Researcher Guidance for the Use of Qualtrics in Data Collection

**This guidance may be updated with additional information as it becomes available.*

Introduction

Qualtrics is the primary survey platform supported at Pepperdine University for collecting research data. While it offers a secure environment, researchers must configure settings correctly to protect participant privacy and ensure compliance with federal regulations and IRB standards.

This document provides guidance on:
- How to enable anonymization in Qualtrics
- The distinction between anonymous and confidential data collection
- Best practices for data deletion and security.

General Considerations in Study Design

1. Understanding Anonymous vs. Confidential Data Collection

- Anonymous: No identifiers are collected, and responses cannot be linked back to individuals. If you turn on the 'Anonymize Responses' setting in Qualtrics, the system will not store IP addresses, geolocation, or contact information.
- Confidential: Identifiers are collected, but researchers take measures to protect them (e.g., removing names before analysis, storing master lists separately). Confidentiality means the researcher knows participant identities but agrees to protect them from disclosure.

Many researchers confuse these terms. If Qualtrics default settings are left unchanged, the survey is confidential, not anonymous.

2. Enable Anonymization Settings

Qualtrics can collect IP addresses, geolocation (latitude/longitude), and device meta info (for example, browser, browser version, operating system, screen resolution, and java support) if the meta info question is selected for a survey. To prevent this, researchers must turn on 'Anonymize Responses' **before** distributing a survey.

Step-by-step instructions: https://www.qualtrics.com/support/survey-platform/survey-module/survey-options/survey-protection/

3. Data Security and Storage

Store research data in Pepperdine's Google Drive or other Pepperdine-approved secure storage solutions. Do not use personal Dropbox, Box, or consumer cloud accounts. If identifiers must be collected, keep them in a separate, password-protected master list and limit access to essential research personnel disclosed in the IRB protocol.

4. Data Deletion in Qualtrics
When you delete data in Qualtrics, it is deleted permanently and cannot be recovered. All disaster recovery backups are purged within 90 days. Researchers should download necessary de-identified data files prior to deletion if ongoing analysis is required. Only keep identifiable data for as long as necessary to complete the study.

5. Working with Vulnerable Populations
If you are collecting data from minors or vulnerable adults, anonymization is strongly encouraged unless identifiers are essential to the study design. Clearly communicate in consent forms whether the study is confidential or anonymous, and what protections are in place/

Privacy and Security Best Practices for Using Qualtrics

1. Turn on Anonymize Responses (required for anonymous surveys).
2. Avoid collecting unnecessary identifiers (e.g., names, birthdates, contact info).
3. Disable geolocation tracking by ensuring the anonymization setting is active (enable "Anonymize responses" under Survey Options > Security).
4. Clarify confidentiality vs. anonymity in consent forms so participants understand how their data will be handled.
5. Restrict access to Qualtrics accounts and stored data to only approved research team members.
6. Use Pepperdine-approved storage for backups and data exports, and consult with Pepperdine IT if needed.
7. Delete data responsibly once no longer needed; remember that deletion in Qualtrics is permanent within 90 days.

IRB Protocol Requirements

When submitting an IRB protocol that involves Qualtrics:

1. In Study Procedures, describe whether your survey will be anonymous or confidential and justify your choice.

2. In Data Protection/Confidentiality, explain whether 'Anonymize Responses' will be enabled and how identifiers (if collected) will be managed.

3. In Consent Forms, state explicitly:
   - If responses are anonymous, that no identifying information will be collected.
   - If responses are confidential, how participant identities will be protected