Tertiary Education Commission
Te Amorangi Mātauranga Matua

Analysing student data

Ōritetanga learner analytics ethics framework

Acknowledgements

The Tertiary Education Commission would like to thank Victoria University of Wellington – Te Herenga Waka and the Office of the Privacy Commissioner who worked with us to build the guidance and advice in this resource.

Published by the Tertiary Education Commission

Te Amorangi Mātauranga Matua

National Office

44 The Terrace

PO Box 27048

Wellington, New Zealand

January 2021

ISBN 978-0-473-55367-8 (PDF)

Authors

The Tertiary Education Commission

Contents

Introducing the Ōritetanga learner analytics ethics framework

Learner success is essential to a successful and thriving New Zealand

Every person should receive the support they need to succeed in education, and achieve sustainable employment and lead fulfilling lives. However, our current tertiary education system does not always deliver an education experience appropriate to the needs of a large group of learners. Māori, Pacific and disabled learners are over-represented in this group.

A tertiary education system driven to achieve equity

The Government's vision for shaping a stronger education system is focused on a tertiary experience that is inclusive, equitable and connected.

Developing a tertiary system that works well for all learners is complex, as it requires coordination across a wide range of areas. While we have a specific focus on Māori, Pacific and disabled learner achievement, the Ōritetanga learner success approach will identify and support all learners at risk because it is based on a range of nuanced indicators to identify specific learner needs.

In order for tertiary education organisations (TEOs) to make a difference for all learners, we need to see a shift from individual interventions and pockets of focus to a systemic learner focus in all aspects of their operations. To achieve this goal, a holistic approach is required, involving several key elements:

- strong leadership within TEOs and in relationships with key partners (including employers, family, whānau, iwi)
- systems and processes designed with the learner in mind, including teaching and learning environments
- a 'guided pathways' approach that makes it clear to learners before they enrol what they need to do to gain a qualification and where their qualification will lead them
- data and technology solutions that can be used to appropriately track learner progress and support learner success.

Introduction to analysing student data

Using large amounts of student data as the basis for predicting learner success is not without risks. Predictive analytic models typically use millions of data points relating to the characteristics and behaviours of thousands of learners. Collating and using this data raises a number of significant issues and potential risks, including: privacy, informed consent, de-identification of data, and the appropriate collection and management of data. In addition, there are real concerns about how the outputs of any predictive analytic models might be misused, for example, profiling to exclude "high-risk" learners'.

Back to Contents

Learner analytics

Learner analytics uses data to better understand the pastoral and education needs of your students

Learner analytics activities are designed to help tailor support services and pastoral care to students and improve the quality of teaching.

Learner analytics involves using student data to indicate where an early intervention may improve the student's experience, or to target specific support to individuals.

Intervention may include referral to student services, academic advice, or sending messages to students to encourage certain actions.

Learner analytics may inform changes to teaching and classroom learning design and may support staff to provide effective information and pedagogical input.

Learner analytics uses personal information

Personal information is collected from students before and during enrolment for verification and reporting purposes. This personal information can include previous education records, and detailed personal information such as date of birth, next of kin, gender, ethnicity, addresses, passport, and birth or marriage certificates.

With more complex learner analytics, information relating to the student's class attendance and academic performance can be collected during the whole cycle of student life.

The use of such personal data needs to balance the student's rights and responsibilities against your rights and responsibilities as the TEO.

There are several risks involved in using personal data to determine whether interventions are needed. You need to comply with privacy law, and you don't want to be perceived as overly intrusive, or to negatively impact on your TEO's reputation.

Learner analytics risks

Risks of poor management of personal data include:

- students may have insufficient knowledge of where their data is and how it's being used, which could affect their perception of the learner analytics programme
- inaccurate data can skew results and will not deliver the benefits intended
- relying on analytical tools without human oversight could result in less tailored results that don't recognise nuance
- bias (perceived or actual) can negatively impact the learner analytics programme's results
- failing to account for Māori data sovereignty could disempower Māori students, their whānau, hapū or iwi
- analysing data outside of its cultural context may not help Pasifika students to succeed

Back to Contents

› careless security practices could result in accidental disclosures and susceptibility to theft from outside parties.

These risks would make your TEO non-compliant with privacy law. They could reduce trust in your organisation and lead to reputational damage, disaffected students and declining enrolments.

Should you use learner analytics?

Before you start using learner analytics, consider the following questions.

› **Why do you want to apply learner analytics?** What value will it add to your organisation?

› **What are the objectives and boundaries of learner analytics?** What data will you collect, for what purpose and for how long?

› **What data do you already collect?** Will you need additional data to apply learner analytics?

› **Have you involved your stakeholders?** Do you know the views of students, staff, the community, Māori, Pasifika, international students, disabled persons?

› **What is your consent process?** Can you clearly explain to students what information is needed and why? Do students have the ability to opt out without consequences?

› **Can data be aggregated or anonymised and still achieve the desired results?** Does all the data need to be identifiable?

› **Is your data stored securely?** Do you know who has access to it and can you control and monitor access?

› **Do external providers meet data security standards?** Do your contracts clearly specify the responsibilities for data security?

Process checklist

Given the risks of poor data management, can your TEO implement a learner analytics programme?

Use the Learner analytics process checklist on the next page to confirm what documents and processes you have in place currently.

If you are lacking anything, read on for guidance on how to establish an ethical data practice, data management principles, and for helpful links and templates to adapt for your TEO.

The size of your organisation, the number of students enrolled, the type of data you want to use, and the interventions you intend to use will all factor into your decision to implement learner analytics.

The checklist includes all documents and processes needed for a large TEO that intends to target interventions to individuals. A small TEO may want to limit interventions and have fewer organisational policies overall. The checklist offers all the documents you need for best-practice privacy generally, and especially before you implement learner analytics.

You can ask for support from the Tertiary Education Commission (TEC) to guide you through this process.

Learner analytics process checklist

You should have these processes in place before you implement learner analytics in order to achieve optimal privacy and ethical practice. Where shown, templates are available in this resource and can be downloaded from the TEC website

Name	Description	Template
Data governance board	A board should monitor and approve changes to data use, check ethical principles are followed and be accountable for maintaining data-related policies.	
Privacy notice	Commonly located on websites, this document publicly sets out your TEO's personal information management practices.	Page 36
Data analytics ethics policy	This policy outlines ethical management of student data.	Page 39
Data analytics ethics procedure	To be read alongside the above policy, this sets out the responsibilities of ethical data analytics.	Page 43
Code of Conduct	This addresses the need for staff to adhere to the privacy and ethical data use policy.	
Privacy training	All staff should be trained in privacy generally; however, those working directly with data must receive specific training in ethical data use.	
Frequently asked questions (FAQs)	These clearly explain learner analytics to students who wish to know more about the process.	Page 17
Data request access process	Your TEO needs a process for managing student information requests and responding in time.	
Complaints process	Students need an established channel to complain and give feedback on use of their data.	
Consent explainer	Students must have full knowledge of learner analytics before they consent to participate.	Page 22
Records retention policy	This provides a clear structure for managing, storing and disposing of the information held.	
Privacy impact assessments (PIA)	Any change to systems or processes should be subject to a PIA to mitigate privacy risks.	Page 52
Risk and assurance model	Strategic data decisions should be made in alignment with your risk and assurance model.	
Secure systems	Data must be stored in a system with controlled access and IT security protections including monitoring and auditing to show exceptional access.	

Frameworks and principles

Aspirations and principles

Ethical and privacy issues in learner analytics include:

- the conditions for the collection or aggregation of data
- informed consent
- de-identification of data
- transparency
- data security
- interpretation of data, and
- data classification and management.

The aspirations and principles below can be adapted by your TEO to guide your approach.

Aspirations

To ethically employ student data analytics in order to support personal academic success and improve enrolments and retention within the TEO.

To ensure that all use of student data at the TEO is carried out ethically and in accordance with all legal requirements and TEO policy, including Te Tiriti o Waitangi.

