# Values and Ethics to Guide JMU’s Early Alerts Development

## Introduction

The Early Alerts system is intended to identify students who may be at risk of withdrawing from the institution to support interventions that would increase retention rates and closing equity gaps. As such, it will integrate multiple forms of student-generated data, and this data will necessarily be identifiable. To design and implement such a system in ways that protect student privacy and well-being, and that promote JMU values, will require care and commitment throughout the design, implementation, and deployment phases.

The Early Alerts system can be understood as one form of learning analytics, which refers to “’the measurement, collection, analysis and reporting of data about learners and their contexts, for purposes of understanding and optimizing [*sic*] learning and the environments in which it occurs’” (Jones, 2019, 2, quoting Long & Siemens, 2011, 33). In the case of Early Alerts, the focus is not on classroom learning per se, but the entire learning environment—the campus—within which students’ academic process is linked to a number of other factors in the context of retention. In this sense, it can also be understood as institutional analytics, or an institution-wide analytics system that enables administrators to access data and dashboards to track students across individual courses and to compare students (Jones, 2019, 4). Because systems geared toward retention may be designed to incorporate a wide variety of data, from classroom-based learning analytics to enrollment data to social media analytics, this section will use the umbrella term of ‘data analytics’, which should be understood in this context as data analytics implemented and used by the university.

**Learning Analytics**

Collects data about learners and their contexts to optimize learning and learning environments

**Institutional Analytics**

Collects and analyzes data about students across the institution, not just in the context of an individual course

**Data Analytics**

Collects and analyzes data across disperse, large datasets to support pattern recognition, prediction, and intervention

## Process

Effectively implementing an ethical data analytics benefits from an ethical design process. This section recommends an evidence-based framework for responsible innovation that highlights four distinct categories of praxis: Anticipation, Inclusion, Responsiveness, and Reflexivity (AIRR) (Owen, et al., 2013). While the AIRR framework has been applied to many different areas related to innovation and technology, from genetically modified crops (MacNaghten, 2016) to STEM education (Tomblin and Mogul, 2020), to our knowledge it has not been applied to help universities navigate the complex challenges related to responsibly developing and implementing data analytics. One affordance of the AIRR framework is that it translates easily across the diverse group of actors and stakeholders that are involved in such projects, it is broad enough to be tailored to institutional needs, and it aligns with well-established practices for stakeholder-engaged development of projects and programs within a university setting.

    Anticipation Inclusion Responsiveness Reflexivity

Anticipation requires responsible innovators to assess multiple scenarios in relation to an innovation in order to proactively identify and analyze potential ‘unintended consequences.’

**Anticipation** recognizes that there is always the possibility of an unintended consequence. A robust anticipatory practice should make visible a variety of plausible use cases and analyze these in relation to different stakeholders, in order to determine whether design decisions in the innovation process can better maximize benefits and minimize harm. For anticipation, a guiding question is: What could go wrong with this implementation? This includes failure to achieve the goal, as well as the potential consequences of different assumptions and design decisions.

*What could go wrong with this implementation?*

**Inclusion** refers to authentic engagement with all relevant stakeholders to guide decision-making with stakeholder input. Importantly, this should occur early in the process, when input still has the potential to shape outcomes. A guiding question here is: Who are the relevant stakeholders, and how can practices of inclusion attend particularly to those with the least power in the situation?

*Who are the relevant stakeholders?*

**Responsiveness** requires innovators to not only listen to stakeholders, but to genuinely work to integrate their insights and concerns. This does not necessitate acceding to every demand, but does imply addressing legitimate concerns in a robust way. Here, a key question is: How can design and implementation best incorporate input from relevant stakeholders, and insights gleaned by anticipating diverse scenarios?

*How can we best respond to stakeholder input?*

**Reflexivity** signals the willingness of innovators to recognize the limits of their own perspectives, and to update their thinking in relation to the other three areas of praxis identified in AIRR. In other words, how can innovators make visible and transparent the assumptions and values that shape design and implementation? This also entails reflecting on decisions and documenting their rationales.

