# Data Analytics Ethics Procedure

### 1. Purpose

1.1. These procedures apply to the staff and students of [organisation name] who manage data for any analytical purposes and should be read in conjunction with the Data Analytics Ethics Policy.

1.2. The [organisation name] recognises that there are privacy risks around combining and analysing student data and that trust in data management is the foundation on which the [organisation name] social licence to use student data is based. All data use is underpinned by the [organisation name] core ethical values.

1.3. This Procedure acknowledges that access to data and sharing of knowledge is of high value to [organisation name] and its students and ensures sharing of information can occur and academic freedom is preserved.

### 2. Organisational scope

2.1. This Procedure applies to all staff of [organisation name] and should be read in conjunction with [organisation name] Records Management and Security Policy, Data Governance Board Terms of Reference (the Board), and the [organisation name] Privacy Notice. Any issues relating to the use of student data in relation to academic research must be carried out with reference to [organisation name] Human Ethics Policy.

## Procedure content

### 3. Governance

3.1. The Board is responsible for ensuring data analytic activities are carried out lawfully, in line with [organisation name] policy and in line with the Strategic Plan. The role of the Board is to facilitate and support data stewardship activities.

3.2. Where data analytics approval is granted, applicants are not permitted to deviate from the approved proposal. If new data fields or information is required an updated application for approval is required.

3.3. Applications for data are to be consistent with the Information Security Policy and requests for data are approved by Board Policy. Applications for the purposes of research should be made in accordance with the Human Ethics Policy.

3.4. Where a student or user is dissatisfied or disagrees with a Board decision they may appeal to the Board or to privacy@ or call 0800 for further advice.

### 4. Responsibilities

4.1. Users are responsible for understanding their specific responsibilities to manage information securely and complying with [organisation name] policy. Users must have a working understanding of legal, ethical practice and complete in house or on-line privacy training.

4.2. Managers and staff are responsible for promoting security and compliance with [organisation name] policy.

4.3. Information owners are responsible for complying with [organisation name] Security Manager’s advice regarding the management and storage of [organisation name] information related to [organisation name] branded websites and all confidential information.

### 5. Privacy

5.1. All data used for analytical purposes at [organisation name] must comply with the [organisation name] Privacy Notice, Information Security Policy, the Privacy Act 1993, the Public Records Act 2005 and, if you are in the European Union, the General Data Protection Regulation (GDPR).

5.2. Care must be taken to remove any personal information (including direct and indirect identifiers) before publication of reports unless consent has been granted by the persons whose information is linked to, or Board approval, or is required under [organisation name] or regulatory reporting requirements. Further safeguards may be imposed by the Board for sensitive information.

5.3. The Board may require a Privacy Impact Assessment (PIA) to be provided with applications for data for analytical purposes. The PIA should focus on the risks and help identify ways a new proposal, project, pilot or system (or changes to) may affect personal privacy.

5.4. If a privacy breach or an adverse incident occurs during data use for any analytic purpose, it is the responsibility of the user to protect individuals and/or [the organisation] by reporting this immediately to their manager or to privacy@ or call 0800.

5.5. Where there is a possibility of disclosure to a user, of an individual’s personal or sensitive information that wouldn’t ordinarily occur during their use of data for analysis that could conflict with personal or professional relationships – or a perceived conflict – appropriate steps must be taken to minimise potential risks. Conflicts of Interest Statute.

5.6. Where [organisation name] becomes aware as part of the analytic process that an individual is at risk, the usual privacy restrictions may be overridden.

### 6. Consent

6.1. [Organisation name] is permitted to collect, use and disclose personal information where there are reasonable grounds to believe that the student has authorised use of their information. However, an individual might at any point, request withdrawal of that consent and [organisation name] must respond accordingly. Where a student asks to withdraw consent or opt out of their data being used, it may not always be possible because of statutory requirements or where certain situations apply exposing the student to an adverse consequence. Where this occurs, this must be explained to the student. The student can be referred to the privacy@ or call 0800 for further advice.

6.2. The Privacy Notice sets out examples of data that do not require an individual’s consent or Board approval for data analytics purposes and lists examples of data considered sensitive or confidential that do require an individual’s consent or Board approval for data analytics purposes.

 6.3. While the Privacy Act 1993 does not specify a time that a person’s consent or authorisation for their information to be collected, used or disclosed expires, a useful rule is to seek a renewed authorisation if there is any doubt about whether the original authorisation still applies. The greater the consequences for the individual mean the more regularly the [organisation] should check with the individual for their consent for information to be collected, used or disclosed[[1]](#footnote-1).

