Code of Practice for Learning Analytics at the UofA

Adapted from the JISC Code of Practice for Learning Analytics

"The real challenge for postsecondary institutions is to keep pace with the students they serve, by providing them with the tools to succeed."

- Sheldon Levy, President, Ryerson University

The scope of this code of practice is any use of data about students and their activities to help students and the university understand and improve educational processes, and provide better support to students. Such data may be gathered and retained by systems and applications developed and managed centrally, or by Faculties, departments, or instructors. The purpose of this code of practice is to assign responsibilities and outline practices to ensure that learning analytics is carried out responsibly, appropriately, and effectively at the UofA.

Learning analytics will be used for the benefit of students. This might be through assisting them individually, or through using aggregated and anonymized data to help groups of students. Learning analytics may also be used to improve the student experience more generally. Providing feedback as early as possible in the term, rather than after a course has finished, is intended to improve learning outcomes for students. Learning analytics is distinct from assessment, and will be used for formative rather than summative purposes.

The general intent is for learning analytics to be used in larger sections where it is more difficult for instructors to engage personally with each student in their class. Learning analytics can be used in this context to provide a greater degree of individualized guidance than might otherwise be possible. Personal interactions are very valuable, and the goal of learning analytics is not to replace those.

The UofA will practice complete transparency towards students, faculty and staff regarding the purposes of learning analytics, the data collected, the processes involved, and how these data and processes will be used to enhance the student experience.

Responsibility - the university must allocate responsibility for the data and processes of learning analytics, including collection, analysis, interventions, and stewardship.

The UofA must decide who has overall responsibility for the legal, ethical and effective use of learning analytics. The university should allocate specific responsibility within the institution for:

- The collection and retention of data used for learning analytics
- The anonymization of the data where appropriate
- The analytics processes to be performed on the data, and their purposes
- The interventions to be carried out
- The stewardship and retention of data used for and generated by learning analytics

Student representatives and key staff groups at the UofA should be consulted about the objectives, design, development, roll-out, and monitoring of learning analytics.

Informed consent – ensuring students provide meaningful consent

Students must be "provided with clear and transparent information on the purposes for data collection so that they are in a position to give informed consent." (Corrin et al, "The Ethics of Learning Analytics in Australian Higher Education") While students should be given the opportunity to provide informed consent wherever possible, this is not a strict legal requirement as much of the data gathered by the institution is for the legitimate business purposes of the university.

The notions of "consent" and "informed consent" are often conflated. The latter requires clear and transparent information on the purposes for which the information being gathered may be used. Informed consent should also be gathered for any interventions that may result from the analytics be used. There may be legal, safeguarding or other circumstances where students are not permitted to opt out of particular interventions. If so, these must be clearly stated and justified. Lastly, it must be possible for students to amend consent at any time.

As Prinsloo and Slade note "Users' choices and their understanding of the scope and effectiveness of their privacy self-management are developed in context rather than in the abstract…" (LAK '15). They suggest that students be given the choice to opt-in (or not) at a point where the potential benefits are most clear. Therefore, practice at the UofA should be to request consent at the time that specific analytics are being proposed on defined data with known interventions. Possible examples include:

- asking for opt-in within an individual course section, at the point in time when an instructor has enabled a particular analytic. That might be at the beginning of the course, or later during the term.
- asking for opt-in to one or more defined analytics proposed for use throughout a student's program. This could be done during program orientation, during the first course in the program, or later during the term.

Once a student has made their selection, they should be presented at regular intervals (although not annoyingly frequently) with an option to amend their choice, and to inspect their data.

For consent to be meaningful, students must be informed about the nature and intent of data use. This must occur multiple times during the school year, such as one or two weeks after the start of each new term. Information should be disseminated in a variety of ways. These should include, for example, a social media campaign, video vignettes displayed in SUB and elsewhere, brochures distributed during orientation, brief in-person surveys conducted by student volunteers, and an instructional module available through the learning management system.

Privacy and security – ensuring individual rights are protected, and data protection legislation is complied with

This framework does not amend the UofA policies on information privacy - it is subordinate to them. Access to student data and analytics will be restricted to those identified by the university as having a legitimate need to view them. This includes, for example, access by instructors and staff. Such access will be determined by the UofA privacy policies.

