Te Tāhuhu o te Mātauranga
Ministry of Education

Te Rito Privacy Impact Assessment

Author: Alan Heward

Version: 1.0 Final

Approval Date: 21 October 2024

Release Date: December 2024

Proactively released

Te Kāwanatanga o Aotearoa
New Zealand Government

Contents

1 Executive summary 5
2 Introduction 10
3 Methodology 12
4 Summary of findings 13
5 Assessment part 1 – Te Rito system information 21
6 Assessment part 2 – Privacy Principles' analysis 56
7 Assessment part 3 – Risk assessment 72
8 Assessment part 4 – Data Protection and Use Policy (DPUP) 80
9 Assessment part 5 – GCSB Information Classification 83
Appendix A - Information Privacy Principles 84
Appendix B - Ministry risk assessment methodology 85
Appendix C - Previous PIA risks, privacy responses, and recommended controls 89
Appendix D - Te Rito summary of student data categories 90
Appendix E - Te Rito All data attributes 92
Appendix F - Logical architecture view 93
Appendix G - Document Information 95
Revision History 95
Distribution List 95
References 96

Proactively released

Figures

Figure 1 Te Rito current state - including data flows 25
Figure 2: Edsby features & functions 27
Figure 3: Te Rito planned scope – inc data flows 28
Figure 4: Te Rito Data flows – categories from source 30
Figure 5: Te Rito user roles and access 33
Figure 6: Student Admin profile view 37
Figure 7: Consents in Student Admin page 37
Figure 8: Student About Me and Portfolio 39
Figure 9: Student profile visibility to other students 39
Figure 10: Parent profile view 43
Figure 11: Change Principles 53
Figure 12: Te Rito - Student Data Overview 90
Figure 13: Te Rito data flows – logical view 93

Tables

Table 1: Summary of privacy risks 13
Table 2: Privacy enhancing controls 15
Table 3: Additional security controls 17
Table 4: Recommended additional controls 19
Table 5: Edsby functionality mapped to Te Rito Service Roadmap 26
Table 6: Te Rito attribute totals – approximation 31
Table 7: Approximate numbers of Te Rito users 31
Table 8: Example Medical condition information 41
Table 9: Privacy principles related to collection of information 57
Table 10: Privacy principles related to protection of information 61
Table 11: Privacy principles related to accessing and correcting information 63
Table 12: Privacy principles related to relevance and retention of information 64
Table 13: Privacy principles related to use and disclosure of information 66
Table 14: Privacy principles related to identifiers 69
Table 15: Te Rito AADC analysis 70
Table 16: Privacy risk assessment 72
Table 17: Controls for P-03 continued from previous page 73
Table 18: Controls applicable to every Privacy risk 79
Table 19: DPUP guidelines and Te Rito's compliance 81
Table 20: Data flows elaboration 93

Proactively released

Approvals

The following person endorses and acknowledges that the appropriate privacy risks and privacy enhancing controls have been identified:

Name and Position	Signature	Date
Maya Jones, Manager Privacy	Approved by email	20/11/24

The following person endorses and acknowledges the identified risk and recommended privacy enhancing controls:

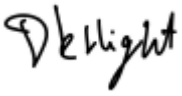
Name and Position	Signature	Date
Mark Brumby, Te Rito Program Manager	Approved by email	10/10/24

The following person approves and accepts the risks identified in this Privacy Impact Assessment, and is responsible for ensuring that the agreed privacy enhancing controls are implemented:

Name and Position	Signature	Date
Craig Haywood, Manager, Sector Products and Services	Approved by email	21/10/24
Stuart Wakefield, Chief Digital Officer	Approved by email	22/10/24

Name and Position	Signature	Date
Myles Ferris Chair Te Rau Whakatupu Māori	Approved by email	21/10/24
Graeme Barber Chair Te Rau Whakatupu – Auraki | English and Chair Te Rito Data Kaitiakitanga Group	Approved by email	21/10/24

Additional approvals/acknowledgements

Name and Position	Signature	Date
Dayton Hight, Manager Digital Assurance & Cyber Security		21/10/2024
Katrina Young, Chief Data Steward	Approved by email	28/10/24

Proactively released

1 Executive summary

Introduction

This Privacy Impact Assessment (PIA) for Te Rito identifies and assesses the privacy risks associated with the collection, use, disclosure, and storage of personal information in Te Rito. Compared to previous Te Rito PIAs, there is now more certainty about the purpose and use of Te Rito by education providers, both currently and over the next few years.

