**Research Data Best Practices at WNC**

1. Introduction

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

* Easy comparison of faculty 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)

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

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

1. Best Practices Descriptions and Information
   1. Work with institutional data only under consultation with IRE

In order to make use of record level data for research projects it is advised that the researcher discuss the scope of their project with IRE in order to develop data requests that will simplify as much as possible processing by the IRE staff. Involving IRE early in the design of any project involving student data will ensure compliance with applicable rules and ensure better usability of data generated or used in the study for any future projects. Faculty requesting institutional data will be required to sign an MOU:

<https://intranet.wnc.edu/files/policymanual/mou_on_data_for_research.docx>.

* 1. Use NSHE IDs to identify students in data sets

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. This is the best way to ensure that researcher generated data can be readily compared with institutionally-available data.

* 1. Maintain confidentiality of student data

Be sure that student data is kept confidential and such confidentiality is maintained 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.

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.

* 1. Familiarize yourself with applicable law and institutional policy

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. All faculty working with data for research purposes must have current (within three years) FERPA training.

* 1. 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.

* 1. 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 of course 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.

1. Conclusion

The above guidelines are designed to aid both faculty 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 SPFIE subcommittee on College Sponsored Research.

Last Revised: 2/11/2016 by Tom Herring