NWU Institutional Review Board
Best Practices for Data Security and Privacy

NWU-IRB policies and procedures stipulate that:

- When appropriate, the research plan makes adequate provision for monitoring the data collected to ensure the safety of subjects.
- When appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.

NWU policy also requires that all research data be kept in a secure location for a minimum of three years after study completion. The level of security required is relative to the risk posed to research participants should the data be accessed by an unauthorized person.

NWU-IRB is responsible for determining if the proposed data storage plan is sufficient to protect research subjects and minimize risk. Principal investigators are responsible for ascertaining and describing how their data collection and storage methods meet data protection requirements. Investigators should address this in question 4, *Risks and Benefits for Research Participants*, on their IRB application form. Data management plans need to be consistent with any applicable institutional or other privacy policies (for example, HIPAA in healthcare settings and FERPA in college/university settings). If your project involves multiple sites, address how you will securely share the data between investigators at the different sites.

The following recommendations and best practices can help investigators create a sound plan for managing research data.

Data storage guidelines

To maintain data privacy and confidentiality:

- When creating surveys, don't ask for more identifying information than is necessary for the study. Identifying information includes a person's name, social security number, date of birth, etc.
- If it is necessary to collect identifying information, separate identifying elements from the dataset immediately after collection and store them separately.
- Since IP addresses have some potential to identify a person, if a survey platform you are using has the option to collect the IP addresses of respondents, turn that off.

To prevent unauthorized access to data:

- Use a unique, strong password to log into the device or account where the data is stored.
- Don't share your password with others or save it on your device.
- Log out at the end of your work session.
- If a device is lost or stolen, immediately change passwords for any cloud accounts where data is stored.

To ensure data is preserved for the three-year period:

- Store digital data on OneDrive or Sharepoint (in Office 365), not on a flash drive or computer hard drive. (**NOTE**: Office 365 accounts are purged when a student or faculty member leaves NWU. If you are leaving and have data stored in Office 365, download it before leaving and give it to the faculty sponsor for safekeeping.)
- Store paper files in a locked cabinet or locked room that only researchers can access.

To securely destroy data when no longer needed:

- Destroy paper records/files by shredding.
- To permanently delete Sharepoint/OneDrive data, contact NWU's Office 365 administrators for assistance.
- For files on a hard drive, use data-wiping software to ensure information is permanently deleted.

Secure online survey tools

If creating and distributing online surveys, use a service or platform that has appropriate security and privacy controls in place. At this time, Nebraska Wesleyan does not have a campus-wide site license to any full-featured systems such as Survey Monkey or Qualtrics. However, NWU does license two secure platforms that offer at least some survey functionality:

Microsoft Forms, available within Office 365

Sona Systems, available through Cochrane-Woods Library

Other secure third-party options (not licensed by NWU) include Survey Monkey individual subscriptions (student and educator discounts and free plans are available) and Google Forms.

Store data within your account on the platform, rather than downloading, to ensure security.

If working on a multisite project, evaluate survey and data storage options available at each site and choose the one that offers the most security and privacy.