Principles

1. The purpose of and approach to analysis must be transparent.
2. Quality systems must be in place to ensure accuracy and privacy.
3. Analysis must be human-focused.
4. Bias and discrimination must be identified and managed.
5. Data will be used safely and securely.
6. Analysis will be underpinned by Treaty of Waitangi principles.
7. Governance will be in place ensuring analysis is lawful and ethical.
8. Rules apply around the use of data in evaluations.

Adopt an ethical framework

TEOs are the trusted kaitiaki (custodians) of non-research data. You have a legal obligation to keep the information secure at all stages of collection, storage and analysis, and use it ethically and lawfully.

The law you need to follow is the Privacy Act 1993. This legislation sets out 12 information privacy principles to guide your data collection, security and use. You can find the full text of the act on the New Zealand Legislation website and useful information about the principles on the Privacy Commissioner's website.

Ethical considerations need to go further than legislation.

---

*Remember, even though you can collect, use and disclose the data in a way that's legally compliant, you need to think about whether you **should**.*

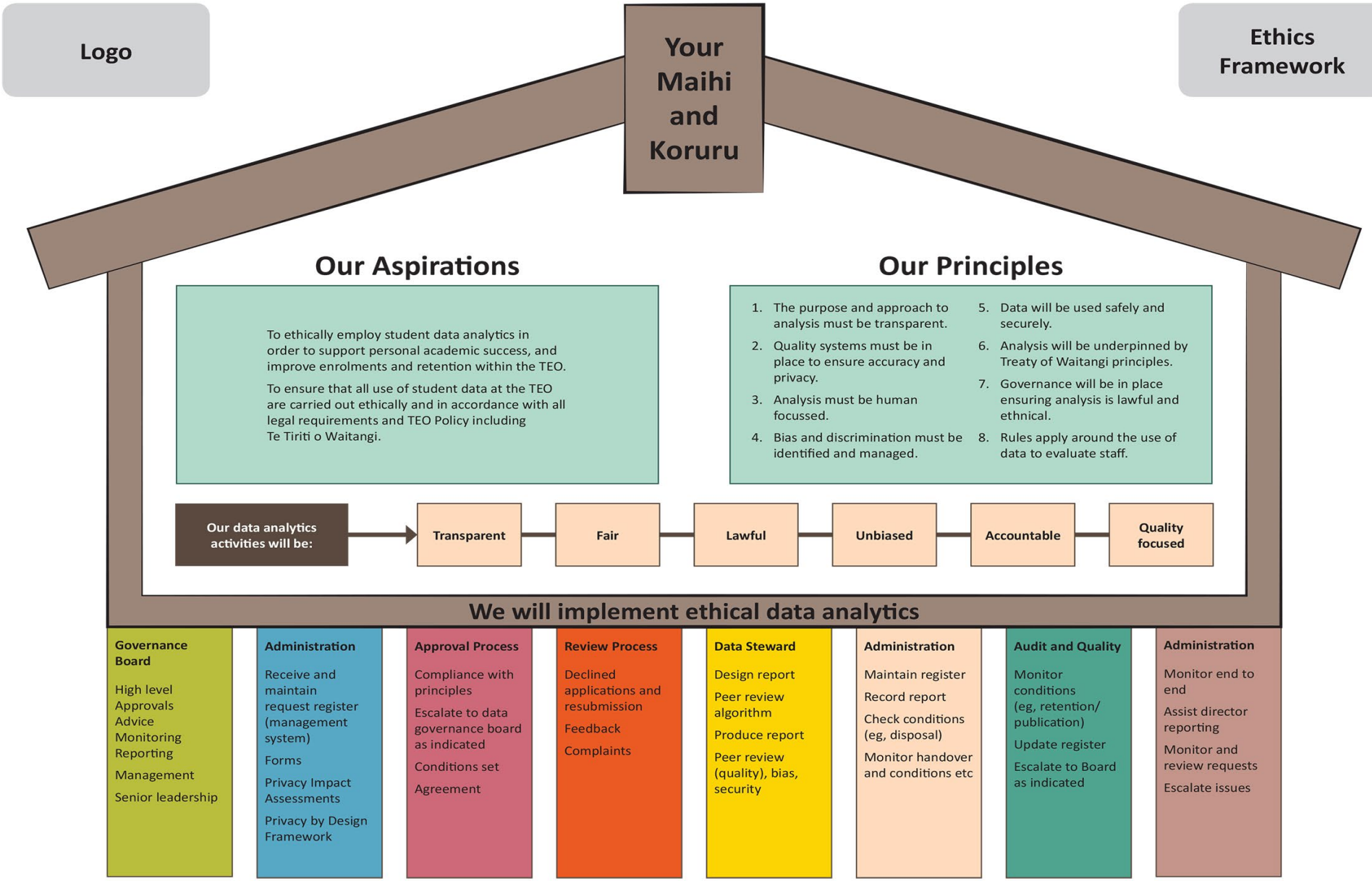

Figure 1 A framework for the ethical use of student data analytics © Victoria University of Wellington, New Zealand 2020

Privacy Act principles

New Zealand privacy law is governed by the Privacy Act 1993. You should familiarise yourselves with the 12 information privacy principles to begin.

1. Collection purpose: Only collect personal information if you really need it

- There must be a lawful purpose for collecting information which is connected to a function or activity of your TEO.
- When collecting information about a person, consider:
  - Do you really need all that information?
  - Is the information connected to one of your purposes?
  - What information do you need to help this person?
  - Can you achieve the same outcome with less information?

2. Information source: Get it straight from the person concerned

- Collecting information directly from the person concerned is always the best approach. However, there can be situations where it's not appropriate or possible to do this, and you need to collect the information from another party.
- You can do this if the information is publicly available, if the person authorises it, or to maintain the law.
- You can also collect personal information from another source if collecting it directly would compromise collection, endanger someone's safety, or is not reasonably practical.

3. Transparency: Explain what you're going to do with it

- Being open and transparent is the key to collecting personal information. People have the right to know what information is being collected about them, what it will be used for, who will receive it and how long it will be kept.

You must tell people whether collection of personal information is authorised under law, whether they are required to provide the information, and the consequences of not providing it.

- Being open and transparent also means telling people of their rights to access and correct their information.

4. Collection manner: Collect it legally and fairly

- Information must always be collected in a lawful, fair and reasonable way. Be fair and respectful about how you get information.

5. Storage and security: Keep it safe and secure

- Ensure personal information is not lost, modified, disclosed or accessed inappropriately.
- Simple ways to protect the security of information include using encryption to transfer information and anonymising or de-identifying information where possible.

Back to Contents

6. Access: Let the person see it if they ask to

- Subject to certain conditions, people have the right to access their personal information if they request it. You have 20 working days from receiving the request to decide whether the information will be granted and to let the person know the outcome.

7. Correction: Let the person ask for it to be corrected

- People have the right to ask for correction of the information held about them. You must either correct the information or decline the request and attach a note to the information stating that a correction was requested and what the request was.

8. Accuracy: Make sure it's accurate and up to date before it gets used

- Before you use or disclose information about a person you need to be confident that it's accurate. That means making sure it's up to date, complete, relevant and not misleading.

9. Retention: Dispose of it when it's no longer needed

- You must dispose of information when you no longer have a reason to retain it. You can't keep information just because it might be useful in the future or for another purpose. If you have stated that you will destroy the information within a certain timeframe, you must do so.

10. Use: Use information only for the purpose it was collected for

- Generally, you can only use information for the same reason that you collected the information.
- If you need to use the information for a different purpose, get permission from the person to do this.
- The exceptions to this are:
  - if the information is publicly available
  - the use is necessary to uphold or enforce the law
  - the use could prevent or reduce a serious threat to public health or safety, or
  - if the person is not identifiable (this involves more than just removing someone's name).

