Category 8: Continuing Review of Certain Research

Continuing review (also referred to as Status Reports) of research previously approved by the convened IRB where:

- the research is permanently closed to the enrollment of new subjects;
- all subjects have completed all research related interventions, and
- the research remains active only for the long term follow-up of subjects. The renewal process will be described in more detail in a subsequent section.

Category 9: Continuing Review of Minimal Risk Investigational Drug or IDE Research

This category refers to research that required full board review initially and has already received approval. During continuing review, when the application needs to be renewed each year, status reports may be reviewed as expedited projects when:

- the research is not conducted under an investigational new drug application or investigational device exemption AND
- categories two through eight do not apply AND
- the IRB has determined and documented at a convened meeting that the research involves no greater than minimal risk AND
- no additional risks have been identified.

C. Full Board

If a study is greater than minimal risk or cannot be categorized as exempt or expedited, it must be reviewed by the full convened IRB committee.

If a protocol goes to full board for review, the board may request the researcher to come to a brief portion the meeting to address any questions. If the Principal Investigator is a student, the Faculty Advisor must be present.

[Skip to Next Section](#)

[Go to the Top](#)

8. Research Guidance by Project

A. Student Conducted Research

Students should work closely with their faculty advisor to ensure that their research methods are sound, ethical principals have been met, and their application is complete. Both the student and their faculty advisor are responsible for the conduct of the research.

B. Use of Student Education Records

Family Educational Rights & Privacy Act ([FERPA](#)) is a federal law that protects the privacy of student education records. FERPA is regulated by the Registrar's Office, not the WWU IRB.

Western has extended the protections of FERPA to include personally identifiable information such as student names, ID numbers, and contact information. Please read [Western's Summary of FERPA](#), which includes a description of what constitutes a student education record.

Student education records are confidential and may not be released without written consent of the student, or with parental permission if the student is under 18 years old, except by certain provisions outlined in FERPA.

When obtaining consent to release education records, the form must include [the following information](#).

If you are intending to request education record information from the Registrar's Office to conduct research, we recommend consulting with them as soon as possible. The Registrar's Office reviews studies on a case by case basis to determine if the disclosure is justifiable. The Registrar's Office approval is not guaranteed.

The IRB will require documentation of clearance from the Registrar's Office prior to approval. This can be in the form of an email or letter.

C. Research in K-12 Schools

All research conducted in or with K-12 schools/districts, including research interactions with school faculty, staff, or students, requires approval from the district or school prior to initiating research activity. Whether clearance can be obtained at the school level rather than the district level will depend on the district in question. We recommend consulting with the district in question.

The IRB will require this documentation of clearance/permission in order to approve this portion of your research activity.

This documentation is typically given in the form of a clearance letter. This letter must be signed by the administrator in charge of making decisions at the school site or capable of giving approval for the school. Email approval is possible as long as the email is sent from an institutional email address. The clearance letter should include:

- The protocol title,
- A brief description of the research activities that are approved to be conducted at the site,
- The person or entity providing permission including their title, contact information, and confirmation that they have appropriate authority to provide permission for the school or school district.

Please note that FERPA and PPRA may apply to your research.

D. Research in University Classrooms

Faculty are allowed to recruit students as subjects in research, but special protections must be in place.

1. Protection against possible coercion

Researchers who are in a position of authority over their participants must be particularly careful to avoid the appearance or possibility of coercion. The power dynamic between students and their professors/teachers requires careful consideration. When researchers have a dual role as professors or teachers, it is important that measures are taken to prevent any possibility

for coercion. Although you may feel like your research is not coercive, students may feel pressured to participate.

When using coursework in research, faculty with a dual role cannot know who opted in or out of the study until grades have been submitted to the Registrar's office at the end of the quarter. Depending on the chosen method of consent, there are options for how to achieve this:

a) *Dual role researchers/faculty do not consent subjects*

One method for preventing the possibility of coercion is to have another individual who is not in a position of authority conduct informed consent of the student subjects. If electronic consent is used, the other individual's Qualtrics account would have to be used to host the online survey.

b) *Consent after grades are submitted*

Consent can be obtained after grades have been submitted to use coursework as data. Your consent form would be written to describe what specific work would be included in the research.

c) *Separate written consent forms from data*

Researchers can use a written method of consent where the completed forms are placed in envelope, sealed, and not opened until after grades have been submitted.

2. Incentives (Credit vs Extra Credit)

Giving credit or extra credit is allowable for research in classrooms.

Just like with monetary compensation, the IRB will want to know the amount of course credit or extra credit you plan to offer, or an estimated range.

If you plan to offer course credit or extra credit as an incentive you must provide an alternative to participating in the research. This can include an assignment of the same effort and duration that will allow the student to earn the same level of course credit. Many professors will propose an alternate non-research option and also allow students to propose their own alternative for consideration.

The IRB is, as much as possible, attempting to standardize the research alternative across departments. The current standard alternative for 1 hour of research credit is an ungraded (pass/fail) 2-3 page written assignment based on a topic of choice or between an array of choices provided by the instructor. You can suggest other alternatives, however.

Research options and alternatives (course and extra credit) should be posted for all students to see. This could include the course syllabus and/or Canvas or another method to ensure that all students are given the same opportunity.

If all students receive course credit for an assignment and you only use the data of those who consented to participate in the research, this is not considered providing an incentive. In this case the consent form should specify that there is no incentive for participating.

3. The Family Educational Rights and Privacy Act (FERPA)

Please see the section above about [Use of Student Education Records](#).

If you are a professor, teacher, or similar role you normally have access to student education records, which include Western ID numbers, contact information, and any coursework. As soon as you access this information for research purposes, however, it becomes research data and requires separate consent for use and disclosure.

Recruitment can be tricky when considering FERPA regulations. For example, teachers are able to email their students about class matters. Faculty and staff, when acting as an “institutional official” (performing their duties as an employee), can use student education records, which include email addresses, for “legitimate educational use.” For example, teachers can email their students about class activities. Research recruitment, however, is not explicitly listed in FERPA as a “legitimate educational use.”

Teachers should consider the following points if they plan to disseminate research recruitment notices for research (their own or another person’s) using education record based email addresses:

- FERPA is not the jurisdiction of the IRB. While the IRB will give as much counsel and direction as possible, IRB approval of a research application does NOT relate to your responsibilities to FERPA.
- The Registrar’s Office is available for counsel.

- Go at your own risk. If a teacher uses education record based email addresses for research recruitment and there is a complaint, it will fall on that teacher to justify the use.

If the email addresses are received through a different method, not related to the students' education record, then FERPA does not apply. Classroom announcements in-person or on Canvas are common methods of recruitment that would not require FERPA consent.

E. Ethnographic Research

Unless you are working with a vulnerable population it is likely that ethnographic research will be eligible for an exemption. While ethnographic or anthropologic research is often evolving in nature, researchers will need to describe their research methods in the application in as much detail as possible. The IRB can approve a scope of questions or a starting point for interviews, rather than a specific study instrument or survey, as long as this is thoroughly described.

F. International Research

Research conducted outside of the United States will also be subject to the local laws and regulations of the country. These regulations vary and it is the investigator's responsibility to research and follow all applicable laws, policies, and procedures. Please review Office of Human Research Protections' (OHRP) [International Compilation of Human Research Standards](#).

For applications determined exempt, the WWU IRB will not require documentation of separate international IRB/ethics committee approval.

Study materials, including recruitment materials, consent forms, and survey instruments, need to be written in the language that will ensure the best comprehension for the research subjects. Your application should include information about how these materials are translated and how the researcher has ensured that the translations are appropriate.

G. Cross-cultural and International Research

Cultural Competence refers to understanding the importance of social and cultural influence on the beliefs and behaviors of the research subjects. Cultural competence is required in all contexts whether local, national, or international and requires more than just awareness of cultural differences. It is necessary both to exhibit respect for persons, but also to establish a trusting relationship between the subjects and the researcher.

While human subjects in foreign countries merit the same level of protection as subjects in the United States, acceptable practices vary from place to place. Different mores, traditions, and institutions may require different research practices, particularly relating to informed consent, recruitment practices, interview questions and documentation. Special attention should be given to local customs and to local cultural and religious norms in drafting consent documents.