Overview

Te Rito is:

- a service for students, their school, and in the future their parents and whānau, so they can access and use the student's education related information from one place
- based on the premise that the student's record is owned by the student, under the custodianship of the Ministry and their school
- access by school staff is based on the student's enrolment status with a school
- being rolled out progressively for groups of schools, users, and functionalities. Initial access to Te Rito is for principals and teachers
- being co-designed, co-governed and co-delivered with the education sector by the Ngā Rau Whakatupu working groups.

Te Rito is provided through Edsby, a global educational service provider. The Ministry and Edsby are responsible for the overall management and operation of the Te Rito service on a day to day basis. Individual schools remain responsible for ensuring that their use of Te Rito is consistent with the Privacy Act.

Te Rito objectives and benefits

Te Rito's objectives are to have:

- information available to support students to fulfil their learning potential
- timely access to high quality information about a student to enable effective decisions to support teaching and learning
- reduced administrative burden for everyone who uses the system.

The benefits will include:

- students records travel with them as they transition from school to school. Transient children are identified quickly, and information is available to support them
- increased amount of quality information about learners is available to parents, learners, schools, and education agencies in a more timely and complete manner
- increased use of student information by teachers to improve their practice and make evidence-based decisions affecting learning
- trends for individual learners and cohorts such as Kāhui Ako can be tracked.

Te Rito data guardianship

The Te Rito Data Kaitiakitanga Group has been set up to provide a data guardianship function to oversee access and use of data in Te Rito. The group will comprise a range of stakeholders, they will provide advice to schools and kura and have a continuing role overseeing the appropriate access to and use of data in Te Rito.

To maintain trust, we need to ensure ethical and appropriate data collection, protection and use. Safely shared data is critical for the design and function of the education system, using trusted providers, platforms and services. Privacy is a core focus for Te Rito.

Proactively released

Willingness to share, partner with, and use education data is fostered by trust, confidence, capability and opportunity. To enable that, we must be clear, consistent and transparent about purpose and use.

Summary of risk and control findings

As articulated in Te Rito's objectives:

> *"It is critically important to protect the privacy and security of our learners' information whilst ensuring that the right people have access to it, for the right purpose, at the right time."*

The overall assessment of risk in this PIA is consistent with the Ministry's *Enterprise Risk Management Framework* being 'Receptive to risk' in the Strategy Design and Delivery, Service Design, and IT Functionality categories.

The level of preventative controls in place is consistent with being 'Averse to risk' in the IT Security category. Te Rito is able to demonstrate both high privacy by design and high safety by design. The residual level of privacy risk is consistent with an overall 'Aversion to risk' for Te Rito as expressed by the Ministry and Ngā Rau Whakatupu. The Edsby platform on which Te Rito is delivered has received formal certification against ISO27001 and has been successfully assessed by Safer Technology for Schools (ST4S).

Risks

Eighteen (18) privacy risks were identified through the PIA with the following residual risk ratings (see Summary of privacy risks Table 1 on page 13):

- 3 medium risks (one of these are specific to schools rather than to Te Rito)
- 15 low risks (eight of which are directly related to schools).

Nine risks identified in earlier PIAs had previously been assessed as medium-level risks after implementation of recommended controls. Of these nine:

- 4 risks continue to be assessed as medium-level risks in this PIA
- 5 risks are now assessed as low-level risks.

The previous PIAs, their risks and recommendations are summarised in Appendix C on page 89 and reviewed in detail in the Supplementary document to Appendix C.

