Assessment Data Stewardship: Tips for Academic Programs

Office of Assessment of Teaching and Learning, Washington State University, October 2016

Context: Assessment data collected by degree programs are valuable tools in making decisions about teaching and learning. As such, it is important to both protect data and provide appropriate stakeholders with access to data and results from data analysis (i.e. information derived from data). This document provides data stewardship tips for those collecting and managing degree program assessment data that align with WSU's Executive Policy #8, available: http://public.wsu.edu/~forms/HTML/EPM/EP8_University_Data_Policies.htm.

1. **Recognize Responsibility**-Assessment data are valuable resources and must be carefully managed. Data custodians are responsible for its safekeeping and appropriate use. In program-level assessment, a number of faculty, staff and administrators may be involved in the collection, use, and storage of student work and student data. Examples of individuals who may have a role in assessment include program assessment coordinators, department chairs or school directors, teaching faculty, advisors and administrative assistants.

   Note: Assessment data may come from a wide range of assessment measures, including capstone papers, senior theses, dissertations, embedded assessments, observations of student performances, portfolios of student work, pre-test/post-test assessments, standardized tests, supervisor evaluations of interns, focus groups, interviews, surveys, and course evaluations.

2. **Inform All Faculty and Staff about Data Stewardship Policies**-All faculty and staff need to be informed about WSU's data policies, including when data are not intended for public use. Maintain and refresh FERPA training and review current guidelines at ITS. ATL and the Graduate School are a resource for policies and practices regarding assessment data.

3. **Classify Type of Data and Who Should Have Access**-Data should be available to those needing the information to inform or perform their responsibilities. Each individual with access to assessment data has the responsibility to use those data and any information derived from them appropriately. Non-public and confidential data should be labeled and only be used to support assigned roles and duties at WSU.

   Note: Programs may decide to categorize the various data about students and student learning that they collect and analyze for program assessment as "non-public" (if it is not categorized in another way); in general, assessment data are intended for internal use by authorized department faculty and administration for program improvement in support of their assigned roles and duties. Determinations to share data outside the program can be made as needed and care taken in presentation (see Tip #8).

4. **Share Results with Appropriate Constituents**-Programs may decide to limit access to assessment data to authorized department faculty and administration in support of their assigned roles and duties (*see Tip #3)*. Ideally, the data analysis results from program-level assessment should be shared with the department chair or school director, all faculty members with teaching responsibilities on all campuses, and committees, such as curriculum or assessment committees.

5. **Develop an Archive**-Assessment data and any information derived from data are managed as assets for use by the degree program, department or college. The usefulness and effectiveness of data depend on their being kept accurate and complete. Each department needs a secure location behind a WSU login for storage of assessment data, results, tools, and reports. This could take the form of a shared drive, SharePoint, or another software or secure storage.
   (See Tip #10 for ITS data security guidelines).

6. **Protect Access to Data**-Assessment data must be effectively protected from unauthorized acquisition or disclosure as well as accidental or intentional modification, destruction, or loss. This must be done to ensure data confidentiality, integrity and to prevent unnecessary litigation. The most effective approach is to not store sensitive data on mobile devices or media; instead use secure remote access such as your remote desktop or department shared drive to connect to a university server or your office workstation.

   Note: *Transport of non-public data on portable devices/media, such as laptops or flashdrives, should only be done when required to conduct functions associated with assigned roles at the WSU, which includes work as assessment coordinator, assessment committee member, chair and teaching faculty. In that case, confidential or non-public data should be stored securely on physically secured storage devices and encrypted and/or password protected, using commercially reasonable business practices. (See Tip #10 for ITS data security guidelines and EP8.)*

7. **Take Care in Distribution of Data**-If data or any information derived from data are non-public or confidential they should be marked in some way to indicate this (such as a footer or watermark), as a reminder about the intended audience. Care should be taken to avoid confidential or non-public data being released for public viewing.

8. **Take Care in Presentation of Data**-WSU has a general policy of *not* presenting results with group or cell sizes less than five, particularly for demographic information (gender, age, ethnicity, etc.). Instead, it's recommended to group small cell sizes in some other logical way (such as into an "other" category). This policy is intended to decrease the likelihood of unintentional breaches of confidentiality and to avoid reporting where averages are unlikely to be representative.

9. **Avoid Common Blunders with Assessment Data**-Assessment data are usually collected at the program level, but must be protected, maintained and distributed in the same way as institutional data. Avoid these common blunders:

   - Keeping assessment data on an individual's laptop or desktop, and not protected, backed-up, or archived
   - Presenting or disseminating results from very small groups, increasing the likelihood that individuals represented in the data may be recognized and thus their confidentiality unintentionally breached
   - Including student names or identifying information in summary reports (or failing to, wherever possible, remove student names for assessment work)
   - Overly restricting internal access and distribution of results, thus preventing use of data to inform degree program decisions
   - Not keeping the intended audience in mind when creating a report or presentation and/or not explicitly indicating on reports or presentations of assessment results if the information is non-public, confidential, public, etc.

10. **Questions?** Please contact us with questions or concerns as they arise, so we can help you implement good practices that fit your department and context, and support your assessment work.

    - Undergraduate programs contact the Office of Assessment of Teaching and Learning
    - Graduate programs contact the Graduate School
    - Institutional Research is a resource for all programs
    - ITS good practices: data security, security awareness, and EP8.