In some cases, research projects must be approved by local experts or community leaders prior to IRB submission. This is often referred

to as gatekeeper consent. Leadership approval must be obtained prior to contact with the subjects. The IRB requires documentation of this "local approval" before it approves. Depending on the community, it may be the leadership of a Native American tribe, a village chief in an international setting, or the president of an organization. In their protocol, researchers should describe what, if any, knowledge or experience they possess regarding the language and culture of the country in question.

The proposed research must comply with the ethical rules of the country or community in which the research is conducted.

H. NIH Funded Clinical Trials

According to the NIH, clinical trial means a research study in which one or more human subjects are prospectively assigned to one or more interventions (which may include placebo or other control) to evaluate the effects of the interventions on biomedical or behavioral health-related outcomes.

For additional help in determining if your study meets this definition, please see the [NIH Definition of Clinical Trial Case Studies](#) document.

The NIH has specific requirements for posting clinical trial consent forms and results online. Please refer to your sponsor agency's website for additional information.

[Skip to Next Section](#)

[Go to the Top](#)

9. Vulnerable Populations

Certain populations are considered vulnerable in research and must be afforded special protections.

A. Minors

In research, a minor or child is someone who has not reached the legal age of consent for research procedures, according to the laws of where the research is conducted. In Washington State, the age of consent is 18 years old. The Principal Investigator is responsible for investigating the laws of the study location to determine the age of consent.

In some cases minors are allowed by law to consent to medical procedures without parental permission, such as use of contraceptives, treatment of sexually transmitted infections, and treatment of alcohol or drug abuse. If the research is using these medical procedures, the IRB may be able to waive the requirement for parental permission. This waiver would not apply to Food and Drug Administration (FDA) regulated studies.

For a full description of the protections around children in research, please read [The Office for Human Research Protection's FAQs on Research with Children](#).

For non-federally funded research that does not involve FERPA or PPRA, the WWU IRB will allow enrolled Western Washington University students to act as adults in research, regardless of whether they are under the age of 18.

Research with minors may be eligible for exemption, with some exceptions. Read through the [Exemption Categories](#) for these exceptions.

When conducting research with minors, researchers are required to get parental or guardian permission as well as child assent, if the child is considered capable.

1. Parental/Guardian Permission

A parent is a child's biological or adoptive parent. A guardian is an individual authorized under applicable laws to consent on behalf of the child. For the purpose of this handbook we will refer to both as guardians.

Guardian permission is required for minors to participate in research. This permission should be treated in the same way as informed consent.

If there are two guardians, typically permission is only required from one. There are some circumstances in higher risk research however that will require permission from both guardians.

There are special protections as well for children who are wards of the state. For more information, please read [The Office for Human Research Protection's FAQs on Research with Children](#).

2. Child Assent

In addition to parental consent, assent from the child is also required in many situations. "Assent" is an affirmative agreement from the child to participate in research. An

affirmative agreement means that the child is actively showing interest to participate rather than simply not resisting. Typically, minors aged 7 years or older are considered capable of providing assent.

The assent process should be developmentally appropriate for the age and maturity level of the child. The closer a minor gets to 18 years old, the more the assent process should resemble that of adults.

The federal regulations do not require documentation of assent, though the IRB may determine if a method of documentation is appropriate. Consider the maturity level of the minors involved when deciding whether documentation of assent is warranted.

3. Protection of Pupil Rights Amendment (PPRA)

The PPRA applies to any research funded by the US Department of Education or in public schools. It gives guardians controls over the content of research questions. For more information, please read the [PPRA](#).

4. Protection of Minors on Campus

If a researcher or staff person will be alone in a room with a child on Western's campus, without the accompanying guardian(s) having a direct line of sight at all times (either in person or via streaming video), that researcher is required to have a background check.

An exception is made for minors who are enrolled students at WWU.

B. Prisoners

If you are conducting research with prisoners please read [the Office for Human Research Protections Prisoner Research FAQs](#).

C. People with Diminished Capacity for Consent

There is no specific definition of a diminished capacity for consent. There are many conditions that might affect someone's ability to reason and make sound choices. An impairment may be temporary, stable, or changing over time. For example, someone with Alzheimer's or dementia may have a diminishing capacity to consent over time depending on the progression of their condition. Please work with the Research Compliance Office to determine whether your subjects may have a diminished capacity for consent.

Research with these populations must have some assessment of the capacity for consent included. They must carefully describe how comprehension will be ensured for the subject. Surrogate consent may be required.

For more information please read the [Office for Human Research Protections Recommendations Regarding Research Involving Individuals with Impaired Decision-making](#).

[Skip to Next Section](#)

[Go to the Top](#)

10. Informed Consent

Informed Consent is a process. The consent form is documentation of the process. The purpose of the process is to ensure that prospective subjects or their legally authorized representative are given all the information necessary to understand the research, the risks and benefits of participation, and their legal rights, as well as to allow sufficient time to ask questions and consider whether they would like to participate.

A prospective subject is an individual who has not yet consented to participate in the research. For the purposes of this manual (and brevity's sake), we will refer to "prospective subjects" as just "subjects".

A legally authorized representative means an individual or judicial or other body authorized by applicable law to consent on behalf of a prospective subject to the subject's participation in the procedure(s) involved in the research. If there is no applicable law, legally authorized representative means an individual recognized by institutional policy as acceptable for providing consent in the non-research context on behalf of the prospective subject. For the purposes of this section, when we say "subjects", that can also include the legally authorized representative.

Informed consent does not end when the consent form is signed or the study task has begun. Researchers have a responsibility to ensure that subjects have a continued understanding of the research procedures.

A. Requirements

Unless otherwise waived by the IRB, these are **required practices** for consent:

- Consent must be obtained from all subjects before initiating any research activities
- Treat informed consent as a process between the researcher and potential subject, rather than just a form
- Consent forms need to be written with language appropriate for the reader
- For federally funded research, informed consent must begin with a concise and focused presentation of the key information that is most likely to assist a subject in understanding the reasons why one might or might not want to participate in the research
- Consent forms must present sufficient detail relating to the research
- Consent forms must be organized and presented in a way that facilitates the subject's understanding of the reasons why one might or might not want to participate
- Informed consent may NOT include any exculpatory language through which the subject is made to waive any of their legal rights
- Informed consent may NOT include an exculpatory language that releases or appears to release the investigator, sponsor, the institution, or its agents from liability for negligence
- Allow subjects adequate opportunity to consider the research
- Ensure that subjects understand the consent form
- Ensure the privacy of subjects during the consent process
- Give subjects a paper or electronic copy of the consent form

B. Best Practices for the Consent Process

The IRB recommends certain methods of consent for different types of research.

- Exempt studies: [Electronic](#) or [Verbal](#) Consent
- Expedited & Full-Board studies: [Written](#) Consent

C. Best Practices for Consent Forms

Below are some best practices for writing the consent form. Please see our [available consent form template and example forms](#) for extra guidance. Tips include:

- Write for a reading level ideally no higher than 8th grade. Reading level can be checked with your word processing tool.
- Please write in second person (“you will complete. . .”) or third person (“participants will complete. . .”). OHRP indicates that use of the first person (“I understand that...”) can be coercive.
- Use words familiar to the average reader. Avoid jargon.
- Define any unfamiliar terms or acronyms when first used.
- Use short, simple, and direct sentences.
- Paragraphs should be short and limited to one idea. Avoid large blocks of text.
- Use at least 11-point font and consider a larger font based on your audience.

- Use formatting such as bold or underlined text or bullet points to make your form easy to read.
- Avoid repetition.
- Use photos, graphics, or tables if they will help clarify procedures.

D. Methods of Consent

1. Written Consent

This is the default method of consent for most research.