11. Disclosure: Share information only if there is a good reason

- You can share personal information outside your TEO if the reason for disclosing it is directly related to the reason you collected it.
- You can also share personal information if:
  - the person gives permission
  - it is required to uphold the law or prevent a serious threat to someone
  - the information is already publicly available, or
  - the person can't be identified in the information.

12. Unique identifiers: Only assign these to information where it's clearly allowed

- A unique identifier (such as a student ID) is assigned to a person to enable an agency to carry out its functions. Unique identifiers can only be assigned when certain of the person's identity.

Key components

Transparency

Communication

Organisations should be open when collecting information. Make sure that the person will not be surprised about how that information is used later on, or whom it will be given to.

Consent is difficult for an enrolling student to understand and what real consent looks like is largely dependent on wording of your Privacy notice. Students are at risk of being involved in learning analytics without their consent, or having given uninformed consent.

Remember that individual human lives are behind the data, and that all data activities must comply with the ethics policy principles.

Make use of our templates:

- Privacy notice
- Frequently asked questions (FAQs)
- Consent forms
- Data analytics ethics policy
- Data analytics ethics procedure.

Privacy notice

A privacy notice is an outward-facing document, usually on a website, that shows the public how you manage personal information. It is especially necessary for people who will use your services, ie, students, to understand what you do with their information.

Privacy notices contain similar information to consent forms. The difference is that a privacy notice relates to your whole organisation and can be referred back to students. A consent form is specific to one use of the information.

A student may sign several consent forms during their study, but you only need one privacy notice.

A draft privacy notice that you could adapt for your organisation, if you don't already have one, is available on page 36 or can be downloaded from the TEC website.

Ethical data analytics

Data analytics ethics policy and procedure

The following policy and procedure templates are designed to be adapted by your organisation.

› The data analytics ethics policy ensures that all use of student data is carried out ethically and in accordance with all legal requirements.

› The data analytics ethics procedure applies to the staff and students who manage data for any analytical purposes. It recognises that there are privacy risks around analysing student data and outlines procedures and responsibilities to manage this effectively.

These templates (pages 39 – 43) can also be downloaded from the TEC website.

Principles for the safe and effective use of data and analytics

The Privacy Commissioner and the Government Chief Data Steward have jointly developed six key principles to support safe and effective data analytics. Using these principles in systems and thinking means stronger, more secure and safer data use.

The six principles are:

› deliver clear public benefit

› ensure data is fit for purpose

› focus on people

› maintain transparency

› understand the limitations

› retain human oversight.

The Privacy Commissioner's website provides:

› details on the principles

› data analytics resources.

Frequently asked questions

Make this information and FAQs available to students and people who want to know about the use of personal information through learner analytics. Keep a note of other frequently asked questions and add them, with answers, to the webpage.

› Privacy covers the way we handle personal information about our data subjects (the people we deal with, including our students, alumni, donors, research participants and colleagues). We need this information to do our jobs, but people will only give us their information if they trust us to use it responsibly and treat it with care and respect.

› Personal information is any information about an identifiable individual – hard copy, electronic or verbal. It is information that could allow someone to identify an individual.

› Privacy is not about secrecy or confidentiality (although some of our processes, such as research projects or health services, do require special consideration of confidentiality). We must protect personal information from misuse, but we must also use and share that information appropriately to deliver services and do our work.

Privacy is about the fair and responsible use of personal information. We have developed policies and procedures around the following fundamental privacy concepts:

› data minimisation – limiting the amount of personal information we collect and retain

› transparency – being open and honest about what information we collect and how it will be used

› security – protecting the personal information we hold from harm

› use limitation for intended purposes – making sure we use and share personal information only when necessary and with a lawful basis

› privacy rights – helping our data subjects to exercise their privacy rights and maintain some control over their information.

If we all try our best to stick to these key principles, then we'll have a good chance of getting privacy right and protect our data and our people from harm.

The links and guides on this page should help you to understand your obligations and manage important privacy processes well. This is a summary of some questions that are answered in accordance with our privacy notice.

1. What legal basis does [organisation name] have to use my information?

[Organisation name] collects information to carry out operations, functions and activities or legitimate interests. Learner analytics helps us to help you receive the best education and opportunities, tailored to your specific needs.

The rights and responsibilities that apply to the [organisation name], students and all users can be found in the terms of the [organisation name] Privacy Notice.

2. Do I have to give my consent before [organisation name] collects and uses my personal information for learner analytics?

Typically, you are asked to provide consent as part of enrolling at [organisation name]. Under the [organisation name] Privacy Notice you can see the privacy rights and responsibilities (for yourself and the organisation name).

3. **Can I opt out or withdraw consent from [organisation name] collecting and using my personal information for learner analytics?**

   You can ask to withdraw consent or opt out of your data being used for learner analytics; however, it may not always be possible for us to delete your data because of statutory obligations that require us to keep student data. Where we are required to keep your data, this must be explained to you. If you have any questions email your [organisation name] Privacy Officer, privacy@[organisation name], or call 0800 [organisation].

4. **Can I get a copy of my data or information [organisation name] holds on me?**

   Yes. The [organisation name] acts as the guardian of your personal information and under the Privacy Act 1993. You are entitled to request access to or a copy of personal information an agency holds about you. However, the [organisation] may withhold information under special circumstances as set out in the Privacy Act 1993. If you have any questions email your [organisation name] Privacy Officer, privacy@[organisation name], or call 0800 [organisation].

5. **Can I ask for my information to be corrected?**

   Yes, you have the right to ask for your information be corrected if you think it is wrong (and you are unable to update it yourself online).

6. **How do I complain if I think my rights or privacy has been breached?**

   You can contact your [organisation name] Privacy Officer, privacy@[organisation name], or call 0800 [organisation].

7. **What is the GDPR and why do we need to worry about it?**

   GDPR is the general data protection regulation. If the [organisation name] is collecting new information about people who reside in the European Union, it needs to apply the rules of the GDPR. If you have any questions email your [organisation name] Privacy Officer, privacy@[organisation name], or call 0800 [organisation].

8. **Can my data be sold?**

   No. We will only ever provide your data to other external parties when it is required by law (eg, to government agencies such as the TEC for enrolment purposes).

9. **Can my data be used to discriminate against me?**

   No. The Bill of Rights Act sets out certain freedoms for New Zealanders, including the right to be free from discrimination.

   The Human Rights Act includes prohibited grounds for discriminating, exceptions, the creation of the Human Rights Commission, the creation of the Human Rights Review Tribunal, etc. The act elaborates on the right to be free from discrimination and creates certain government institutions to provide resources to those who have suffered discrimination. The two statutes work in conjunction with one another.

10. Where can I go to get more information?

If you have any questions email your [organisation name] Privacy Officer, privacy@[organisation name], or call 0800 [organisation].

You can also check out these useful websites:

- Privacy Act 2020
- Privacy Commissioner
- Bill of Rights Act 1990
- Human Rights Act 1993
- Information on the privacy principles (Office of the Privacy Commissioner)
- Code of Practice for Learning Analytics JISC UK
- Ethical Use of Student Data Open Polytech UK

Notice and consent

Transparency in privacy

Core principles

› Before we collect information from people, we should be clear about what we are collecting and why we need it. When we understand this ourselves, we are better able to explain this to the people we are collecting information from.

› We have developed some principles to help you keep people fully informed when you are collecting their information. These high-level principles are to help you ensure you are providing clear and detailed information to people.

› Where practicable, you should gain consent from individuals when you wish to collect and use their information – particularly for the purpose of learner analytics. Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation.

› Keep these principles in mind when you are developing consent processes for each piece of work you do.

Principles of notice and consent

› **People are informed before giving consent**

- Individuals should understand what personal information will be/has been collected, how it will be used or shared, and for what purposes.

- They should understand how long their consent is given for and agree to when consent starts and finishes.

› **Consent is voluntary**

- Consent should be opt-in rather than opt-out (do not gain consent using pre-ticked boxes or any other method of consent by default).
- People must also have a realistic choice regarding whether or not they provide consent. When considering whether someone has a choice to provide consent, TEC must consider the likely impact on them if they don't provide consent. The person must also understand this.

