Guidelines for Handling Research Data at WNC

1. Introduction

The intent of this document is to provide guidelines for the handling of data about students and their course performance gathered for the purpose of research and evaluation by personnel at Western Nevada College (WNC). The guidelines are designed with the following considerations in mind:

- Easy comparison of locally gathered data with institutional data
- Security of data and protection of data under FERPA and NSHE rules
- Maintain the confidentiality of student Personally Identifiable Information (PII)

WNC Personnel should be aware that these are guidelines and not binding, except where federal, state or local law, or NSHE rules specify otherwise. However, not implementing the suggestions made here may introduce difficulty in comparing locally gathered data to institutional data. Additionally, these guidelines help to ensure the accessibility of the data to other researchers and the office of Institutional Research and Effectiveness (IRE).

For help in using these guidelines and/or designing a research project please contact the Subcommittee on College-Sponsored Research.

2. Guidelines Descriptions and Information

   a. Work with institutional data only under consultation with IRE

      To make use of record level data for research projects the researcher should discuss the scope of their project with IRE. Involving IRE early in the design of any project involving student data will ensure compliance with applicable rules and ensure better usability of data.

   b. Anonymized IDs

      Whenever possible, institutional data provided to WNC personnel by IRE should be anonymized so that nothing can be tracked back to individuals included in the study

   c. Use NSHE IDs to identify students in data sets

      When anonymized IDs can’t be used and in order to comply with NSHE and FERPA rules concerning PII it is recommended that researchers use student NSHE ID numbers as the primary identifier for any student data. Researchers requesting institutional data may be required to sign an MOU: (insert link to MOU here)

d. Maintain confidentiality of student data

   Keep student data confidential within the bounds of local, state, and federal law. For data and results used only internally at WNC and/or NSHE make all possible efforts to obscure any student PII from results. If data will be disseminated outside of NSHE in any way all student PII should be removed from published results unless the researcher has obtained written permission from each student whose PII will be published. Whenever possible, anonymized identifiers should replace NSHE IDs.

   Be aware that even within data sets without student PII some data may unintentionally identify specific students. For example, male students in the nursing program or a single Hispanic student enrolled in a specific course. In order to comply with FERPA rules such instances must be masked in any external reports.

e. Familiarize yourself with applicable law and institutional policy (eg. FERPA and Human Subjects Research and Protections training)

   There are many laws and policies regarding the gathering and use of data on human subjects. It is recommended that faculty researchers familiarize themselves with these laws and policies. Important examples of such guidelines are available in the MOU between IRE and WNC employees.

f. Encrypt Data

   To ensure the security of data it is advisable to employ encryption, particularly if the data is ever stored on any portable media, including but not limited to, external hard drives, CD/DVD optical discs, USB (thumb) drives, and laptop computers. Even data stored on an office desktop should be encrypted. Note that data stored by cloud services (Google drive, iCloud, OneDrive, Dropbox, etc.) may have an uncertain level of encryption. Before storing data on the cloud the researcher should ensure that their cloud storage provider encrypts data both in transit and at rest on their servers. Contact specific providers for detailed information. For aid in using up to date and secure encryption contact IRE.

g. Long Term Data Storage in IRE

   IRE is the best place to secure and store data long term. Upon the completion of any study, all data, whether from IRE or generated by the researcher, is to be removed from office and or personal computers and stored in the IRE office in compliance with the current policies of NSHE, WNC, and IRE. Such stored data will be made accessible to the original researcher upon request. A copy of any reports generated with institutional data originally supplied by IRE must be stored with IRE upon completion of the study subject to NSHE's Records Retention and Disposition Schedule

3. Conclusion

   The above guidelines are designed to aid both researchers and the IRE staff in studying student data. Input on these guidelines from faculty, staff, administrators, students, or other constituencies should be brought to the attention of the Subcommittee on College-Sponsored Research.

Last Revised 3/31/2023 by the Subcommittee on College-Sponsored Research