Information about the study is written into a document called a consent form. The paper or electronic form is either read by the subject or to the subject. The subject signs the form to indicate their consent. Any legally valid signature is allowable as documentation. This can include an ink signature, depending on your country/state a “digital signature.” Qualtrics and some online survey programs allow for signature blocks, which can be considered a valid electronic signature. [Retention requirements](#) apply to signed consent forms.

a) *When Read By the Subject*

This process includes:

- Writing a consent form that includes all of the elements listed in our standard consent template
- Provide a copy of the consent form, or a similar level of information about the research, to the subject prior to

beginning the study tasks. This allows subjects adequate opportunity to read about and consider the research

- Talk through the consent form with the subject to highlight the main points and ensure understanding
- Take steps to ensure that the subject understands the content of the form, especially if the study is complicated or includes a lot of jargon. This includes looking for cues that the subject is listening and understanding
- Provide an opportunity for questions
- If the subject consents to participate, they sign the consent form
- Provide a copy of the consent form to the subject
- The signed copy of the consent form is retained by the researcher, separate from the subject's data

b) *When Read to the Subject*

This process includes:

- Writing a "short form" written document. This form states that all the elements of informed consent have been presented orally to the subject or their legally authorized representative
- Submit a "written summary" to the IRB of what information will be said to the subject

- A witness is required to be present at the oral presentation of the consent form
- The short form is signed by the subject and the witness
- The summary is signed by both the witness and the person obtaining consent
- A copy of the summary and short form are given to the subject or the representation

2. Waiver of Documentation of Consent: IRB Approval Required

These are alternative methods for consent that can be used in certain circumstances.

Information about the study is written in a consent form. The process of informed consent is completed, but the subject does not need to physically sign the statement to indicate consent. The researcher must document that consent was obtained from the subject, including the date consent is provided.

Researchers on non-exempt applications will need to provide a justification for the use of these alternatives. This request is completed by downloading the Waiver Supplement and attaching it to the application.

a) *Electronic consent*

Electronic consent will include all of the same form elements as written consent, but rather than a legally valid signature, the subject clicks a button and or types their name to consent to participation.

Note that typing your name is not considered a legally valid signature, so this method still involves waiving documentation of consent.

The most common way that electronic consent is used involves using an online survey platform. The consent language is included as the first page of the survey. At the bottom of the consent language is a question that asks participants if they would like to participate. The participant clicks one of two statements "I agree to participate in this survey" or "I do not agree to participate in this survey." The text of these statements is flexible. If the subject clicks I agree, they continue to the survey. Researchers who need to link the data to an identifier will include a text box for the participant's name. If the subject clicks I do not agree, they are taken to the end of the survey.

b) *Verbal consent*

In this method, the participant and researcher go through the consent process, where information about the study is explained. After the consent discussion, the participant is asked whether they are interested in participating. The participant either declines or gives their verbal consent in place of written consent. A copy of the consent form is provided to the participant.

If it is not feasible to provide subjects with a consent form, the IRB will want to review a consent script.

The person obtaining verbal consent will document in the research file when the consent discussion took place.

c) *Implied Consent*

Implied consent is when a subject is given the option to consent by performing a specified task or activity. The consent form must specify the task or activity that if completed would indicate consent.

An example of this type of consent is mailing out a survey with a cover letter requesting your consent to participate by answering the questions and returning the survey. The cover letter would contain information about the study as well as a statement that returning the survey indicates a willingness to participate.

3. *Waiver of Consent: IRB Approval Required*

This option is generally for retrospective research. Consent can be waived for research involving existing medical records, data, or specimens if a study is deemed to be minimal risk and that the research could not practicably be carried out without a waiver.

4. *Broad Consent*

Broad consent is an alternative to written consent, but only with respect to the storage, maintenance, and secondary research uses of identifiable private information and identifiable biospecimens.

Broad consent forms, like informed consent forms, have a list of required elements. Unlike with traditional informed consent,

there are no provisions that allow elements of broad consent to be omitted or altered.

Broad consent is allowable for either a specific type of specified future research or a broader scope of research.

If any individual is asked to provide broad consent, and they refuse, the IRB cannot waive consent. It is unclear whether or not subjects may be approached again if they refused consent at an earlier point.

Please review the [CITI Final Rule Revisions: Understanding Broad Consent](#) document for additional information.

E. Deception & Incomplete Disclosure

There are times where deception or incomplete/delayed disclosure in consent can be valuable research methodologies. For example, it may be necessary to mislead subjects (deception) or initially provide vague information (delayed disclosure) to avoid biasing a subject's responses. These methods do present a challenge, however. Respect for persons and obtaining full informed consent are central ethical standards for humans subjects research. Informed consent is not fully possible under these circumstances. If these methods are used, additional safeguards need to be in place to protect the rights and welfare of participants.

1. What is deception?

Deception is when participants are deliberately given false or misleading information about aspects of the research.

2. What is incomplete disclosure?

Incomplete disclosure is when researchers withhold information about aspects of the research. This can be called delayed disclosure if the subjects are debriefed afterwards with the complete information.

3. When is it possible to use deception or incomplete disclosure?

Deception or incomplete disclosure are permitted when the following criteria are met:

1. The research presents no more than minimal risk to participants.
2. The alteration will not adversely affect the rights and welfare of the participants.
3. The research could not practicably be carried out without the alteration. The researcher must demonstrate that the deception is necessary to conduct the study.
4. Where appropriate, the participants will be provided with additional pertinent information after participation. This is known as debriefing.

The IRB will consider the following points when reviewing applications:

1. The use of deception or incomplete disclosure must be justified in the protocol to show that the research cannot be performed without this methodology. The benefits of the

research should outweigh any risks that deception may create.

2. Research participants cannot be deceived about significant aspects of the research that would affect their willingness to participate or that would cause them physical or emotional harm.
3. The deception or incomplete disclosure must be explained to participants (known as debriefing) as early as possible, preferably at the conclusion of their participation, but no later than at the conclusion of the data collection.
4. Participants should be permitted to withdraw their data, unless it was necessary to collect data without a link to identifiers.

4. What is debriefing and when is it necessary in a study?

A debriefing is when participants are given a full explanation of the study after participation.

When deception or incomplete disclosure are used, the IRB will expect the inclusion of a debriefing unless the researcher can justify why this would not be appropriate. The debriefing should include:

- The aspects of the study that were withheld or the false information provided.
- The reasoning for the deception or incomplete disclosure.
- Any other relevant background information for the study.

- A method for contacting the researchers for questions.
- When possible, the option for participants to withdraw their consent to participate or to withdraw their data from the study.

Researchers may use debriefings even in cases without deception and incomplete disclosure. It can be used as an educational tool to provide additional information to participants.

5. How do you conduct a debriefing?

Debriefings can be completed in-person, over the phone, or online.

- Participants should be given a copy of the debriefing information or allowed the opportunity to print a copy.
- If the process is conducted in person, the researcher giving the debriefing should be knowledgeable about the study.
- Researchers should provide an opportunity for participants to obtain additional information about the study.
- If the researcher becomes aware that the procedures have harmed the participant, they should take reasonable steps to minimize the harm.

For example:

- After an online survey containing incomplete disclosure, the last page of the survey could be a debriefing form.

- Subjects may be sent an email after the conclusion of data collection providing the debriefing information.
- Subjects may be given a URL where they can get debriefing information after a particular date.

[Skip to Next Section](#)

[Go to the Top](#)

11. Research Subject Incentives

Incentives are payments made to individuals to compensate them for participation in research projects.

Incentives include any:

- Cash
- Cash equivalents
 - Checks
 - Stored-value products such as gift certificates and gift cards
- Non-cash equivalents (for example, cookies, a coffee mug, etc)
- Course credit
- Extra credit

Please note the reimbursements for parking or mileage are not considered research incentives. Also, grants may restrict the purchase of food as incentives. Researchers should be sure to check with their sponsor to determine if food purchases are allowable.

A. How much can I give?

The IRB has a responsibility to ensure that incentives are not coercive, but there are no specific regulatory guidelines around how much you can or should provide. You will be asked to provide details for your compensation/incentive mode and amount in your application.

Best practice is to pay subjects even if they withdraw from the study early. Payments can be approved as pro-rated, such that a subject receives a certain incentive for a particular task. These pro-rated payments need to be approved by the IRB and described in the study consent form.

B. Requirements

Requirements for all research regardless of funding:

- Incentive amounts and format must be specifically approved in advance by the WWU IRB.
- Arrangements should be made by the principal investigator to assure proper accounting of payments made to subjects for fiscal accountability and federal tax purposes.
- Principal Investigators should consider the privacy of subjects and the security of their data.