› **Consent is current and specific**

- The individual must provide a very clear and specific statement of consent.
- Consent forms should be adapted for specific collection and use.
- There is an easy way of withdrawing consent, and that is clearly communicated to them.

› **People are able to understand and communicate their consent**

- The individual or their guardian must be legally capable of understanding the nature of a consent decision, including the effect of giving or withholding consent, forming a view based on reasoned judgement and how to communicate their decision.
- Issues that could affect an individual's capacity to consent include:
  - age
  - physical or intellectual disability
  - a temporary or ongoing condition which may affect capacity
  - limited understanding of English.

Note: You should seek advice if you are unsure that the person has the capacity to provide informed consent. You should also seek advice about providing assistance such as translations into other languages, or accessible formats (eg, Braille, large type, audio, etc).

Consent forms

Each time you carry out work that requires the collection of information from people (such as learner analytics), consider whether to gain informed consent from the individual(s) you will be working with.

Decide whether you can use an existing consent form or need to develop a new form. It is important to consider whether the consent form covers all the information needed to fully inform people about the proposed collection.

The next page provides an example of the information you should provide in a consent form to explain why you are collecting personal information. The six headings below are the minimum that should be included in your consent forms to ensure you meet the requirements of the Privacy Act 1993.

We have added some example text under each heading to help you with what you could include.

Consent form explainer example

Collecting your information

Thank you for taking part in our [xxxx] programme. As part of this programme we will be collecting personal information from you. This includes things like your name, date of birth, ethnicity, gender and contact information [and specific information required for the xxxx programme]. We will collect this information directly from you and not from any other source.

Using your information

We use this information to make decisions about our [xxxx] programme and about how best to support you.

Sharing your information

Sometimes we need to share your information outside of our organisation. The table below outlines who we will share information with and why:

Who we share information with	Why we share information with them
Agency A	For reporting obligations
Agency B	To enable funding for your education [etc]

Evaluation and reporting

To help us improve our service, we might invite you to take part in an evaluation of our service. Please note that we collect non-identifying information for evaluation and research purposes.

Respecting you and your information

We make sure we follow the Privacy Act 1993 to do what's right when we use your information. We treat you and your information with respect, by acting responsibly and being ethical. We make sure any technology we use meets strict security standards, so it keeps your information safe.

Get in touch if you have a question

You have a right to ask to see your personal information and to ask for it to be corrected if it's wrong. If you have a question or complaint, please get in touch by emailing us at name@address.nz. You can also withdraw your consent at any time.

Learner analytics communication example

This is an example of how you can tell students specifically about learner analytics.

This paragraph is taken from the example privacy notice. You can include it in the notice, but you should also seek specific consent from each individual to undertake learner analytics.

> **Learner analytics**
>
> With your permission, we use the information from your enrolment application to help you succeed, improve your experience at [TEO] and complete your qualification. We analyse information about you is analysed to identify areas where you may need additional support from us.
>
> Through data analysis, we may offer such support as referring you to student services, providing academic advice or regularly checking in to help you get the most out of your course. We follow strict ethical guidelines to ensure that we treat your data with care.
>
> The information we analyse may include your: previous education records, date of birth, next of kin, gender, ethnicity, addresses, passport, and birth or marriage certificates. If you keep allowing it, we will keep collecting information about you as you continue to study here (such as lesson attendance and academic results) and with each year's enrolment application. You can opt out at any time.

Consent scenarios

Consent needs may differ and will depend on what information you are collecting and how you are collecting it. The scenarios below will help to explain consent generally, and the types of situations it will arise in.

Scenario 1

You are developing a case study about a learner which you intend to publish on the TEO website. You propose to collect detailed information from the learner including their study history, career history and aspirations for the future, and imagery or video for the website. In this scenario, as you are collecting identifiable information about an individual, you need to ensure the learner is fully aware of what and why you are collecting, and how it will be used and stored. Use a detailed consent form and information sheet in this situation.

Scenario 2

You are conducting a number of focus group sessions with approximately 15 tertiary-level students in each, to gather thoughts on proposed changes to the tertiary education system. You only intend to collect general feedback from the group, as written notes. Comments won't be attributed to specific people. In this scenario, you need to fully inform the focus group participants about the piece of work and what you are collecting. You could develop an information sheet that outlines key information about the work and how information will be collected and used. You could also develop a sign-in sheet with check boxes to confirm participants have read the information sheet and agree to participate.

Scenario 3

You are standing at the railway station with a clipboard and asking passers-by whether they agree or disagree with a proposed change to the location of your TEO. You are recording the answers as a tick in a yes or no column. In this scenario, you don't need to obtain consent, as it is not possible to identify individuals. If you are asked why you are collecting this information and what will happen to it, you should be able to provide this information and answer any additional questions.

Scenario 4

You are doing a piece of work which will assess outcomes for students with learning disabilities. You will run focus groups for learners and young people with learning disabilities. No comments will be attributed to specific people as you only intend to collect general feedback from the group, and this will be written notes. You may need to sit down with each individual to discuss the piece of work and ensure they fully understand what is being asked of them. If you are not confident that they can provide fully informed consent, then you should engage with their guardian or not collect their information.

Regardless of the group of participants you are working with, it is always important for you to assess whether those participants are capable of providing fully informed consent. In some situations, you may need to discuss consent with each individual, especially when working with persons with disabilities or youth.

Where to store your consent forms

Consent forms should be stored locally with the content that you have collected. This will make it simpler to revisit the consent if required to determine if your use of the information is still appropriate. It also allows other people to readily retrieve the consent form in future.

If you have any questions about the process, or what type of consent may be required for a piece of work, or would like some assistance in developing a consent form, please email customerservice@tec.govt.nz with 'EDUMIS - organisation name - Analysing student data' in the subject line.

Good governance

Data governance board

Good data ethics are supported by good governance, which requires commitment by senior leadership. A data governance board can help achieve this.

The data governance board develop and update the policy and procedures, ensure they are being followed and make decisions about what can and can't be done. Ideally it would include one or more members of the executive leadership team, and senior members of staff.

Requests for high-level and sensitive data can be escalated to the board for approval and the proposals decided in relation to your TEO's strategic plan, values and mission statement.

Your risk and assurance model and PIAs should be used to assist decision making.

Your data analytics processes should align with your risk and assurance policy and strategic direction, comply with Te Tiriti o Waitangi principles, and be ethical and lawful.

Regular reviews of reports and evaluations into interventions can assess data quality and effectiveness. You should regularly evaluate methodologies to help detect and minimise the risk of misinterpretation and over-analysis of data.