*How can we be transparent?*

## Considerations

While the university already gathers data about each student, there are several key aspects to a data-driven system that merit particular attention. First, consolidation of data into central and connected systems makes visible more aspects of a single student than when such data is collected and stored in a distributed and disconnected way. For example, the university as such may “know” when a single student misses multiple classes, when they use the university gym, when they go to the dining hall, and what they check out from the library. But when these data are disconnected, no meaning can be inferred about any relationship between these disparate facts. When this data is connected and analyzed, patterns might emerge: perhaps they checked out materials about depression, suddenly missed class and stopped going to the gym, and for the last two days has not been present in a dining hall. This might raise a flag of concern.

*Connecting data about a person creates significant, new privacy considerations as compared to the mere collection of data.*

However, this leads to a second consideration: while big data analytics can make visible patterns of correlation, this is a tool that does not provide the answer to the question of why. What a system user or analyst infers from a pattern may be incorrect. This student might have a paper due on mental health. Knowing that they could afford to miss a class or two, perhaps they went home to focus on writing this paper. Or, perhaps the student is concerned about a family member and has returned home, but is in no considerable danger themselves. Or, perhaps these events are entirely disconnected. They might have the flu, and friends are bringing them food. The difference between a correct and incorrect inference can result in harm when actions and interventions are taken based on a false narrative. Such harm can be individual, for example, decreasing a student’s sense of belonging. It can also be aggregate, for example, if a disproportionate number of false narratives target a specific student demographic that results in a pattern of poor interventions. And, whether individual or aggregate, such harm can adversely affect the university – from negatively impacting stakeholder trust in the early alerts system itself to resulting in reputational harms or even legal liability for the university.

*Actions and interventions based on false inferences can result in harm*

Moreover, as previously indicated, a third consideration in the case of a system such as an early alerts system is that this data is not only connected in order to enable analytics, it is tied to the individual. In many learning analytics and data analytics projects, data might be de-identified. While there are increasingly tools to re-identify data, which is outside the scope of this report, in the case of a system designed to enable individual interventions the data is never de-identified to begin with. It can also be highly sensitive—this is a system that likely connects a student’s personal information with physical and mental health data, educational data, social patterns, and more.

*Student data in the context of an Early Alerts system is, by design, identifiable*

This leads to a fourth consideration: Such data is consolidated and highly sensitive, which means that not only is there a potential of harm even when the system is being used correctly, the risk of a data breach is potentially considerably more damaging than in it might otherwise be. Whether in the case of normal use, i.e., the ways that the university might legitimately use the data as part of an early alerts system, or in the case of a breach, a student’s privacy may be infringed upon. Privacy can be defined as: “…an individual’s ‘right to determine for themselves when, how, and to what extent information about them is communicated to others.’ A control approach to privacy assumes not that information is absent in others’ minds, but that we can determine who can access information about ourselves and limit to whom and under what conditions it is disclosed…. Privacy-as-control is biased toward individual choice and treats information as part of one’s person.” (Jones, 2019, 6). Student privacy should be addressed, therefore, both in relation to students’ rights and in relation to outcomes that can always include data breaches.

*The sensitivity of such student data increases the potential harm of a security breach*

Even in the case of a secure system with multiple layers of protection to ensure a student’s privacy and well-being, a data analytics system, as a technology designed and implemented by humans and deployed within an institution, reflects the assumptions, values, biases, and power relations within which it is designed, implemented, and deployed: “…We suggest that learning analytics be seen as ‘a structuring device, [that is] not neutral, informed by current beliefs about what counts as knowledge and learning, coloured by assumptions about gender/race/class/capital/literacy and in service of and perpetuating existing or new power relations” (Prinsloo & Slade 2017d)” (Prinsloo and Slade, 2018). That is to say, while design, implementation, and evaluation, should strive to embody institutionally stated values, be transparent about assumptions, root out biases, and mitigate the harms of power dynamics, a human-designed system is necessarily a social product of its time and place, imbued with values and politics, that can have enormous governing power.