When incentives are purchased by, administered by, or distributed through Western Washington University, these requirements also apply:

- Researchers are expected to use the preferred incentive format described below, unless otherwise approved for an alternative method.
- Documentation of payments is required.
- Unused funds allocated for incentives must be accounted for at regular intervals.
- At the end of every fiscal period, funds should be returned to the funding source.
- Undistributed non-cash equivalents remain the property of WWU and should be returned or disposed of according to the University's Disposing of University Assets procedure, which can be found on the [WWU Policies and Procedures website](#).
- Payments are requested and managed through an approved process.

C. Incentive Methods

The University recognizes the need to compensate research subjects using the method that is appropriate for the research and reduces barriers for subjects to participate. The University balances these considerations with the need to:

- Ensure that funds are spent appropriately,
- Meet federal and state internal control and reporting requirements, and
- Ensure the protection of research subjects' identifying information.

For cash or cash equivalent incentives, the preferred incentive format is:

- Amazon Electronic Gift cards

Other methods are allowable if the researcher can demonstrate that the integrity of the research will be affected in a material, negative way by using the preferred method. These alternative incentive methods include:

- Gift cards
- Cash
- MTurk payments
- Non-cash equivalents

D. Incentive Documentation

When grant or department funds are used, all payments to research subjects must be documented. This can include a signed receipt or acknowledge of payment that involves documenting:

- The fund distribution date
- The amount distributed
- Study location
- Name of Study
- Subject acknowledgement of receipt or distribution
- Full name of subject (not required, but is considered a best practice)

The researcher may determine the best method for recording this information.

There may be cases where elements of documentation are not feasible. For example, online survey tools like MTurk do not require a subject's name. In this case, a report showing the worker ID, date of payment, and payment amount may act as a receipt to show participation in the study. If non-cash equivalents are of nominal value, some elements of documentation may be waived. In these and other scenarios, the researcher will need to demonstrate that the integrity of the research will be affected in a material, negative way by full documentation.

E. Incentive Tax Reporting

Cash and cash equivalent incentives, in some circumstances, may be subject to federal income tax reporting requirements.

The Internal Revenue Service (IRS) treats human subject payments, whether cash, check, gift card, or in-kind items (books, DVDs, etc) as taxable income to the recipient. The recipient is supposed to report the payment when they file a personal tax return. As the payer, Western Washington University must follow IRS regulations.

Nominal value non-cash equivalents, course credit, and extra credit incentives are not taxable. Reimbursements for subject travel/parking/etc. are different from incentives and are not taxable.

1. Payments Requiring Reporting

When **incentives are purchased by, administered by, or distributed through Western Washington University, tax reporting requirements apply** when any of the following are true:

- A research subject is paid a total of \$600 or more in a calendar year
- The research subject is a foreign national (all research payments to foreign nationals are subject to 30% tax withholding)

2. Reporting Process

When a research subject will make over \$600 in a calendar year, the investigator is responsible for ensuring appropriate reporting. Investigators can either:

- Collect contact information and
 - for U.S. Citizens and permanent residents collect social security numbers OR
 - for Western faculty, staff, or students collect Western ID numbers OR
 - for non-residential aliens collect foreign taxpayer identification numbers and date of birth
- Guide subjects through completing the appropriate IRS form (1099-MISC for U.S. Citizens and permanent residents or 1042-S for non-residential aliens)

This information should be sent through a secure method to WWU Accounts Payable. The current contact for tax reporting is:

Donna Foley, (360) 650-6815, Donna.foley@wwu.edu

Please remember that Western email is not secure. Social security numbers are considered highly sensitive data and should never be sent over unsecure email servers without additional encryption in place. Email subject lines should read "1099 Tax Reporting."

Reports for the calendar year (January through December) should be made to Accounts Payable **by January 6th** of the following year.

Western must protect confidential information at all times. Identifying information is required when reporting for tax purposes, but the specific study information (the one in which the person participated to receive the money) is not required.

3. [Payments made in other countries](#)

When making research payments to subjects in another country, it is the researcher's responsibility to be aware of and fulfill any tax reporting obligation of the country in which the study is conducted.

4. [Payments to Foreign Nationals](#)

All research payments made to foreign nationals are subject to 30% tax withholding. This includes Canadian citizens.

A visa does not necessarily include authorization to receive compensation. If a foreign national is not authorized to receive compensation from WWU, they cannot be paid for participating in the study. Foreign nationals can receive reimbursements (mileage, parking, etc.) as these are not considered income.

F. Incentive Requests and Approval

Incentives are first approved through the IRB application process. After the application is approved, the researcher should submit the [e-sign form for requesting the purchase of research subject incentives](#).

G. Payment Process

The method of processing payments will be different based on your department. Please investigate your department procedures prior to receiving approval for an incentive type.

Please note that **reimbursing investigators for spending personal funds on research incentives is not allowable**.

Investigators are responsible for planning for an appropriate method of paying incentives during the IRB application process.

1. Electronic Gift Cards

Amazon gift cards are the preferred type of incentive. Amazon gift cards can be:

- delivered as email gift cards to the subject. This method requires documenting a subject's email address.

- given as a gift code. The subject takes the code and adds it manually to their account. This method does not require a subject's email address.

2. Cash

Cash payments can be made from revolving fund accounts/petty cash accounts. Investigators will need to speak with their departments about this procedure for setting up these accounts.

Investigators are expected to follow university policies and procedures related to account set-up, reconciliation, management, and closeout as outlined on [Western's Policies and Procedures site](#). This includes (but is not limited to) the following procedures/policies:

- Obtaining Petty Cash and Change Funds
- Authorizing and Maintaining Petty Cash and Change Funds
- Reconciling University Financial Accounts Policy

3. Physical Gift Cards

Gift cards can be purchased through appropriate department procedures. Investigators are expected to follow all applicable university procedures and policies related to account set-up, reconciliation, management, and closeout.

12. Data & Security Protections

Researchers have a responsibility to protect the privacy of subjects and their data. The Principal Investigator is responsible for ensuring that research data is secure when collected, stored, transmitted, or shared. The IRB has established a framework around protecting data, so that a baseline of protections can be established. Exempt eligible applications are not required to describe their security procedures (except where “Limited Review” is required for certain Exemption categories), however these protections are still recommended for all research activity.

A. How Does This Work?

For non-exempt applications, or Exempt Limited Review applications the IRB will ask you to confirm your data and security protections in the IRB application. Below are the steps that you’ll need to take to complete this.

1. Identify your data sensitivity.

The IRB categorizes data into 4 sensitivity levels. Read through the sensitivity levels listed and identify where your data falls.

2. Identify the protections required for that data sensitivity level.

After you have determined the data level, go to the data protections section where we have listed methods for protecting data. Next to each method a range of levels will be listed. If your data sensitivity level is included in the parenthesis, then you'll want to read that section and ensure that you have that method of protection in place for your research.

B. Data Sensitivity

The sensitivity of data depends on the risks of harm that would result if disclosed. This is on a spectrum from very low risk of harm to severe harm to individuals if disclosed.

1. Level 1 Data

Information that is considered public or no longer determined to be human subjects research. This can include:

- Data collected with the intention to disseminate directly to the public
- Data sets de-identified according to [standards set by OHRP](#)
- Published research data
- Faculty and staff directory information

- Directory information about students who have not requested a FERPA block

2. Level 2 Data

Disclosure would not cause material harm, however, the researchers have chosen to keep this information private. This can include:

- Research data from minimal risk studies about non-sensitive topics

3. Level 3 Data

Disclosure could possibly cause some material harm or may damage a research subject's reputation, employability, or legal standing. This includes:

- FERPA protected data
- Western ID numbers
- Research data from minimal risk studies on sensitive topics

4. Level 4 Data

Disclosure would likely cause significant harm to subjects if disclosed.

- Research data from greater than minimal risk studies

- Social security numbers / taxpayer identification numbers
- [Protected health information](#)
- Genetic information

C. Data Protections

Management of and protection of data is an essential component of a research project. Research subjects place trust in researchers to protect their information according to the terms laid out in the consent process. Please review the protections below for research data as well as [Western's Security Best Practices and Policies](#). Recipients of NIH funds will also want to review NIH's specific requirements ensuring data security.

The IRB will expect that these practices are followed unless otherwise described to and approved by the IRB.

1. Limit Access (Levels 2 – 4)

A data access plan should be an element of every research project. Limiting data access to only authorized users is a fundamental security practice.