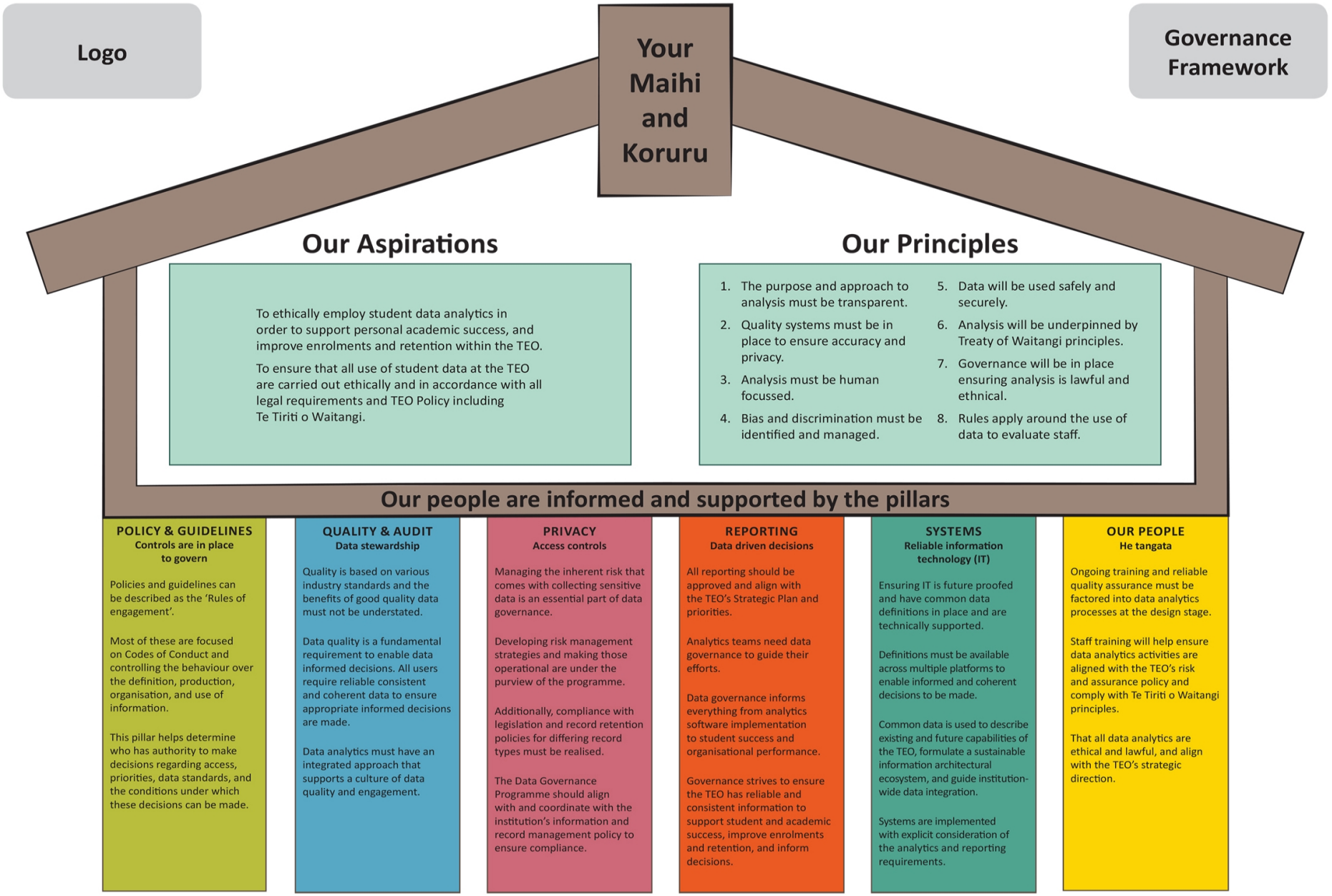

Figure 2 A governance framework for the ethical use of student data analytics © Victoria University of Wellington, New Zealand 2020

Safe and secure data use

Data anonymisation and de-identification

Anonymised data means that all the links between a person and the person's record have been irreversibly broken so that it would be impossible to identify the person in the original record.

De-identification of data means that the personal identifiers in a record have been extracted so that it would be difficult to identify the person in the original record.

De-identified data can be re-identified and be made identifiable again. Anonymised data cannot.

Where possible try to anonymise information before use and ensure that data cannot be reverse-engineered or combined with other datasets later to disclose personal information.

Where anonymisation or de-identification is not possible, a case-by-case decision should be made balancing the rights of the individuals concerned against the organisation's needs.

All data analytics activities must be carried out in compliance with the Privacy Act and with the student's best interests in mind. If in doubt, seek advice from the data governance board or your privacy officer.

De-identification

Once information is de-identified it is not 'personal information'. However, this may not completely remove the risk that an individual can be re-identified. For example, another dataset or other information could be matched with the de-identified information.

Generally, de-identification includes three steps:

1. removing personal identifiers, such as an individual's name, address, date of birth or other identifying information
2. removing or altering other information that may allow an individual to be identified, for example, because of a rare characteristic that could enable identification
3. putting controls and safeguards in place to appropriately manage the risk of re-identification.

De-identification techniques

Consider all relevant factors, including:

- the kind of information or data that is to be de-identified
- who will have access to the information, and for what purpose
- whether it contains unique or uncommon characteristics that could enable re-identification
- whether it could be targeted for re-identification because of who or what it relates to
- whether other information or data could be matched up or used to re-identify the de-identified data
- what harm may result if the information or data is re-identified.

There is sometimes a trade-off here. In some cases modifying the data may reduce its usability. Nevertheless, this may be necessary to minimise the risk of disclosing personal or confidential information.

Examples of de-identification techniques include:

- sampling — providing access to only some of the total records or data
- choice of variables — removing quasi-identifiers that are unique to an individual or are likely to identify them when combined with other information
- rounding — combining information that could identify an individual into categories, eg, express ages in ranges (25–35 years) rather than single years (27, 28)
- perturbation — altering information that is likely to identify an individual in a small way, so that the aggregate information is not significantly affected
- swapping — swapping information that may identify an individual with that of another person with similar characteristics to hide its uniqueness.
- manufacturing synthetic data — creating new values from original data so that the overall totals, values and patterns are preserved, but do not relate to any particular individual
- encryption or 'hashing' of identifiers — obscuring the original identifier, rather than removing it altogether, usually for the purposes of linking different datasets together.

Quality systems to ensure privacy

Privacy impact assessment

Privacy risk is typically managed by a privacy impact assessment (PIA).

A PIA is a process to assess risks to privacy when you are changing a process or implementing new products or services. It is a tool to help you get it right. It is not a legal opinion or a compliance exercise to tick off on your path to approval.

Consider a PIA across all phases of a project/change:

- **Start:** Complete an initial assessment pre-business case to identify any obvious privacy risks you need to be manage.
- **Design and development:** During the design phase, identify, assess and manage risks. Keep a register of recommendations and decisions.
- **Before go live:** Before implementation, check that risks have been mitigated appropriately.
- **After implementation:** Ensure that controls are operating as intended and address remaining recommendations.

Privacy impact assessment report

If you don't have an organisational PIA process, you should complete this report when you want to use learner analytics at your TEO, to help mitigate risks before implementation.

First, complete the Privacy Impact Assessment Questionnaire (page 52) to outline the different components of learner analytics at your TEO. Then get your privacy officer or a privacy expert to complete the Initial Privacy Impact Assessment Report (page 54) to outline any risks that learner analytics may pose.

Below are some common privacy risks and associated mitigations that might help to complete this process.

Highly complex learner analytics programmes may require a more thorough PIA, possibly by an external party. If in doubt, talk to your privacy officer or TEC.

You should be prepared to publish a PIA (or summary of it) on your TEO's public website.

Common risks and mitigations

Risks to consider	How to mitigate these
Collecting data above and beyond the original or legal purpose risks breaching information privacy principle (IPP) 1 of the Privacy Act.	Set a clear purpose of collection and ensure that it is related to your functions as a TEO. Being transparent about this purpose through notices and detailed explanations to student participants will help ensure that additional information is not illegitimately collected.
A lack of transparency about data that is collected and how it is being used could risk breaching IPP 3 of the Privacy Act.	Website privacy notices, clear explanations on application forms or face-to-face conversations can aid transparency. Ensure that student consent processes are well explained, documented and able to be adjusted whenever the student requires it.
Careless security practices could result in accidental disclosures and susceptibility to theft by outside parties, and risk breaching IPP 5.	Reasonable steps must be taken to ensure the security of information. Consider whether data could be anonymised or de-identified and encrypted. Ensure that staff are trained in security and ethical data management.
Having no process in place to manage requests for access to or correction of information risks breaching IPPs 6 and 7.	Establish a dedicated address where people can submit access and correction requests. It is also a good idea to create a set of templates to acknowledge, transfer, accept and decline requests. Large TEOs may wish to invest in redaction software to support document collation.
Inaccurate or out-of-date information can skew results and not deliver the benefits intended, and risk breaching IPP 8.	Data must be accurate and up-to-date before use. The risk can be mitigated through regularly checking with participants to ensure details are correct. Human oversight can also improve results with tailored interventions.