Analysis against the UK Information Commissioners Office (ICO) Age Appropriate Design Code (AADC) shown in Table 15 on page 70 identified no additional privacy risks.

The full description of risks is provided in section 7 Assessment part 3 – Risk assessment.

Controls

Identified controls that are or will be completed before further onboarding are elaborated in Summary of privacy enhancing controls on page 15 and include:

- 28 recommended privacy-enhancing controls for Te Rito that directly reduce privacy-related risks
- 33 additional security controls that reduce the likelihood or impact of identified risks. 28 are directly related to Te Rito, 5 are not.

Five (5) additional controls are recommended, as identified in section 4.3. These will need investigation to determine their likely effectiveness in further reducing the identified privacy risks.

Additional risk review and assurance activity

Given the high level of interest and concern relating to children's privacy, as well as Te Rito effectively representing a national student repository, significant additional risk review and assurance work was undertaken. This included:

Proactively released

- detailed review of previous PIAs and similar documents prepared for Te Rito, the identified risks and applicable controls that have been implemented
- consulting with and receiving advice from external stakeholders including the Office of the Privacy Commissioner (OPC) and the Government Chief Privacy Officer (GCPO)
- collaborating and receiving feedback from Ngā Rau Whakatupu
- independent Privacy analysis and assurance of Edsby from the US Common Sense Privacy programme
- assessment by the Safer Technology for Schools (ST4S) programme used in Australia and New Zealand, and the UK Information Commissioners Office (ICO) Age Appropriate Design Code (AADC).

Advertising to, or digital profiling of, children is of heightened concern given unanticipated consequences that have now been identified particularly with social media platforms. Neither Te Rito as a service, nor the Ministry or Edsby as service providers, perform any form of advertising, targeted or otherwise, to any Te Rito users. There is no selling of Te Rito user data to any third parties, nor building of user profiles. Sharing of Te Rito data is strictly limited to authorised parties, i.e. schools.

Review of previous Te Rito PIAs

A supplementary document to Appendix C provides the detail of the risks, recommendations and controls identified in earlier PIAs, to enable traceability from the prior work to the current PIA.

The scope and design of Te Rito has changed, so some previously identified risks or recommended controls are no longer relevant. With all current controls implemented, some medium-level risks from the prior PIAs are reassessed in this PIA as being low risk. This applies to four (4) risks from the *Data Analysis ESR PIA*. Two (2) risks from the *Te Rito high level discovery phase PIA*, one (1) risk from the *SISI SMS ESR PIA*, two (2) risks from the *SISI SMS ESR PIA* remain as medium-level risks.

Scope

Scope of this PIA

The scope for this PIA is broad and covers the information that has been identified by Ngā Rau Whakatupu as being necessary to help a student's attendance, participation and progress in education, especially during changes of school. Realising this outcome will take several years.

All potential uses of Te Rito relating to this are not known at this time. Discovery and evaluation work with schools will be required to qualify and consider whether identified information is useful, necessary, and beneficial. While remaining consistent with the stated purposes and objectives of Te Rito. The planned scope for user access and technical connectivity is discussed in section 5.3.3 on page 26.

As the programme progresses and more information becomes available from schools, the Te Rito programme will:

- evaluate different approaches to deployment, reflecting differing needs and priorities for different regions, types of schools, and special cases
- and refine the definition of what student information is necessary for Te Rito's purpose

Schools and kura will decide which features or functions of Te Rito they use once they have access. Schools remain responsible for ensuring that their use of Te Rito is consistent with the Privacy Act.

Anticipated future changes that are not in scope of this PIA are listed in section 5.4 on page 28.

Proactively released

Scope of data

This PIA considers the full volume and scope of information that may be accessible via Te Rito for the full national deployment.

Across the ~2,550 schools in New Zealand there are currently ~831,000 students, ~73,000 teachers and ~50,000 other school staff. Retention of student information for up to seven years after leaving school provides an estimated total of 1,285,000 student records in Te Rito after full national rollout. Alongside this will be ~1,900,000 parent records associated to those students.