Where data is to be used anonymously particular care must be taken to avoid:

- Identification of individuals from metadata
- Re-identification of individuals by aggregating multiple data sources

A privacy and security committee focusing on student data should be struck, and chaired by the Chief Information Security Officer, and the Director of the UofA Information & Privacy Office. Members should include representatives from the SU, GSA, and Postdoctoral Fellows. The University Records Officer and the Vice Provost and AVP, Information Services & Technology should be ex officio members.

The UofA Access to Information and Privacy Policy and Procedure define responsibilities and processes for gathering, retaining, using, and disclosing personal data. The responsibility for retention includes deletion of data, under GDPR regulations.

Access and control - students must be able to access their data and must be able to correct inaccurate personal data held about them

Students should be able to access all learning analytics performed on their data in meaningful, accessible formats, and be able to obtain copies of this data in a portable digital format. They should normally also be able to view the metrics and labels

attached to these data. If the UofA considers that the analytics may have a harmful impact on the student's academic progress or wellbeing it may withhold the analytics from the student, subject to clearly defined and explained policies. However, the student must be shown the data about them if they ask to see it.

Data collection for learning analytics must comply with existing institutional, provincial and federal data policies, and, in particular, be:

- Kept to the minimum necessary to deliver the purposes of the analytics reliably
- Retained only for appropriate and clearly defined periods

Students must be able to correct inaccurate personal data held about them. On request by a student any personal data used for, or generated by, learning analytics should be destroyed or anonymized, with the exception of certain, clearly specified data required for educational or statutory purposes such as grades.

Stewardship of data is the responsibility of the Data stewards in the appropriate areas, as defined in Appendix A of the Institutional Data Management and Governance Procedure.

Validity – the university must ensure data, algorithms, metrics and processes are valid

It is vital to monitor the quality, robustness, and validity of data and analytics processes in order to develop and maintain confidence in learning analytics, and to ensure it is used to the benefit of students. The UofA should ensure that:

- Inaccuracies in the data are understood and minimized
- The implications of incomplete datasets are understood
- The optimum range of data sources is selected
- Spurious correlations are avoided

All algorithms and metrics used for predictive analytics, as well as interventions should be understood, validated, reviewed and improved as appropriate by qualified staff.

Data stewards in the appropriate areas, as defined in Appendix A of the Institutional Data Management and Governance Procedure, are responsible for the validity of data in their functional areas.

Transparency of purpose - being open about all aspects of the use of learning analytics

The UofA will define the objectives for the use of learning analytics, what data is necessary to achieve these objectives, and what is out of scope. The data sources, the

purposes and goals of the analytics, the metrics used, the procedures and practices used, who has access to the analytics, the boundaries around usage, and how to interpret the data must be recorded and explained clearly to staff and students.

Positive interventions – creating appropriate interventions based on analytics

The UofA will specify the circumstances under which the university should intervene when analytics suggest that a student could benefit from additional support. This may include advising students that they should not continue on a particular pathway. Students may also have obligations to act on the analytics presented to them – if so these obligations should be clearly set out and communicated to the students.

The type and nature of interventions, and who is responsible for carrying them out, should be clearly specified. Design of interventions must consider the potential effects of those interventions, and attempt to anticipate and mitigate unintended effects. Some interventions may require human rather than digital intermediation. Predictions and interventions will normally be recorded and be auditable, and their appropriateness and effectiveness reviewed.

Context - recognizing that a student's digital footprint and any derived analytics can never give a complete picture of that person's life

"If a person's behavior doesn't make sense to you, it is because you are missing a part of their context. It's that simple."

> - Devon Price, Social Psychologist, Professor, Loyola University Chicago, School of Continuing & Professional Studies

The UofA must recognize that analytics can never give a complete picture of an individual's learning, and may sometimes ignore personal circumstances. The UofA will take steps to ensure that trends, norms, categorization, or any labelling of students do not bias staff, student or institutional perceptions and behaviours towards them, reinforce discriminatory attitudes, or increase social power differentials.

Analytics systems and interventions must be carefully designed and regularly reviewed to ensure that:

- Students maintain appropriate levels of autonomy in making decisions relating to their learning, using learning analytics where appropriate to help inform their decisions
- Opportunities for "gaming the system" or any benefit to the student from doing so are minimized
- Knowledge that their activity is being monitored does not lead to non-participation by

students or other negative impacts on their academic progress or wellbeing
- Adverse impacts as a result of giving students and staff information about the students' performance or likelihood of success are minimized
- Staff have a working understanding of legal, ethical, and unethical practice