Goals and Principles for Learning Analytics at the University of Washington

Learning analytics

Learning analytics refers to the collection, analysis, and use of student data to improve learning, retention, and academic planning. For example, learning analytics may employ statistical modeling or machine learning techniques to recommend degree pathways or identify students who are at risk of leaving the university.

As UW begins employing learning analytics to improve student success, it is important to establish clear goals and principles that will help guide the appropriate and ethical use of learning analytics. These goals and principles are aspirational and intended to serve as a foundation for UW in the rapidly emerging field of learning analytics.

The use of learning analytic data is for UW personnel to support teaching, learning, and the student experience. The goals and principles in this document are intended to help guide UW faculty, administrators, and staff in the appropriate use of learning analytics.

Goals for the use of learning analytics

Inspired by its fundamental values, UW currently has three goals for the use of learning analytics:

- To help students achieve their learning goals,
- To improve persistence and retention, and
- To reduce the time it takes to finish a degree.

These goals may be achieved in a variety of ways, including, but not limited to: (1) using learning analytics to support academic departments and units as they strive to customize the teaching and learning experience to better meet student needs; (2) matching UW-provided support and services with the students who need them the most; (3) aligning advising practices and student interest or needs; or (4) shaping academic planning tools for students.

Principles for the use of learning analytics

Responsibility

The foundational and guiding principle for the use of learning analytics at UW is responsibility.

- Following its core values, UW has a responsibility to improve student persistence, help students achieve their learning goals, and support their journey toward a degree. This can be accomplished, in part, by extracting meaning from student data via learning analytics.
- As described in the following sections, UW also has the responsibility to ensure that: learning analytic approaches and practices are valid and effective, UW privacy principles and security policies are upheld, and a governance structure is in place to ensure that such activities do not compromise UW’s values and policies.

Validity and efficacy

Assessment and refinement of modeling, analysis and practices will be an ongoing process to ensure valid results and useful and effective service delivery.

- The accuracy of the models will be closely scrutinized on a periodic basis to ensure they are
meeting an acceptable level of accuracy.

- Algorithms and other analytical processes performed on student data will be available for review with collaborating institutions so long as review does not expose student data.
- Modelling and analysis of student data will be free from undesired biased, and practices for mitigating bias in the application of learning analytics will be encouraged.
- As much as possible and practical, errors in the data will be corrected in the systems from which the data is sourced rather than in the systems in which the data is consumed, analyzed, or displayed.

Governance
Learning analytics may be required or essential to the UW’s mission. However, the benefits and risks associated with learning analytics require careful review to ensure that such activities do not compromise the UW’s values and policies.

- The Faculty Council for Teaching & Learning will exercise oversight over the goals for the use of learning analytics.
- The Vice Provost for Academic and Student Affairs or designee, will exercise oversight for the principles for the use of learning analytics.
- As needed the above governance structure will be re-evaluated and modified in order to stay consistent with the evolving data governance structure at UW.

Privacy and Security
Organizations that collect or use learning analytic data are required to follow UW privacy principles and related policies, standards, or guidelines that are in place for upholding the UW’s humanitarian, ethical, and legal obligations when it comes to individuals’ privacy. UW privacy principles are as follows:

- Due Care: Understand how UW’s global presence relates to geographical privacy requirements for protecting individuals’ privacy.
- Limited Data: Collect and use only what data are needed to provide the product or service, and de-identify whenever possible or appropriate.
- Protection: Respect and protect the data we collect using multi-layered controls and practices.
- Transparency: Use and share information only as we say we will. Provide education about data collection and use, publication, and public records disclosure and exemptions.
- User Choice: Provide user control or “choice” over the data collected about them whenever possible.

Organizations that manage or utilize information systems with learning analytics data are required to follow the UW information security policies for safeguarding UW institutional information.

UW will clearly communicate to the university community the student data that are used, how they will be used, and plans for future use. Similarly, UW’s goals for current and planned applications of learning analytics will be communicated in a timely manner.

Student data used in learning analytics
Common data sources that are in scope include, but are not limited to:

- **Enrollment information.** Data includes degree program affiliation, academic probationary status, campus affiliation, and demographics provided by the student.
● Transcript data. Data from past and current courses, including grade data.
● Data from teaching and learning tools. Activity in tools like Canvas, Panopto or Poll Everywhere, such as viewing patterns, number of discussion board posts, and logins.
● Student applications data. Data from MyUW, MyPlan and other student systems.

The student data in scope will not be sold by UW to third-party vendors. Further, third-party vendors who have access to these data to provide services to UW students will not be able to sell these data to other parties and must follow UW data privacy and ownership requirements.

Common data that are not in scope:
● Health information. Disabilities and data on visits to student health centers.
● Complaints. Formal complaints made by a student.
● Affiliations. Affiliations not directly related to academic success, such as religious or political affiliations.
● Social media activity. Student activity on third-party social networking sites.
● Biometrics. Fingerprint and other physical identifiers used in automated recognition technology. Some facilities, such as laboratories and locker rooms, may have these technologies.

1 http://www.washington.edu/about/visionvalues/
2 https://privacy.uw.edu/principles/
3 https://ciso.uw.edu/policy/uw-policies/