*Data analytics systems build in values and biases, even when this is unintentional*

These considerations raise legitimate questions about student agency. According to Reidenberg and Schaub, “For users to have control or agency, they must have awareness of the data practices and an ability to make decisions regarding participation” (Reidenberg & Schaub, 2018, 269). One way that many systems attempt to enable agency is through some form of informed consent. This refers to “…the process by which individuals are notified of how a secondary party, such as organizations (like a business) or institutions (like a university), will use information about them (Tene & Polonetsky, 2013, p. 260). It also informs them of their rights to privacy, as well as the express rights the second party retains regarding the information. After being informed of rights and information practices, individuals can then choose whether or not to agree—to *consent*—to the terms in front of them and enter into a relationship with the second party or not” (Jones, 2019, 7-8).

Yet, research on how informed consent might work in the context of data analytics in higher education suggests that there are unique challenges in this environment, and tradeoffs to be managed (Jones, 2019). For example, if students are allowed to opt in rather than to opt out—generally considered desirable from the perspective of privacy advocacy—this could result in lower levels of participation, which results in less data and a less robust data analytics system that does achieve the university’s retention goals. Additionally, much of the data collected will be metadata. Metadata is the data about data. For example, in the case of a phone call, meta data refers to the times and phone numbers involved in an exchange but not the content of the call. In the case of a university, this complicates the question of how and when consent is pursued. Determining the appropriate level of granularity for requiring student consent entails questions of ethics that span concerns about university responsibility, student autonomy and rights, and the effectiveness (outcomes) of the entire system.

One question for this system, then, is how it can achieve its goals while supporting student agency and avoiding harm. According to Prinsloo and Slade, “…Student-centered learning analytics proceeds from the basis that students are not data-providers or data-points, but that they are and should be involved in determining what data would be valuable for them to make better informed decisions within their loci of control” (Prinsloo and Slade, 2018). Could an early alerts system be designed not just to enable appropriate interventions, but to support student learning and agency in relation to their own success at JMU?

*Students are persons, not data objects*

## Recommendations

1. Define an institution-wide set of principles and policies concerning learning analytics at James Madison University and make these publicly accessible.
2. Frame ‘Early Alerts’ as a student-centered success support system that foregrounds student agency and utility in supporting their own learning and success.
3. Proactively educate students on the benefits and risks of learning analytics, as well as their rights with respect to data usage at JMU.
4. Identify which data should be opt-in, which should be opt-out, and which should be neither. These decisions should be documented and should be aligned with the stated principles and policies.
5. Document all design decisions with rationales.
6. Implement a plan for evaluating and monitoring the system once it is live.

# References

Jones, K. M. L. (2019). Learning analytics and higher education: A proposed model for establishing informed consent mechanisms to promote student privacy and autonomy. *International Journal of Educational Technology in Higher Education*, *16*(1), 24. <https://doi.org/10.1186/s41239-019-0155-0>

Owen, R., Stilgoe, J., Macnaghten, P., Gorman, M., Fisher, E., & Guston, D. (2013). A Framework for Responsible Innovation. In R. Owen, J. R. Bessant, & M. Heintz (Eds.), *Responsible innovation: Managing the responsible emergence of science and innovation in society* (pp. 27–50). John Wiley & Sons Inc.

Macnaghten, Phil. (2016) Responsible innovation and the reshaping of existing technological trajectories: the hard case of genetically modified crops, Journal of Responsible Innovation, 3:3, 282-289, DOI: [10.1080/23299460.2016.1255700](https://doi.org/10.1080/23299460.2016.1255700)

Prinsloo, Paul & Slade, Sharon. (2018). Mapping responsible learning analytics: A critical proposal. In *Responsible Analytics & Data Mining inEducation: Global Perspectives on Quality, Support, and Decision-Making*. Routledge.

Reidenberg, J. R., & Schaub, F. (2018). Achieving big data privacy in education. *Theory and Research in Education*, *16*(3), 263–279. <https://doi.org/10.1177/1477878518805308>

Tomblin, David & Nicole Mogul (2020). STS Postures: responsible innovation and research in undergraduate STEM education, Journal of Responsible Innovation, 7:sup1, 117-127, DOI: [10.1080/23299460.2020.1839230](https://doi.org/10.1080/23299460.2020.1839230)