Limiting access can occur through both physical and electronic means. The amount of protections taken will depend on the risk level of your research. Examples of ways to limit access to data include, but are not limited to:

- Level 2 - 4:
 - sealed envelopes for signed consent forms

- password protection
- locked cabinets
- locked offices
- Level 3 - 4:
 - data encryption
 - documentation or logging of data access

2. Passwords (Levels 2 – 4)

Passwords are not inherently secure. Here are the IRB's expectations for password security:

- Level 2 – 4
 - Passwords should be protected

Store your password in a protected location or consider using a password management application such as KeePass that securely stores your passwords.
 - Use strong passwords

Follow the [WWU guidelines for strong passwords](#).
 - Use different passwords between access points, when possible.

Using the same password for everything puts data at risk. For example, if a researcher is password protecting a USB drive for temporary data storage,

they should use a password that is different than their computer password.

- Change passwords periodically
- Change passwords immediately if compromised
- Level 4
 - No shared passwords between users

3. Data in Motion (Level 2 – 4)

Security should be considered when transmitting data, whether it is between a device and a computer, between two computers via email, or any other transfer.

- Level 2 – 4:
 - Data must be password protected while on a portable device. USB/thumb/external drives are not considered secure devices on their own.
 - Data should be password protected when sent via email. Western Washington University email is for university business communication, which is public information. Western emails are not encrypted, so identifying information and identifiable data should not be sent via email without password protection or encryption.
- Level 4:
 - USB drives should be encrypted

- Use cryptographic protocols such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL) for secure electronic transmissions
- Use a Virtual Protocol Network (VPN) when working with data off Western's campus

4. Data at Rest (Level 2 – 4)

Your data storage will depend on how the data was collected and the risk level of the data itself. Data storage requirements include:

- Level 2 – 4
 - Data should not be permanently stored directly on portable devices (locally on computer desktops, USB drives, etc), unless otherwise approved by the IRB. Data should be uploaded from local and/or portable systems onto secure WWU network servers or secure cloud services (described at the end of this section). This is to protect data in the event that a device fails.

For example, a researcher has collected data stored on their computer's desktop. If that computer is damaged or lost, the data will be lost as well because it was stored locally on a desktop. If the data is stored in a location such as a secure server, even if a physical computer is damaged or lost the data is still accessible through the server. This logic applies to storing data in any "local" location. Non-

local systems include servers and cloud storage like OneDrive.

- When data is linkable to identifying information, data should be stored separately from the identifiers. For example, signed consent forms should be stored separately from the data.
- Electronic data should be backed up. WWU network servers are backed up automatically.
- Level 3 – 4
 - Data must be encrypted in storage.
 - Storage on secure WWU network servers is recommended, rather than cloud storage (OneDrive, etc). Please see [Academic Technology and User Services' \(ATUS\) Guidelines on Cloud Storage of Educational and Sensitive Data.](#)

5. Data Storage Options

Based on the data sensitivity level and the recommended data protections, choose the most appropriate data storage option.

a) [Network Storage](#)

Western provides storage on WWU network file space. These networks can be restricted for access, so that only authorized users can see and work with the data. Please contact [Academic Technology and User Services \(ATUS\)](#) for help with setting up network file space.

b) *Cloud Storage*

Investigators are responsible for ensuring that cloud storage is secure. OneDrive is the preferred platform for cloud storage. Please see [ATUS's Guidelines on Cloud Storage of Educational and Sensitive Data](#).

Important: OneDrive is specifically linked to each employee. Please take care to ensure that data is not deleted if the employee leaves WWU.

Other cloud services, such as Google Drive, are available, though they cannot inherently provide the same security and require additional steps to ensure protections are in place. Please see the [Appendix below about OneDrive vs. Google Drive](#) to review security needs for Google Drive.

c) *Commercial Services (MTurk, SurveyMonkey, etc.)*

Investigators are responsible for learning about the security protections for any commercial service they use, such as Amazon Mechanical Turk. The security of Qualtrics is well-known, as it is the preferred survey administration software for Western Washington University. All other services should be investigated for the protections in place and select any appropriate configurations that will enhance protection.

SurveyMonkey, as an example, is not inherently HIPAA compliant, though this is offered as a service with a HIPAA-enabled account and a business associate's agreement.

D. Certificate of Confidentiality

A certificate of confidentiality protects identifiable information from forced or compelled disclosure. These are issued by the National Institutes of Health and other Health and Human Services agencies. If you work with sensitive data that may cause substantial harm to research subjects if disclosed, it would be recommended to apply for a certificate of confidentiality.

E. Identifiable Information

Identifying information is any piece of information that can either individually, or in combination with other data, lead to the identification of a human subject. Identifiers include:

- Name
- Address (including geographic subdivisions smaller than state – for example, zip code is an identifier in most circumstances)
- Telephone or fax numbers
- Email addresses
- date of birth (with the exception of just the year or someone's exact age, unless the subject is over 89 years old)
- university ID or student number
- social security number
- medical record number
- Internet Protocol (IP) addresses

- Full-face photographs and any comparable images
- Biometric identifiers, including finger and voice prints (audio recordings)
- Account numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Any other characteristic, unique number, or code that could uniquely identify the individual with the exception of:
 - A code assigned by the researcher that is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual.

Collection of identifiers can often be integral to the research process. The researcher should be mindful however that when identifiers are collected, a certain level of data security protections must be in place. It is a good practice therefore to use the fewest identifiers necessary for your research.

F. De-identification

De-identification is the process of removing identifying information from a dataset.

Western uses the [standards set by OHRP to define de-identification.](#)

G. Protected Health Information

Protected health information (PHI) is individually identifiable health care information or clinical specimens from an organization considered a “covered entity” by federal Health Insurance Portability and Accountability Act (HIPAA) regulations.

PHI includes:

- Common identifiers
- Demographics
- Data that relates to the individual’s past, present, or future physical or mental health or condition
- Data that relates to the provision of health care to an individual
- Data that relates to the past, present, or future payment for the provision of health care to the individual

Please read more about HIPAA requirements below.

H. Health Insurance Portability and Accountability Act (HIPAA)

HIPAA protects the security and privacy of protecting health information created, received, maintained, or transmitted from a “covered entity.” Covered entities include health plans, clearinghouses, and certain health care providers. Clinics at Western Washington University are covered entities. [Read more about HIPAA on HHS.gov.](#)

Under HIPAA, PHI may only be used or disclosed to others in certain circumstances or under certain conditions. For example, PHI may be disclosed to facilitate treatment or health care. Specific HIPAA authorization from the individual is required for additional use or disclosure beyond this, including research use.

It is the researcher's responsibility to receive HIPAA authorization from the subject for PHI used in research, not the covered entity. This includes use of PHI for both recruitment and study procedures.

HIPAA authorization forms must include:

- A specific description of the protected health information being disclosed
- The individuals who will be authorized to access the records
- The place(s) where the information will be requested
- The purpose of the disclosure for this research
- An expected expiration of the disclosure permissions (the terms "end of the research study" or "no expiration" may be used)
- A statement that they have a right to revoke this authorization in writing and either (1) the exceptions to the right to revoke and a description of how the individual may revoke Authorization or (2) reference to the corresponding sections of the covered entity's Notice of Privacy Practices
- Notice of the covered entity's ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the Authorization, including research-related treatment, and, if applicable, consequences of refusing to sign the Authorization

- The potential for the PHI to be re-disclosed by the recipient and no longer protected by the Privacy Rule. This statement does not require an analysis of risk for re-disclosure but may be a general statement that the Privacy Rule may no longer protect health information

Researchers should create a HIPAA authorization form that includes these elements. It is recommended that the HIPAA authorization form and informed consent form be kept separate, because the forms have different regulatory requirements.

Unlike informed consent, which focuses on the process of consent rather than the form itself, HIPAA only requires that the form be read and signed.

HIPAA has stringent requirements around de-identification of protected health information. Please read the [guidelines for the methods of de-identification of this data](#).

I. Anonymous vs Confidential: Describing Data Protections

In research there is no consistent usage of “anonymous” and “confidential.” Sources disagree on the definitions of these terms. Anonymous in some contexts can mean no face-to-face interaction has ever occurred. In others anonymous is only referring to the lack of a link between data and identifiers. Confidential in some contexts can mean that the information is kept private, which would mean that anonymous data can also be confidential. In other contexts, confidential refers to the link between data and identifiers and therefore making “anonymous” and “confidential” mutually exclusive. For subjects and researchers alike, this a problem for comprehension.