Risks to consider	How to mitigate these
Keeping information even when it is no longer useful, or the student has left your TEO, risks breaching IPP 9.	Make sure that your TEO has a retention policy and/or disposal authority to ensure that your records are appropriately archived or destroyed.
Finding a secondary use for the information you have collected on student risks a breach of IPP 10, particularly if they do not consent to this other use.	Ensure that staff are trained in ethical data analytics and know the legal exceptions for data use outside of the original purpose for collection. If you consider a secondary use ensure that each individual whose data will be used is informed of the change and consents to it.
Sharing the results of learner analytics could breach student privacy (and IPP 11) if their individual details are disclosed.	Interventions that come about as a result of learner analytics must be carefully managed, with the student fully aware of and involved in the process. It may be tempting to share results of learner analytics to the academic community, but ensure that identifying information is removed from any published reports. If a cohort is small (i.e. fewer than 5 individuals) consider masking it (eg, <5).

Training

All staff should be trained in privacy practice. However, different staff will have different training needs depending on how much personal information they manage in their day-to-day job.

All staff should understand the basics, ie, the information privacy principles from the Privacy Act, what personal information is and what to do in the event of a privacy breach.

Larger organisations could consider creating a short privacy module for staff, especially as part of an induction package.

Smaller organisations may wish to use the Office of the Privacy Commissioner's of privacy e-learning modules. These include a short 30-minute introduction to privacy, and a longer two to three hour module on the Privacy Act.

Community perspectives

Personal data collection, use and disclosure is governed by the New Zealand Privacy Act 2020, which is a principles-based framework for information management.

In addition to the legislation, however, it is recommended that you consider a wide range of community perspectives when you are considering a new use of personal information like learner analytics.

You should consider the perspectives of:

- Māori
- Pacific Peoples
- disabled communities
- refugee and migrant communities
- speakers of other languages.

Transparency and consultation with communities is key, as well as ensuring that individuals have a full understanding of data use before you begin.

The following pages examine recent guidance on personal information management beyond the Privacy Act: Māori data sovereignty and the Social Investment Agency's Data Protection and Use Policy (DPUP).

Māori data sovereignty

Te Mana Raraunga

Te Mana Raraunga (Māori Data Sovereignty Network) advocates for the realisation of Māori rights and interests in data and the ethical use of data.

- **Māori data** refers to digital or digitisable information or knowledge that is about or from Māori people, language, culture, resources or environments.
- **Māori data sovereignty** refers to the inherent rights and interests of Māori in relation to the collection, ownership and application of Māori data.
- **Māori data governance** refers to the principles, structures, accountability mechanisms, legal instruments and policies through which Māori exercise control over Māori data.

Find out more about Te Mana Raraunga.

Principles of Māori data sovereignty

From Te Mana Raraunga, October 2018

1 Rangatiratanga | Authority

1.1 **Control**. Māori have an inherent right to exercise control over Māori data and Māori data ecosystems. This right includes, but is not limited to, the creation, collection, access, analysis, interpretation, management, security, dissemination, use and reuse of Māori data.

1.2 **Jurisdiction**. Decisions about the physical and virtual storage of Māori data shall enhance control for current and future generations. Whenever possible, Māori data shall be stored in Aotearoa New Zealand.

1.3 **Self-determination**. Māori have the right to data that is relevant and empowers sustainable self-determination and effective self-governance.

2 Whakapapa | Relationships

2.1 **Context**. All data has a whakapapa (genealogy). Accurate metadata should, at minimum, provide information about the provenance of the data, the purpose(s) for its collection, the context of its collection, and the parties involved.

2.2 **Data disaggregation**. The ability to disaggregate Māori data increases its relevance for Māori communities and iwi. Māori data shall be collected and coded using categories that prioritise Māori needs and aspirations.

2.3 **Future use**. Current decision-making over data can have long-term consequences, good and bad, for future generations of Māori. A key goal of Māori data governance should be to protect against future harm.

3 Whanaungatanga | Obligations

3.1 **Balancing rights**. Individuals' rights (including privacy rights), risks and benefits in relation to data need to be balanced with those of the groups of which they are a part. In some contexts, collective Māori rights will prevail over those of individuals.

3.2 **Accountabilities**. Individuals and organisations responsible for the creation, collection, analysis, management, access, security or dissemination of Māori data are accountable to the communities, groups and individuals from whom the data derive.

4 Kotahitanga | Collective benefit

4.1 **Benefit**. Data ecosystems shall be designed and function in ways that enable Māori to derive individual and collective benefit.

4.2 **Build capacity**. Māori data sovereignty requires the development of a Māori workforce to enable the creation, collection, management, security, governance and application of data.

Back to Contents

4.3 **Connect**. Connections between Māori and other Indigenous peoples shall be supported to enable the sharing of strategies, resources and ideas in relation to data, and the attainment of common goals.

5 Manaakitanga | Reciprocity

5.1 **Respect**. The collection, use and interpretation of data shall uphold the dignity of Māori communities, groups and individuals. Data analysis that stigmatises or blames Māori can result in collective and individual harm and should be actively avoided.

5.2 **Consent**. Free, prior and informed consent shall underpin the collection and use of all data from or about Māori. Less defined types of consent shall be balanced by stronger governance arrangements.

6 Kaitiakitanga | Guardianship

6.1 **Guardianship**. Māori data shall be stored and transferred in such a way that it enables and reinforces the capacity of Māori to exercise kaitiakitanga over Māori data.

6.2 **Ethics**. Tikanga, kawa (protocols) and mātauranga (knowledge) shall underpin the protection, access and use of Māori data.

6.3 **Restrictions**. Māori shall decide which Māori data shall be controlled (tapu) or open (noa) access.

Data Protection and Use Policy

What is the Data Protection and Use Policy (DPUP)?

The Social Investment Agency's Data Protection and Use Policy (DPUP) was collaboratively developed with government agencies, non-governmental organisations (NGOs) and people who use social services.

The DPUP supports the safe and respectful use of data and information by government agencies and service providers. It includes five principles to guide data protection and use, and four good-practice guidelines in areas identified as needing greater clarity. These principles were created from the viewpoints of a diverse range of service users, social service providers, government agencies, iwi and other Māori groups, Pacific peoples and disabled communities.

The DPUP goes beyond privacy and applies ethical considerations to ensure that if and when we contemplate using people's information, it's done with the involvement, understanding and support of the people impacted by those proposals.

The DPUP principles do not affect laws relating to the collection, use or sharing of personal information (such as the Privacy Act). But they take the position that at times you can go further than the law's minimum requirements, where it's lawful to do so, in order to build trust.

The data protection and use principles

He tāngata – Focus on improving New Zealanders' lives – individuals, children and young people, families, whānau, iwi, aiga and communities.

Strive to create positive outcomes from any collection, sharing or use of data and information. Use appropriate checks and balances and ensure that information is suitable and reasonably necessary for the intended outcome.

Manaakitanga – Respect and uphold the mana and dignity of the people, whānau, communities or groups who share their data and information.

Recognise and incorporate diverse cultural interests, perspectives and needs. Include and involve services users whenever possible. Incorporate the needs and priorities of people with a specific or particular interest in what is done with their data and information.

Mana whakahaere – Empower people by giving them choice and enabling their access to, and use of, their data and information.

Where possible, give people choices and respect the choices they make. Give people easy access to and oversight of their information wherever possible.

Kaitiakitanga – Act as a steward in a way that is understood and trusted by New Zealanders.

Recognise you are a kaitiaki, rather than an owner, of data and information. Be open and transparent; support people's interest or need to understand. Keep data and information safe and secure and respect its value.

Mahitahitanga – Work as equals to create and share valuable knowledge.

Confidentially share relevant information between professionals so people get the support they want and need. Make sure there is a two-way street of sharing (de-identified) data, analysis, results and research findings to grow collective knowledge and improve services.