6.4. A recent authorisation to collect, use or disclose information can generally be relied on and will be unlikely to raise concerns for an individual if their circumstances haven’t changed. However, an old authorisation may raise concerns for an individual if their circumstances have changed since they gave the [organisation] approval to collect, use or disclose their information. For example, the reason they gave their consent in the first place may no longer be valid, and unexpected consequences may result from the ongoing use of their information.

6.5. Where student consent has not been gained to use student data, the Board has the overarching authority to waiver consent if it is considered, that consent is impractical to gain or would impede data analytics, and/or that is in the public good to proceed without consent and that the benefits outweigh possible harms.

6.6. Circumstances where it may be considered appropriate to use data without explicit consent must be directed to the Board for approval.

### 7. Access

7.1. [Organisation name] collects information to carry out operations, functions and activities for purposes or legitimate interests as a [organisation name] and as an employer. The rights and responsibilities that apply to the [organisation], students and all users can be found in the terms of the [organisation name] Privacy Notice.

7.2. [Organisation name] acts as the guardian of personal information and under the Privacy Act 1993, individuals are entitled to request access to, or a copy of personal information an agency holds about them, regardless of who ‘owns’ the information. Individuals also have the right to request their information be corrected if they think it is wrong (and they are unable to update it themselves).

7.3. [Organisation name] is responsible for ensuring the security, access, accuracy and quality of the data sets that they use for data analytics is properly maintained.

7.4. If you have any questions about access email the [organisation name] Privacy Officer privacy@ or call 0800.

### 8. Bias and discrimination

8.1. While using data for analytical purposes data users must not engage in any form of profiling that could give rise to a claim of bias, prejudice or discrimination where a person is treated unfairly or less favourably as another person in the same or similar circumstance Human Rights Act 1993 and Bill of Rights Act 1990 and the Privacy Notice.

8.2. Systems must be in place at all stages of analytic activities to ensure the risk of bias and discrimination are identified and mitigated, that missing or additional fields are identified, and that data that was collected for one particular purpose is not being misused for another purpose later.

8.3. Methods and methodology must be transparent, consistent and ethical and must be able to be explained.

8.4. Interventions resulting from data analysis must be lawful, ethical and effective, and monitored to ensure no harm is done (unintended or intentional) and that there is no breach of the Staff Conduct Policy.

8.5. Where required individuals within data sets must be unidentifiable and unable to be reidentified by aggregating multiple data sources.

8.6. Data must not be bulked up (dehumanised). It must be remembered at all stages of data analytics that each piece of data is or represents an individual person and/or their activity and that the Treaty of Waitangi principles must always be applied. Data must be analysed in context and tell the story. Stakeholder Matrix.[[2]](#footnote-2)

### 9. Complaints

9.1. Where an individual is dissatisfied with a data analytics activity and feels their right to privacy or autonomy has not been respected or that privacy has been breached, they have the right to complain privacy@, call 0800, refer to Whistleblower Policy or to contact Privacy Commission.

9.2. Individuals also have the right to request their information be corrected if they think it is wrong (and they are unable to update it themselves).

### 10. Learning analytics and interventions

10.1. Learning analytic activities are designed to help tailor support services and pastoral care to students and improve the quality of teaching which may result in an intervention.

10.2. An intervention must be student focussed and may refer to analytic information, advice and guidance directed from [organisation name] staff to one or more students.

10.3. Interventions can include:

i. High-touch: Specific advising and support for students flagged with several risk factors such as low-class attendance, poor academic performance, or survey responses;

ii. Moderate touch: Example could be a student who did ‘well enough’ not to require an intervention during their first year but are more at risk after their first year;

iii. Immediate intervention: ID swipe card data, e.g. student is missing from classes.[[3]](#footnote-3)

10.4. Learning analytics may be used to inform changes to teaching and classroom learning design and support staff to provide effective information and pedagogical input.

10.5. [Organisation] should have systems and processes in place to address the possibility of unintended harm if an intervention is not safely managed (e.g. student mental health issues are being managed elsewhere or the intervener is put at mental health risk because of a/interventions).

 *What is the [organisation name] appetite for risk if students are identified as being at risk of failing? What is the ethical and legal path when the analyst/intervener identifies someone at risk? Does the new knowledge gained bring with it a responsibility to act upon it? What are the ramifications of action or inaction? The appetite to face this risk by the [organisation name]? (Griffiths et al., 2018, p. 8).*

10.6. Records of interventions must be managed in accordance with [organisation name] policy and must comply with the Privacy Act 1993. The student’s right of access to their information applies.

10.7. An intervention translation/transcription service should be available e.g. signing, Te Reo Māori, Mandarin etc and intervention ‘scripts’ (the organisation’s accepted good practice) should be agreed and in place and include the record keeping process required for managing the collection and storage of sensitive personal information that may be disclosed during an intervention.