Te Rito currently only stores basic biographic, attendance, enrolment, and limited assessment information about students. Through the discovery and evaluation work, some schools will start storing in Te Rito some of the information identified in section 5.6.5 Information types.

In brief the data scope comprises:

- student data, school years 1-13, normally ages 5–18
- adult students and learning support students, aged 19 or older
- retention of student data for up to seven years after they have left school
- school staff data, primarily principals and teachers, potentially all kaimahi
- parent data, primarily in the context of a student contact relationship
- data primarily from SMSs, additional data will come from other Ministry systems such as ENROL.

A high-level summary of the in-scope student data is shown in Figure 4 on page 30. Student, parent, and kaimahi data in Te Rito is described in section 5.6.5 Information types on page 36. All attributes stored including all data about users is detailed in Appendix E - Te Rito All data attributes on page 92.

Privacy Principles' analysis

Te Rito was assessed against the 13 Information Privacy Principles (IPPs) in the Privacy Act 2020. The analysis looked at the different types of information that have been identified as being necessary by Ngā Rau Whakatupu, even though currently only some information types will be stored in Te Rito from some schools for some students. Te Rito will continue to work with schools to evaluate the information types to confirm which are useful, necessary, and beneficial.

The Privacy principles' analysis is covered in detail in Section 6 Assessment part 2 – Privacy Principles' analysis on page 56.

One of the main purposes for Te Rito is to ensure that information about students is available to their next school. This raises a concern about whether consent for onward sharing is explicitly obtained in school enrolment forms or is stipulated as a purpose for collecting student information in the first place. Analysis of a representative sample of enrolment forms and privacy statements from ~700 schools shows that 71% of schools already address their Privacy Act obligations in the context of sharing information. Further analysis is expected to see this trend to 92% of schools. Practice varies across schools. For example, some schools request consent to obtain information from a previous school and do not proactively request consent to share information to a potential future school. In lieu of consistent privacy practices, schools could rely upon the (1)(a) exceptions under IPP10 or IPP11. Where, in Privacy Act terms, the use and disclosure of information via Te Rito is directly related to the original purpose for collection.

Schools collect and store many types of information about students in the school's SMS. Similarly, a wide variety of information about students is necessary to support Te Rito's purposes. Minimising the amount of data that is collected by schools, stored and used in Te Rito is therefore challenging. To manage this, Te Rito filters input so that only specific fields of data from an SMS or other integrated system are stored in Te Rito.

Proactively released

To balance the limitations on Te Rito minimising data, a strong focus applies to the following compensatory controls:

- Role Based Access Control to ensure that only the right people have access to information
- a comprehensive *Engagement and Communications Strategy* and *Plan*
- school staff being trained in how to use Te Rito safely and effectively
- using robust information security protections to minimise the risk of technical issues leading to a privacy or security breach.

Te Rito will continue to be assessed against evolving frameworks, such as the UK Age Appropriate Design Code (AADC), to ensure the best interests of the child are met in balancing appropriate access to information in Te Rito against privacy and security considerations.

The AADC is a best practice guide published by the UK ICO and consists of fifteen standards, alongside the ICO's *children's code self-assessment risk tool*. Current analysis shows good alignment of Te Rito with the AADC Standards and provided insight for potential areas for improvement. The analysis against the AADC is covered in Section 6.1.2 on page 70.

Transparency

A comprehensive *Engagement and Communications Strategy* and *Plan* has been developed, in which building trust and confidence with stakeholders is the top objective. This is closely linked to the Te Rito iteration of the *Human Trust Framework.*

Schools will be provided with a privacy brief analysis template for Te Rito, to assist schools that choose to perform their own privacy analysis of Te Rito. This will focus on the key privacy risks and controls for schools to consider in their use of Te Rito. Feedback and recommendations about Te Rito from individual schools will be reviewed for inclusion in an update to this PIA.