Western's IRB is asking that instead of (or in addition to) using these terms, researchers describe specifically how the data is collected, whether it will ever be linked to their identifying information, and how the data is maintained securely.

[Skip to Next Section](#)

[Go to the Top](#)

13. Protocol Submission Process

A. Ethics Training

Ethics training is required for the Principal Investigator and all members of the research team who will interact or intervene with research subjects or subject identifiable data.

This online training is provided through The Collaborative Institutional Training Initiative (CITI). The training is free for WWU affiliated researchers.

Researchers funded on NIH grants are required to complete 8 hours of in-person training in addition to the online course.

Other training may be allowable as a substitute if described to the IRB and the IRB determines that the information is sufficient.

Trainings need to be renewed every 5 years.

For more information on training requirements for specific grants, please see the [Training](#) section of our website.

B. Complete an Application

There is one [application form](#) to complete for all research studies. For some research, you may be directed to download and complete additional supplements. Directions and guidance on how to complete your application can be found throughout the application form.

Incomplete applications may be returned to the researcher for completion.

A complete application will include:

- The full, correct contact information for the Principal Investigator and Faculty Advisor (if applicable)
- Signatures for the Principal Investigator, Faculty advisor (if applicable), and the Department Chair
- All questions answered or, if not applicable, marked with "NA"
- All applicable supplement forms attached
- All recruitment materials attached. Please title all of your attachments so that we can easily identify them.
- All study materials and instruments (surveys, interview questions, etc.) attached. Please title all of your attachments so that we can easily identify them.
- A consent form, information statement, or parental permission & minor assent form

Email submissions of applications are preferred. The email account for all human subjects' correspondence is compliance@wwu.edu.

If you need to submit your protocol as a paper application for a particular reason, please follow these guidelines:

- Applications should be typed, not handwritten.
- Please do not use staples anywhere in your application - they get caught in our scanners. Paper and binder clips are okay.
- We encourage documents to be printed double-sided, with each new document starting on its own page.

C. Preliminary Review & Screening

After submission, a Research Compliance Officer (RCO) conducts a preliminary review of the protocol. This involves:

- Confirming that the application is complete
- Determining the appropriate review category (exempt, expedited, or full board)
- Clarifying ambiguous answers
- Requesting revisions

A majority of applications require some minor clarification or revision. Incomplete or significantly flawed applications may be returned to the researcher to complete or rewrite.

After a preliminary review, the RCO will email the Principal Investigator or PI Proxy with screening questions and/or modifications. This email will contain instructions on how to respond. The researcher should respond as promptly as possible. **If no response is received, applications will be closed after 60 days**

and a resubmission will be required. Researchers can request longer than 60 days by replying to the RCO with an expected timeline for response.

There may be some additional screening back and forth as needed. After this preliminary review, the next steps depend on your research category assigned.

D. Review & Determination

Once an application is ready for final review, the next steps depend on the category of research.

1. Exempt Review

The RCO who screened your application will make a final determination. You will receive an email confirming the determination with your application packet attached to the email.

Exempt determined research is valid indefinitely. The ability to make modifications to the research expires after the retention requirement has been met for the paperwork – 6 years after the determination. At that point, our office will no longer have a copy of the determination paperwork on file, and the researcher will need to submit a new application. Please see below for information on modifications and problem reporting for exempt research.

2. Exempt Limited Review

The RCO will review the study's data and security protections (Human Subjects Application Form Question 8.3).

Limited review is required for:

- Exempt Category 2 and 3 determinations when subjects are identifiable and sensitive information is involved
- All exempt Category 7 and 8 determinations

After approval, there are no differences between Exempt and Exempt Limited Review studies, except researchers need to ensure that a modification form is submitted for any change that might affect data and security protections.

3. Expedited Review

The RCO will distribute your application to a second reviewer. The process of screening repeats with the second reviewer. Once the second reviewer is satisfied with the application, the first RCO will make a final determination. As the RCOs have worked with the researcher on revisions and clarifications, typically all applications receive approval at this stage. You will receive a formal determination email with a determination packet attached to the email. If your application is approved, it will be your approval packet.

Expedited research requires regular status reports, review of all modifications and problem reports, and closure upon completion. See more information on [Open Applications](#).

4. Full Board Review

The RCO will distribute your application to the full IRB committee. All comments, clarification questions, and revisions of the committee members will be compiled by the RCO and emailed to the Principal Investigator or IRB contact – repeating the screening process.

When the application is ready, the RCO will schedule a full convened IRB meeting. During the convened meeting, the committee will review the application again, including any revisions, and will hold a vote.

The Principal Investigator (PI) may be invited to attend the convened meeting in order to answer questions directly. If a student PI is invited and would like to attend a full board meeting the Faculty Advisor must attend as well.

The outcome of the vote can include:

- Approval;
- Approval dependent on revisions (“Conditional Approval”);
- Deferral on vote until revisions are complete;
- Fail to approve.

You will receive a formal determination email with a determination packet attached to the email. If your application is approved, it will be your approval packet.

Expedited research requires regular status reports, review of all revisions and problem reports, and closure upon completion. See more information on [Open Applications](#).

E. [Appeal of IRB Determination](#)

If a researcher is not satisfied with an IRB determination, they can submit an appeal to the Vice Provost for Research within 30 days of the determination. The appeal document must provide a regulatory basis for reversing the IRB's determination. The Vice Provost for Research will review the protocol file, meeting minutes, and appeal documents, and determine whether the decision is upheld or overturned.

[Skip to Next Section](#)

[Go to the Top](#)

14. [Open Research Applications](#)

A. [Extending Your Research](#)

After approval, full board applications require regular status reports. When an application is approved, the IRB will assign an approval period. The standard approval period is one year, unless otherwise specified.

If the Principal Investigator would like to continue the research beyond the expiration date set by the IRB, they must submit an

application to extend the project. It is considered non-compliance to continue any work on your research if your project has expired.

Status reports should be submitted 4 weeks in advance of the expiration to allow enough time for review.

B. Requesting Changes

Researchers may want to make changes or modifications to an approved protocol.

1. Changes Requiring Approval

All changes for full board and expedited studies require IRB approval. This includes changes to any of the following:

- The subject population
- The maximum number of approved subjects
- The recruitment plan or materials
- Consent forms
- Study instruments
- The Lead Investigator
- Any investigator working with human subjects or their identifiable data

Some changes on Exempt applications do not require IRB approval as long as they do not change the risk level to the

subjects or fundamentally change your research design.
Changes that do not require IRB review include:

- Edits in spelling, punctuation, and grammar on your recruitment or study materials (not including your consent forms)
- Minor wording changes to your recruitment materials that do not change the overall content and resulting comprehension

2. How to request a modification

To request a change, please submit a [Modification form](#).

Modification requests for exempt and expedited applications can be reviewed by a single Research Compliance Officer (RCO). Requests to modify full board studies will require review of the full IRB Committee.

C. Unanticipated Problems

During the course of a study, it is possible that an unanticipated problem or adverse event occurs. Any incident that meets the following criteria will need to be reported **within 72 hours** to the IRB:

- The event is unexpected in terms of the nature, severity, or frequency given the IRB approved protocol and the characteristics of the population being studied; **and**

- Is related or possibly related to participation in the research;
and
- Suggests that the research places human subjects or others at a greater risk of harm than was previously known or recognized, even if no harm has actually occurred.

If you have described your risks carefully in your consent form and application, this helps to mitigate unexpected events. For example, if your consent form states a risk of dizziness while conducting a task, a subject experiencing dizziness would not be considered an unanticipated problem.

D. Non-Compliance

Non-compliance refers to any behavior, action, or omission in the conduct or oversight of research involving human subjects that deviates from the approved research plan, federal regulations, or institutional policies. It may be unintentional or willful and can be conducted by any research personnel.