### 11. Te Tiriti o Waitangi (the Treaty)

11.1. As [organisation name] we embrace the Treaty of Waitangi as one of our distinctive qualities. In accordance with this, all data use must be underpinned by the principles outlined in
Te Tiriti o Waitangi Statute:

a) **Partnership**: Where data analysis focuses on tangata whenua, users should work with hapū, iwi, and other Māori communities – including Māori academic colleagues and bodies such as Toihuarewa and Māori analytics and other entities within the [organisation name] – in designing their analytics. Where appropriate, the [organisation name] should consult with local tangata whenua

b) **Protection**: Analysts (users) should ensure that their processes actively respects tangata whenua rights and culture

c) **Participation**: Where analysis focuses on Māori participants, Māori should be involved in the design, management, analysis and outcomes of the analysis

d) **Practice**: For analysis focusing on Māori, analysis should provide space for Māori data practices, which includes the use of Te Reo Māori, and Māori ontology, epistemology and methodologies.

 11.2. The [organisation name] must consult carefully with Māori whānau, hapū or iwi concerning the correct protocols and practices that should be observed during any analysis that involves them.

11.3. The [organisation name] should regard Māori Data Sovereignty in the same manner that Te Papa does in that it is responsible for guardianship (safekeeping) of artefacts and is not the owner.

 *“All data is potentially taonga in relation to its utility, through technology or usefulness to the collective”. Dr Will Edwards, Ngaruahine & Data Iwi Leaders Group.*

### 12. Pacific students

12.1. Pacific youth are the lowest achieving ethnic group in education in New Zealand. Reliable recruitment, retention and achievement data must be used intelligently and sensitively, and in cultural context to support and help Pacific students succeed.

### 13. Definitions

13.1. In this document the following indicative definitions apply.

|  |  |
| --- | --- |
| At risk | Characteristics such as mental health, emotional, physical or social, financial issues which may increase the possibility that a student may not complete a course. |
| Data governance board | Board responsible for making sure data analysis activities are approved and are carried out in line with policy. |
| Data steward | Responsible for quality of the data in their domain, the focal point for data governance activity and issue resolution, including but not limited to working collaboratively with other data owners (custodians) to define business term definitions, business rules and manage and maintain the data assets for the data within their charge.[[4]](#footnote-4) |
| Data users | [Organisation name] staff who have been granted access to institutional data in order to perform assigned duties or in fulfilment of assigned roles or functions within the [organisation name]; this access is granted solely for the conduct of [organisation name] business.[[5]](#footnote-5)  |
| Intervention | Contact which may be in the form of referral to student services, academic advice, sending messages to students to spur certain actions.[[6]](#footnote-6)  |
| Learning analytics | Data generated pre-entry, during and post learning at the [organisation name] that can be used to indicate where an early intervention with the student may be appropriate and used to improve their experience, or the generation of data insights which enable the [organisation name] to target specific support to individual students and courses.[[7]](#footnote-7)  |
| Learning analytics pilot | Time limited learning analytics activities that typically apply to students and be experimental in nature and which must use test data, unless otherwise approved by the Board or explicit consent from the individual to use their data for pilot purposes has been gained. |
| Personal information | Any information about an identifiable individual whether hard copy or electronic that is not limited to their name, but where other facts or definitions will allow someone to identify the individual such as contact, demographic and academic information. |
| Privacy impact assessment (PIA) | An [assessment](https://privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment/) identifying the potential risks to an individual’s privacy arising from the collection and use of information. Focussed on identifying the ways a new proposal, project, pilot or operating system (or changes to an existing process) may affect personal privacy. |
| Privacy officer | The employee responsible for the privacy management at the [organisation name] as described by Section 23 of the [Privacy Act 1993](http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html?src=qs). privacy@ |
| Social licence | The ability to collect, use and share data because the [organisation name] has demonstrated trust and that it will practice [lawfully and ethically](https://www.victoria.ac.nz/__data/assets/pdf_file/0009/1713618/Jenkins.pdf). |
| User | Anyone using any [organisation name] information system. |

### 14. Legislative compliance

* [Bill of Rights Act 1990](http://www.legislation.govt.nz/act/public/1990/0109/latest/DLM224792.html)
* [Education Act 1989](http://www.legislation.govt.nz/act/public/1989/0080/latest/DLM175959.html?src=qs)
* [Health Information Privacy Code 1994](https://www.privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/health-information-privacy-code-1994/)
* [Human Rights Act 1993](http://www.legislation.govt.nz/act/public/1993/0082/latest/DLM304212.html)
* [Privacy Act 1993](http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html?src=qs)
* [Public Records Act 2005](http://www.legislation.govt.nz/act/public/2005/0040/latest/DLM345529.html?src=qs)
* [GDPR](https://gdpr-info.eu/)