Find out more about the Data Protection and Use Policy.

Back to Contents

Templates

Privacy notice

[TEO name] privacy notice

This privacy notice lets you know how [TEO] will protect and manage all personal information we hold. This is a general notice that covers the privacy practices across [TEO], including at our premises and on our websites.

Personal information

Personal information is any information that identifies a person. At [TEO], personal information we collect includes:

- name and contact details (eg, phone numbers, email address, home address)
- National Student Number (NSN)
- demographic information (eg, gender, ethnicity)
- education history
- job title and organisation
- residency status.

Collecting your personal information

We collect your personal information to:

- verify your identity
- [analyse your learning experiences and progression through our courses]
- assess your eligibility to receive our services
- correspond with you
- ensure our organisation receives appropriate funding.

We generally collect this information directly from you.

You don't have to provide any personal information to us but if you don't, we may not be able to determine whether you're eligible for our services.

Occasionally, we need to collect information about you from third parties because it is not practical to collect this information directly from you. These third parties are the Ministry of Education, Ministry of Social Development (StudyLink), and TEC. We collect this because we have a statutory function to make sure that you meet eligibility criteria.

Learner analytics

With your permission, we use the information from your enrolment application to help you succeed, improve your experience at [TEO] and complete your qualification. Information about you is analysed to identify areas where you may need additional support from us. Through data analysis, we may offer such support as referring you to student services, providing academic advice or regularly checking in to help you get the most out of your course. Our learner analytics programme follows strict ethical guidelines to ensure that we treat your data with care. The information we analyse includes your: previous education records, date of birth, next of kin, gender, ethnicity, addresses, passport, and birth or marriage certificates. If you keep allowing it, we will keep collecting information about you as you continue to study here (such as lesson attendance and academic results) and with each year's enrolment application. You can opt out at any time.

Back to Contents

Sharing your personal information

We may share your personal information with StudyLink and the Ministry of Education to help them perform their functions relating to student allowances, student loans and administration.

We may disclose some of your personal information to the TEC so that, if you are eligible for fees-free tertiary education, you won't be charged inappropriately. The information we share includes:

- qualification codes
- course codes
- course start and end dates
- course equivalent full-time student (EFTS) factor
- if you withdraw, the date you withdrew
- the amount of fees-free funding you have consumed.

At all other times, we'll only disclose your personal information if you allow us, or if we are required to by law.

Looking after your personal information

We take all reasonable precautions to protect personal information we hold from misuse, loss, unauthorised access, modification or disclosure. We do this by having strong external and internal premises security, storing information in access-controlled systems, limiting staff interaction with data, ongoing auditing of our use of personal information, and providing training on the Privacy Act to all our staff.

[INCLUDE 2-3 SENTENCES ABOUT YOUR CUSTOMER RELATIONSHIP MANAGEMENT SYSTEM OR WHEREVER YOU STORE STUDENT DATA – MENTION HOW LONG INFORMATION IS KEPT IN THE SYSTEM IF KNOWN].

Accessing your personal information

You have the right to request access to any personal information we hold about you, and to ask for it to be corrected if you think that it is wrong. If you would like to request your information or seek corrections, please email us at [TEO email address e.g. for the Privacy Officer or equivalent].

Privacy on our websites

We collect information about all visits to our websites, including the:

- IP address of the device being used
- type of browser being used, eg, Internet Explorer, Chrome, Firefox
- type of device, eg, PC, laptop, phone, tablet

Our systems remove any information that might identify you and send the rest to Google Analytics [IF APPROPRIATE]. We then use Google Analytics to get information like:

- how many people are on our website
- what page was visited most in a given time period
- the location people are connecting from
- what types of devices are being used.

Find out more about Google Analytics.

We use 'cookies', which are record-keeping tokens that are stored on your device when you visit our website. The aggregate data from cookies is collected and stored on our internal servers, and only accessed by authorised staff. Cookies help us provide additional functionality to you and help us analyse site usage more accurately.

If you do not wish to receive cookies from [Your website/s], you can set your browser to refuse them or to warn you when you are about to receive one. Turning off cookies will not affect your ability to use this site.

Contact us

If you have any questions about privacy at [TEO] and our management of your personal information, you can contact us:

Email:

Post:

If you're not satisfied with our response to any privacy-related concern you may have, you can contact the Privacy Commissioner.

Email: enquiries@privacy.org.nz

Post: Office of the Privacy Commissioner, PO Box 10094, Wellington 6143

Phone: 0800 803 909 (NZ only) or +64 4 474 7590

Data Analytics Ethics Policy

1. Purpose

1.1. The purpose of this policy is to ensure that all use of student data at the [organisation name] are carried out ethically and in accordance with all legal requirements and [organisation name] policy including the Te Tiriti o Waitangi Statute, Human Ethics Policy and Records Management and Security Policy and is aligned with the [organisation name]'s Privacy Notice (and Privacy Act 1993) and Strategic Plan.

1.2. Data use for any analytical purpose is covered by this policy and includes but is not restricted to where it is used for the purposes of student support, progress and success, student satisfaction and interventions, and where it is used for teaching, planning and institutional reporting purposes.

2. Organisational scope

2.1. This Policy applies to all staff members of the [organisation name]. Ref; Definition.

Policy content

3. Principles

3.1. Data used for any analytical purposes must have a clearly articulated purpose and where possible be communicated to students. Students should be able to understand the [organisation name] purpose and approach and be confident that data is being used responsibly and by best practice. As far as possible, the [organisation name] will share its methodology and interpretation of data with students.

3.2. Only data that are fit for purpose, that are robust and accurate and to the minimum extent necessary to achieve the purpose of the data analytics activity are to be used for analytical purposes. Data used for analytical purposes must deliver clear benefits (e.g. improve the experience and outcomes) for students and the [organisation name], and to inform good practices and opportunities for improvement.

3.3. The people behind the data (the provider of the data) must be kept in mind and there must be appropriate human oversight and systems in place to ensure oversight is maintained during all stages of analytical purposes. The [organisation name] recognises that data analytics are a tool to inform human decision-making and will not wholly replace human decision-making.

3.4. The [organisation name] recognises that data used for any analytical purpose may contain a risk of actual or perceived bias and will take all reasonable steps to ensure bias is identified and managed appropriately.

3.5. All data use for any analytical purposes at the [organisation name] (including learning analytics) will reflect as far as possible the Statistics New Zealand Principles for the safe and effective use of data and analytics[1] .

3.6. In accordance with the [organisation name] Te Treaty o Waitangi Statute[2] [organisation policy], those using data for any analytical purpose must understand that Māori students, their whanau, hapu or iwi may be affected by the use of data analytics, and that Māori sovereignty (including Kowhiringa – The principle of Options) applies to all aspects of data analytics.

3.7. Reliable data must be used intelligently and sensitively, and in cultural context to support and help Pasifika students succeed.

3.8. Requests for data for analytics activities, tools and software (including testing and deployment of pilots, large project work and for data containing sensitive information) must be approved by the [organisation name] Data Governance Board (the Board) and must align with the [organisation name] Information and Records Management and Security Policy.

3.9. Data governance should include a process for assessing and approving data requests, consent and storage, and destruction requirements where applicable. The Board has authority to approve, decline or subject conditions on any application. Refer to the [organisation name] Records Management Policy for data classification: e.g. sensitive information will require Board approval – publicly accessible information requires no Board approval.

3.10. The data generated from data analytic purposes will not be used to evaluate staff performance without first discussing this with the individual staff member concerned.

4. Definitions

In this Policy, unless the context otherwise requires:

Data governance board	Board responsible for ensuring data analysis activities are approved and are carried out in line with policy. Terms of Reference, scope and name of governance board to be decided.
Information security classification	Determines the confidentiality of the material contained within a document or system. The information classification of a document may change throughout its lifecycle, however the information classification of data contained in a business information system is less likely to change throughout its lifecycle.