Examples of non-compliance include:

- Initiating research procedures, such as recruiting or enrolling subjects, before IRB approval
- Continuing research activities after your IRB approval has lapsed/expired
- Enrolling subjects that do not meet the protocol's approved inclusion/exclusion criteria
- A breach in subject privacy or data security

- For expedited and full board studies, over-enrolling subjects over the approved number
- Enrollment of vulnerable populations (children, prisoners, people with diminished capacity to consent) without prior IRB approval
- Not obtaining consent (unless the IRB waived consent)
- Use of an unapproved consent form
- Failure to report adverse events
- Conducting a procedure in a different manner than approved by the IRB

1. Levels of Non-Compliance

There are three levels of non-compliance: minor non-compliance, serious non-compliance, and continuing non-compliance.

a) *Minor Non-Compliance*

The non-compliance is considered minor when the action does or did not:

- Harm or pose an increased risk of harm to a research subject
- Have a substantive effect on the value of the data collected
- Result from willful or knowing misconduct on the part of the investigator(s) or study staff

b) *Serious Non-Compliance*

Serious non-compliance is action that:

- Adversely affects the rights or welfare of research subjects
- Harms or poses an increased risk of harm to a research subject
- Compromises the integrity or validity of the research
- Results from willful or knowing misconduct on the part of the investigator(s) or study staff.

c) *Continuing Non-Compliance*

When a pattern of minor or serious non-compliance occurs, this may constitute continuing non-compliance.

2. Reporting Non-Compliance

The IRB should be notified promptly of non-compliance. The Principal Investigator (PI) or PI Proxy should submit a Problem Report to the IRB within 7 days of the discovery of non-compliance.

A Research Compliance Officer (RCO) will review the problem report and make a determination of whether it constitutes minor, serious, or continuing non-compliance. The IRB contact will be notified about the determination and the next steps involved.

Actions that may be taken include:

- No action
- Modification of the research protocol
- Notification to the research subjects about the non-compliance
- Required re-consenting of subjects
- Suspension of enrollment into the study
- Notifying the funding agency
- Terminating the research

3. Investigations of Non-Compliance

When non-compliance is reported, a RCO reviews the problem report. Clarifying questions may be asked during the review of the problem report. The RCO will make a determination about the level of non-compliance and the corrective actions that should be taken. The investigator will be notified of the final result.

Non-compliance may or may not constitute [research misconduct](#).

E. Data and Records Retention

In addition to research data storage, researchers must maintain records of the following documents:

- The IRB application approval packet sent with the approval notice

- Copies of all other correspondence with the IRB
- Modification and status report approval packets
- Copies of any inspection or audit reports
- Copies of all signed informed consents

These records may be maintained electronically or in print, according to how the record was originally produced. [Contact University Archives and Records Management](#) for requirements related to replacing hard-copy records with digital copies. For example, when a researcher wants to scan signed informed consents and store them electronically.

There are specific retention requirements for these research records that are set by University policy. Principal Investigators must retain research data for the longest of any applicable retention periods set by university policy, sponsorship agreements, or other agreements. Please see WWU's [Data Retention Policy](#).

WWU policy requires that research records are maintained for **six years** following completion of the research. For example, signed consent forms must be retained for 6 years after the completion of research.

IRB records are subject to inspection by federal authorities as well as the WWU IRB. Sanctions for incomplete or nonexistent records include suspension of funding, fines, exclusion from future funding, and suspension of laboratory access and investigation for non-compliance and research misconduct.

F. Study Closure

Full-board protocols should be closed if either:

- All recruitment and interaction with human subjects or identifiable data is complete
- The Principal Investigator is leaving Western and is requesting a transfer of the research protocol.

To close an application, complete a status report form and select the option to close the study.

G. Data Destruction

Principle Investigators must destroy research data when required by laws, regulations, or other agreements. Please see the [Records Destruction Guidance](#).

[Skip to Next Section](#)

[Go to the Top](#)

15. Research Misconduct

Research misconduct can occur at any point during the research process.

Research misconduct is any of the following:

- Fabrication, falsification, or plagiarism is used in proposing, performing, or reviewing research, or in reporting research results.

Research misconduct does not include honest error or differences of opinion.

- Willful failure to comply with federal, state, or university requirements i) for protecting researchers, involved research employees, and/or engaged students and ii) for human subjects and the public during research.
- Use of university resources such as research funds, facilities, faculty, staff, or students for unauthorized and/or illegal activities.

Investigations of research misconduct will be conducted by a sub-committee of the IRB as appointed by the Research Integrity Officer.

The subcommittee will:

- Contact the researcher with the allegations
- The researcher has 14 days to respond in writing
- The committee will review the protocol, the researcher's response, and any other documents related to the non-compliance allegation. The committee may also interview people with knowledge about the allegation.
- The investigation committee will write a report with their findings and present it to the institutional official.
- The committee will give the report to the researcher who will have 14 days to respond in writing.
- The institutional official will review all relevant documents and determine the actions to be taken as a result of the finding.

Actions that may be taken during or after the investigation of research misconduct include:

- No action
- Modification of the research protocol
- Notification to the research subjects about the misconduct
- Suspension of enrollment into the study
- Notifying the funding agency
- Referral to other organizational entities including a research misconduct committee
- Terminating the research

Please read Western's [Addressing Responsible Conduct of Research policy](#) for more information.

[Skip to Next Section](#)

[Go to the Top](#)

16. Appendix A: How to Conduct Internet-Based Research

First, please read about the definition of [Internet Research](#) above.

A. Internet Privacy

IP addresses are considered private identifiable information and should be treated with appropriate security measures. IP addresses should not be collected, unless the researcher has a compelling reason. Some online survey programs have the capability to turn off the IP address collection function.

Investigators are responsible for ensuring that data stored online is secure. Please see our [guidance on data storage and security](#).

B. Online Survey Considerations

Online surveys are a convenient way to gather data at a minimal cost, but they do present some challenges.

1. Consent

Researchers should consider methods to ensure that informed consent is occurring online. In person methods allow a researcher to be more easily present for questions and ensure understanding. Online survey consents must include easy ways for subjects to ask questions and a reminder to print the consent information for their records.

Technology has come a long way for allowing different methods of consent online. Through Qualtrics, it is now possible to include a signature block, which allows for a valid electronic signature.

Please see the [Informed Consent](#) section for information on different methods of consent, including electronic options. Typical methods for consent online include written consent or a waiver of documentation of consent to allow electronic or implied consent. Waivers are not guaranteed and must be approved by the IRB.

2. Eligibility requirements

The IRB will require some method of screening out subjects who do not fit the criteria for the study – including any individual under the age of 18 years old, if the study is not approved for minors as subjects. This screening can be incorporated into the online survey or may be covered in other ways that should be explained in your research application.

3. Optional Questions

The IRB recommends that all online survey questions be optional, unless the question is necessary for screening purposes or integral to the purpose of the study.

C. Recommendations for Platforms

1. Qualtrics

Qualtrics is WWU's preferred method of online survey data collection. Every Western faculty, staff, and student has access to create a Qualtrics survey.

If you are using Qualtrics, you do not need to describe the security protections of the platform, as these are known by the IRB.

Tip: If you intend to collect data that is not linked to identifiers, please enable the "Anonymize Responses" setting in Qualtrics so that IP addresses are not reported in survey results.

2. Sona

Sona is the WWU Psychology Department's research participation database.

a) *Recruitment*

The study information settings in Sona are considered research materials. For expedited and full board studies, the IRB will want to know the information you will include in these fields: study name, study type, duration, credits, abstract, and description. The information here can be brief, but should sufficiently describe the study.

b) *Consent*

Please see our [options for consent procedures](#).

c) *Data Security*

If your study involves the subject signing up and going to a specified location, the researcher has access to the names of their prospective research subjects. This is considered having access to personally identifiable information and should be discussed accordingly in the IRB application. You can let the IRB know who will have access to these names, how they will be stored for security, whether they will be retained, and whether names will be linked to subject data.

3. Amazon Mechanical Turk Guidance

Amazon Mechanical Turk (MTurk) is described by Amazon as "a marketplace for work that requires human intelligence." It's a

platform where tasks can be posted to a wide pool of workers for completion for a specified amount of money. Researchers can use MTurk to post surveys and provide a small monetary incentive.