### 15. Related documents

* [Data Futures: A Path to Social Licence: Guidelines for Trusted Data Use](https://static1.squarespace.com/static/58e9b10f9de4bb8d1fb5ebbc/t/598d014fdb29d6ff0d50c317/1502413147674/A-Path-to-Social-Licence-Guidelines-for-Trusted-Data-Use-August-2017.pdf)
* [JISC Developing a Code of Practice for Learning Analytics](https://www.jisc.ac.uk/guides/code-of-practice-for-learning-analytics)
* [Principles for the Safe and Effective Use of Data](https://www.privacy.org.nz/news-and-publications/guidance-resources/principles-for-the-safe-and-effective-use-of-data-and-analytics-guidance/)
* [Privacy Impact Assessment Handbook and Privacy by Design](https://www.privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment-handbook/)
* [Government Algorithm Transparency](https://www.data.govt.nz/use-data/data-ethics/government-algorithm-transparency-and-accountability/)
* [Microdata Output Guide](https://www.stats.govt.nz/assets/Methods/Microdata-Output-Guide-2020-v5-1.pdf)
* [Global Guidelines: Ethics in Learning Analytics](https://www.icde.org/knowledge-hub/the-aim-of-the-guidelines-is-to-identify-which-core-principles-relating-to-ethics-are-core-to-all-and-where-there-is-legitimate-differentiation-due-to-separate-legal-or-more-broadly-cultural-env-5mppk)
* [Stakeholder Matrix. Cathy O’Neil (Weapons of Math Destruction)](https://orcaarisk.com/)

#### Examples of Organisational Policy that could/should also apply:

* Academic Progress Statute
* Acceptable Use of Information Systems Statute
* Data Governance Board Policy and Procedure
* Information Security Policy
* Privacy Notice
* Records Management Policy
* Staff Conduct Policy
* Te Tiriti o Waitangi Statute
* Whistleblower Policy

### 16. Appendices

1 Application Process\* (flow chart, data request, breach forms, confidentiality agreements etc)

2 Framework

3 FAQ’s

4 PIA\*

\* Should already be in place or will need to be developed by the organisation.

### 17. References

* [Algorithm Assessment Report: Statistics NZ (2018)](https://www.data.govt.nz/assets/Uploads/Algorithm-Assessment-Report-Oct-2018.pdf)
* [A Path to Social Licence: Guidelines for Trusted Data Use (August 2017)](https://static1.squarespace.com/static/58e9b10f9de4bb8d1fb5ebbc/t/598d014fdb29d6ff0d50c317/1502413147674/A-Path-to-Social-Licence-Guidelines-for-Trusted-Data-Use-August-2017.pdf)
* [Can I See Your Social Licence Please?](https://www.victoria.ac.nz/__data/assets/pdf_file/0009/1713618/Jenkins.pdf)

### 18. Document management and control

|  |  |
| --- | --- |
| Approver | Council OR Academic Board OR Vice-Chancellor |
| Approval date | Date |
| Effective date | Date |
| Last modified | Date |
| Review date | Date |
| Sponsor | Role title |
| Contact person | Role title - extension |

1. Privacy Commissioner, When does a privacy waiver expire? [www.privacy.org.nz/further-resources/knowledge-base/view/341?t=160234\_225308](https://www.privacy.org.nz/further-resources/knowledge-base/view/341?t=160234_225308) [↑](#footnote-ref-1)
2. Stakeholder matrix, Cathy O'Neil, Weapons of Math Destruction, 2016 - [www.oneilrisk.com/](http://www.oneilrisk.com/) [↑](#footnote-ref-2)
3. Institutions’ use of data and analytics for student success, Amelia Parnell, Darlena Jones, Alexis Wesaw, and D. Christopher Brooks 2018, [www.naspa.org/images/uploads/main/Data2018\_download.pdf](http://www.naspa.org/images/uploads/main/Data2018_download.pdf) [↑](#footnote-ref-3)
4. The University of British Columbia, Data governance, Roles and responsibilities - <https://cio.ubc.ca/data-governance/people> [↑](#footnote-ref-4)
5. The University of British Columbia, Data governance, Roles and responsibilities - <https://cio.ubc.ca/data-governance/people> [↑](#footnote-ref-5)
6. Student ARC, Predicative analytics in higher education: five guiding principles for ethical use - <https://studentarc.org/tools-and-resources/report/predictive-analytics-in-higher-education-five-guiding-practices-for-ethical-use> [↑](#footnote-ref-6)
7. Jisc.ack.uk, Code of practice for learning analytics - [www.jisc.ac.uk/guides/code-of-practice-for-learning-analytics](http://www.jisc.ac.uk/guides/code-of-practice-for-learning-analytics) [↑](#footnote-ref-7)