[1] Privacy Commissioner, Principles for safe and effective us of data and analytics, 2018, www.privacy.org.nz/news-and-publications/guidance-resources/principles-for-the-safe-and-effective-use-of-data-and-analytics-guidance/

[2] Victoria University of Wellington Te Herenga Waka, Te Tiriti o Waitangi Statute, 2019, www.victoria.ac.nz/documents/policy/governance/te-tiriti-o-waitangi-statute.pdf

Information systems	Any computer system, telephone or peripherals owned or administered by the [organisation name], together with any associated electronic or mobile data storage systems; and any communication devices, wires or wireless network intended for the transfer of information, whether on [organisation name] campuses or to which users have access through [organisation name] facilities, including the Internet.
Intervention	Contact that may be in the form of referral to student services, academic advice, sending messages to students to spur certain actions[3].
Learning analytics	Data generated pre-entry and during learning at the [organisation name] that can be used to indicate where an early intervention with the student may be appropriate to improve their experience, or the generation of data insights which enable the [organisation name] to target specific support to individual students.
Learning analytics pilots	Time limited learning analytics activities that typically, apply to students and be experimental in nature and which must use test data or have Board approval or explicit consent from the individual to use their data for pilot purposes.
Staff member	Any employee of the [organisation name], employee of a controlled entity of the [organisation name], Council Members, independent contractors or consultants engaged by or working at the [organisation name], adjunct and visiting staff, visiting scholars and interns, emeritus professors and any other person providing services to or at the [organisation name].
[organisation name] information	[organisation name] information is all information and records created by the [organisation name] covered by the Public Records Act 2005 and teaching and learning materials and research.
User	Anyone using any [organisation name] information system.

[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

5. Related documents and information

Legislative compliance

- Bill of Rights Act 1990
- Education Act 1989
- Health Information Privacy Code 1994
- Human Rights Act 1993
- Privacy Act 1993
- Public Records Act 2005

Related documents: (Examples of organisational policy)

- Academic Progress Statute
- Data Governance Board Policy
- Human Ethics Policy
- Information Security Policy
- Privacy Notice
- Records Management Policy
- Staff Conduct Policy
- Statistics NZ Principles
- Te Tiriti o Waitangi Statute
- Whistleblower Policy

6. Appendices

- Data Use for Analytics Ethics Procedure
- FAQs

7. Document management and control: (organisation format)

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].

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

---

[1] Privacy Commissioner, When does a privacy waiver expire? www.privacy.org.nz/further-resources/knowledge-base/view/341?t=160234_225308

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]

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;

---

[2] Stakeholder matrix, Cathy O'Neil, Weapons of Math Destruction, 2016 - www.oneilrisk.com/

iii. Immediate intervention: ID swipe card data, e.g. student is missing from classes.[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.

---

[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

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]
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]
Intervention	Contact which may be in the form of referral to student services, academic advice, sending messages to students to spur certain actions.[6]

[4] The University of British Columbia, Data governance, Roles and responsibilities - https://cio.ubc.ca/data-governance/people

[5] The University of British Columbia, Data governance, Roles and responsibilities - https://cio.ubc.ca/data-governance/people

[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

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]
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 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. 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.
User	Anyone using any [organisation name] information system.

14. Legislative compliance

- Bill of Rights Act 1990
- Education Act 1989
- Health Information Privacy Code 1994
- Human Rights Act 1993
- Privacy Act 1993
- Public Records Act 2005
- GDPR

[7] Jisc.ack.uk, Code of practice for learning analytics - www.jisc.ac.uk/guides/code-of-practice-for-learning-analytics

15. Related documents

- Data Futures: A Path to Social Licence: Guidelines for Trusted Data Use
- JISC Developing a Code of Practice for Learning Analytics
- Principles for the Safe and Effective Use of Data
- Privacy Impact Assessment Handbook and Privacy by Design
- Government Algorithm Transparency
- Microdata Output Guide
- Global Guidelines: Ethics in Learning Analytics
- Stakeholder Matrix. Cathy O'Neil (Weapons of Math Destruction)

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)
- A Path to Social Licence: Guidelines for Trusted Data Use (August 2017)
- Can I See Your Social Licence Please?

Back to Contents

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

Initial Privacy Impact Assessment Questionnaire

Use of learner analytics by [Your TEO]

Sponsor	
Date completed	
Summary of change	[Adoption of learner analytics – when data generated by a student prior to entry and during learning can be used to indicate where an early intervention with the student may be appropriate to improve their experience or target specific support to individual students. Such intervention can include contact in the form of referral to student services, academic advice, or sending messages to students to spur certain actions. Learning analytics may be used to inform changes to teaching and classroom learning design and support staff to provide effective information and pedagogical input.]

Assessment questions

What personal information is involved? Summarise personal information already held that will be used and confirm the original purpose for collection.	
Summarise any new personal information to be collected and provide reasons why we need this.	
Is any of the information sensitive? Could it be viewed as sensitive by those it relates to?	
Where did we get the information from? Did it come directly from individuals? Does the individual understand what we're collecting and why?	
Did it come from a third party?	
Where are we storing the information?	
If outside the organisation, including the cloud, what contractual arrangements are in place?	

How are we keeping the information safe? Has a security risk assessment been completed?	
How will people be able to access and correct their information? Will it be through standard processes or will additional steps need to be put in place?	
How do we know the information is accurate before we use it?	
How will the information be used? What is required to deliver the change proposed?	
Will we use algorithms or automated decision making?	
Do we have the right permission or basis to use it for this? Outline the consent/authority process.	
How have we communicated to individuals how we will be using their information?	
Are we going to be sharing the information with anyone else? If so, what parties will have access to information, what will they have access to and why do they need it?	
Do we have consent or a legal basis to share the information? If so, provide the details here.	
What safeguards are in place to ensure the information will be protected by those we are sharing it with?	
What will we do when we don't need the information any longer? How long we will need to retain the information for? Why is it for this period?	
How will the information be disposed of when it is no longer required?	
Are we using unique identifiers? Provide details of what we're using and why.	

Initial Privacy Impact Assessment Report

Use of learner analytics

This report is to be completed in response to a PIA questionnaire for the use of learner analytics:

Change summary	[Adoption of learner analytics – when data generated by a student prior to entry and during learning can be used to indicate where an early intervention with the student may be appropriate to improve their experience or target specific support to individual students. Such intervention can include contact in the form of referral to student services, academic advice, or sending messages to students to spur certain actions. Learning analytics may be used to inform changes to teaching and classroom learning design and support staff to provide effective information and pedagogical input.]
Sponsor	
Date completed	

Assessment table

This table summarises the privacy aspects of the proposed change and assesses the privacy risk.

The Assessment column key is: S = Satisfactory; MI = More information needed; RM = Risk mitigation recommended (at the conclusion of this report).

	Summary	**Assessment (S/MI/RM)**
Personal information (incl. sensitive)		
Information source	**Individual:**	
	Direct third party:	
	Other third party:	
Storage		
Security		

Back to Contents

Access and correction processes		
Accuracy		
Information use		
	Algorithms or automated decision making:	
	Research/analysis:	
	Consent/authority for use:	
Sharing		
	Communication of use:	
	Rationale for sharing:	
	Parties involved in sharing and information shared:	
	Consent/authority for sharing:	
	Communication for sharing:	
	Safeguards for sharing:	
Retention and disposal	**Period of retention and rationale:**	
	Disposal method:	
Unique identifiers		

Risk mitigation

Identified risk	Recommended mitigation	Completed by

Appendix

For more information

Email customerservice@tec.govt.nz with ‘EDUMIS – organisation name - Analysing student data' in the subject line.

Glossary

DPUP	Data Protection and Use Policy
EFTS	Equivalent full-time student
GDPR	General data protection regulation
IPP	Information privacy principle
NGO	Non-governmental organisation
NSN	National student number
PIA	Privacy impact assessment
TEO	Tertiary education organisation
TEC	Tertiary Education Commission