MTurk is not designed for human subjects research, therefore certain precautions need to be put in place.

a) *Recruitment*

The title and description of the task are considered recruitment materials. The description posted on MTurk should include:

- A description of the task
- The time required to complete the task
- The compensation
- The researcher's name and/or that the research is affiliated with WWU
- A link to the survey

b) *Consent*

The first page of the online survey should be the consent document. Please see our [options for consent procedures](#).

c) *Data Security*

Anonymity of MTurk cannot be guaranteed. MTurk worker IDs can easily be linked to individuals' Amazon profiles including individuals' wish lists and previous product

interviews. This can include identifying information that the MTurk worker has posted on their profile.

If MTurk worker IDs are collected, the IRB will consider the data link to identifiers. Subjects should be notified in the consent form that their ID may be linked to identifying information on their public profile. The IDs should be kept securely, not linked back to survey data, and deleted after use.

D. Chat Rooms & Support Groups

Please see the [Internet Research considerations](#) discussed at the beginning of this document.

If the chat room is a moderated room and requires a login, then the researcher must obtain permission from the gatekeeper/ site administrator in addition to the individual subjects.

Researchers should announce/introduce themselves and their research when entering a chat room. Consider how you will manage individuals entering and leaving the chatroom at random intervals and how these individuals might not have been present for your introduction.

E. Social Media Research (Twitter, Facebook, Etc.)

If a Facebook group is private, the researcher must obtain permission from a group administrator and submit that documentation to the IRB.

Researchers need to consider that even if the researcher may have obtained consent from a subject, the researcher doesn't have consent from the people who comment on the subject's posts. It is an ethical dilemma as to whether a researcher can use not only the data of a consenting subject but also the "friends" of that subject who unknowingly volunteer information that could be used for research. The IRB will expect an explanation of how the rights of third parties to consent to research participation will be respected.

F. Skype Research

If the researcher is recording the interview, they must obtain permission to record in addition to consent to participate in research. This can be included as part of the consent process or separately.

[Skip to Next Section](#)

[Go to the Top](#)

17. Appendix B: Security: OneDrive vs. Google Drive

OneDrive for Business and Google Drive have similar security protections, but OneDrive is the preferred platform. It is possible to be HIPAA and FERPA compliant on both platforms, however, Google Drive requires many added steps to achieve this level of security. While WWU has formal HIPAA agreement with OneDrive, the same steps have not been taken for Google. This means that that investigators are responsible for attaining the same level of security. In summary, if you have access to OneDrive for Business, that is the superior platform. Researchers may justify their use of Google

Drive, but they must be sure to configure their account for security of any sensitive data.

Breakdown of Security between OneDrive for Business and Google Drive.

(As of August 2017)

	OneDrive for Business	Google Drive
HIPAA compliant	Yes	No formal agreement between WWU and Google; Yes, if using a paid account AND a Business Associates Agreement has been signed AND the service has been configured with additional security measures by the account admin HIPAA Compliance Implementation Guide
FERPA compliant	Yes	Yes
Data encryption in transit	SSL/TLS; 2,084 encryption keys; Perfect Forward Secrecy	256-bit SSL/TLS, 2,048 RSA encryption keys; Perfect Forward Secrecy; additional transport encryption options available via Google Cloud VPN for IPsec virtual private network

	OneDrive for Business	Google Drive
Data encryption at rest	Yes, for Business users only; AES with 256-bit Keys; Encrypted at disk and file level	<p>Yes, most data; AES with 128-bit keys</p> <p>Data not encrypted at rest:</p> <ul style="list-style-type: none"> ▪ Serial console logs from virtual machines in Google Compute Engine; this is currently being remediated ▪ Core dumps written to local drives, when a process fails unexpectedly; this is currently being remediated ▪ Debugging logs written to local disk; this is currently being remediated ▪ Temporary files used by storage systems; this is currently being remediated ▪ Some logs that may include customer content as well as customer metadata; this is planned for remediation

	OneDrive for Business	Google Drive
		<ul style="list-style-type: none"> ▪ **data still encrypted at storage level and protected by infrastructure
Federal Information Processing Standard 140-2 Compliant (Security standards for cryptography modules)	Yes	No
ISO 27001 certification for system security	Yes	Yes
ISO 27017 certification for cloud security	Yes	Yes
ISO 27018 certification for cloud privacy	Yes	Yes
Cloud Security Alliance STAR Self-Assessment	Completed	No information
Security Concern(s) Addressed		Open source version of Google's cryptographic library has known security issues, but this is not the version used internally at Google

	OneDrive for Business	Google Drive
Security Concern(s)	User mistakes such as password insecurity, sharing confidential files with unauthorized team members, wrong email attachments, leaving devices with synced materials in public places.	User mistakes such as password insecurity, sharing confidential files with unauthorized team members, wrong email attachments, leaving devices with synced materials in public places.
Access	<p>Promises that it will not search or access your drives without notification of suspicion or a court order.</p> <p>Does take the metadata you provide (device information, login information, location information) to serve up ads and analyze usage</p>	<p>Promises that it will not search or access your drives without notification of suspicion or a court order.</p> <p>Does take the metadata you provide (device information, login information, location information) to serve up ads and analyze usage</p>
Recommendations	<p>General Guidelines:</p> <ul style="list-style-type: none"> • Limit access • No shared passwords • Protect passwords • Strong passwords • Change passwords periodically 	<p>General Guidelines:</p> <ul style="list-style-type: none"> • Limit access • No shared passwords • Protect passwords • Strong passwords • Change passwords periodically

	OneDrive for Business	Google Drive
	<ul style="list-style-type: none"> • Change password immediately if compromised • Report suspected loss, theft, or improper use of data • Separate subject identifiers from data (coded), with the link in a separate password protected file in a different location than the data <p>OneDrive Specific:</p> <ul style="list-style-type: none"> • Do not use your personal OneDrive consumer version – this is not the same as OneDrive for Business • Do not sync files onto a non-University owned device 	<ul style="list-style-type: none"> • Change password immediately if compromised • Report suspected loss, theft, or improper use of data • Separate subject identifiers from data (coded), with the link in a separate password protected file in a different location than the data <p>Follow Google’s guidelines for increasing security including:</p> <ul style="list-style-type: none"> • Turn file syncing off • Set link sharing to off • Restrict share of files outside of domain • Set visibility of documents to private • Disable third party apps and add-ons • Disable offline storage for Google Drive • Disable access to apps and add-ons

	OneDrive for Business	Google Drive
		<ul style="list-style-type: none"> • Configure access controls carefully • Enable auditing • Audit access and account logs and shared file reports regularly • Configure 'manage alerts' to ensure the admin is notified of changes to settings • Back up all data uploaded • Never put PHI in titles of folders or Team Drives • Set up 2-step verification • Configure enterprise sender identity technologies <ul style="list-style-type: none"> ○ Authenticate email with DomainKeys Identified Mail standard ○ Authorize senders with a sender policy framework ○ Prevent outgoing spam with DMARC

	OneDrive for Business	Google Drive
		<ul style="list-style-type: none"> ○ Prevent phishing attacks on users with Password Alert extension

[Skip to Next Section](#)

[Go to the Top](#)

18. Appendix C: Survey Monkey Security

SurveyMonkey is not the preferred survey administrator software. Qualtrics is Western Washington University’s first choice for software and provides licenses for all Western faculty, staff, and students.

If you are dead set on using SurveyMonkey, you need to:

- Justify this to the IRB
- Purchase an account that provides SSL level encryption
- If working with Protected Health Information, a HIPAA-compliance service must be purchase along with signing a business associate’s agreement.

19. Appendix D: Use of Secondary Data

Data Type	Examples	Identifiable	IRB Review Required?
Data that are not about living individuals	Records of deceased individuals; death records	Can contain identifiers	No
Publically available data	Public records; data from unrestricted websites	Can contain identifiers	No *If you merge public data sets with other data sets containing private information this may require review if it enables identification
Non-public, de-identified data where the investigator has no access to identifiable information	De-identified data given by a colleague or provided by a data provider where no collaboration is expected	No access to identifiers	No
Non-public, identifiable data, but where the researcher does not record, retain, or use identifiers	Accessing medical records, but recording information in a manner where the data is devoid of identifiers	The original dataset can contain identifiers, but no identifiable information is recorded, retained, or	Yes, likely Exempt Category 4

Data Type	Examples	Identifiable	IRB Review Required?
		used by any member of the research team	
Non-public, identifiable data where the researcher has access to and records private identifiable information			Yes, likely Expedited Category 5