From a privacy perspective the trust and confidence objective is affected by ensuring transparency to students and parents, using plain language and delivering content in a variety of formats and channels. Helping students and their parents understand that information collected by their school is stored in Te Rito, used by their schools, and shared with other schools as required is dependent on this.

Updates have already been made to the Te Rito *Terms of Use* and *Privacy Statement* to make both easier to understand. A plain language summary of this PIA will be published alongside the full PIA to aid transparency. The *Terms of Use* and *Privacy Statement* are also published in Te Reo, it is planned that the plain language PIA summary will also be translated to Te Reo.

Delivery of privacy related information in age appropriate formats is also planned, feedback from students will be proactively sought. The Te Rito *Student Acceptable Use Guidelines* is one example where feedback from students has resulted in updates.

Schools will remain responsible for informing students and parents about Te Rito in a manner that is appropriate and consistent with existing communications.

Beyond transparency in communications, enabling Te Rito to be accessible to students will improve a student's visibility of information that schools and the Ministry hold about them. This will provide students with the fundamental check and balance that information is accurate and up to date, whenever students use Te Rito.

Proactively released

2 Introduction

This Privacy Impact Assessment (PIA) for Te Rito identifies and assesses the privacy risks associated with the collection, processing, use, disclosure, and storage of the Personal Information (PI) in Te Rito. Te Rito has been in production use by schools and Early Childhood Education providers (ECE's) since 2019. Privacy analysis has been an iterative process since then. There is now more certainty about the purpose and use of Te Rito by students and education providers over the next few years. This PIA considers the full national rollout of Te Rito to all ~2,550 schools in NZ.

The purposes for Te Rito are:

1. ensure the Student records travel with them as they move schools,
2. ensure that Student records are securely shared,
3. schools and teachers are able to make informed decisions, based on access to more and better information, supported by standardised datasets providing consistent data,
4. reduced administrative burden for teachers and parents. Fewer instances of re-collecting information schools or the education ecosystem already holds,
5. A common platform with inter-operability and secure integration to other Ministry and school systems.

The benefits of Te Rito are articulated through this PIA, repeated in summary form in section 5.2.1 Te Rito objectives and benefits, section 8.2 DPUP, and Assessment against guidelines on page 80. As a high level summary:

"Our tamariki are our taonga and the information collected and held about them is also taonga. It is critically important to protect the privacy and security of our learners' information whilst ensuring that the right people have access to it, for the right purpose, at the right time."

2.1 Terms

The following terms are used in these ways in this document, based on the context:

- student or ākonga when referring to children or tamariki in the context of school
- child or tamariki when referring to children in the context of their parents or whānau
- school staff or kaimahi when referring to school staff in general
- principal or tumuaki, teacher or kaiako, teaching assistant, office administrator when referring to a specific role
- parent means people with primary responsibility for the child
- caregiver or whānau is used for extended family or guardians who have a role in the child's education. For example family who provide after-school care or transport the child between school and home. Use of parent or whānau is not intended as a legal definition.

2.2 Legal context

The Ministry and education providers must comply with the Privacy Act 2020 (the Act) when collecting, using, storing, and disclosing personal information (PI). The Act protects information about individuals and applies to every agency (public and private) that deals with PI. The 13 Information Privacy Principles (IPPs) in the Act provide the foundation that governs the protection of privacy for the collection, aggregation, use, disclosure, storage, and access to PI[1].

The Ministry must also operate in accordance with other legislation including the Education and Training Act 2020 (ETA), Official Information Act 1982, and the Public Records Act 2005.

[1] Changes to the Privacy Act came into effect on 1 December 2020 which include a new IPP 12, taking the total IPP's to 13.

Proactively released

References in this PIA to the Ministry, or Ministry of Education, being either responsible or accountable is used as a commonly understood reference instead of the full description of legal accountability being "The Sovereign in right of the Government of New Zealand acting by and through the Secretary for Education or their authorised delegate". The findings and recommended privacy enhancing controls in this report are not a legal opinion.

Schools remain responsible for ensuring that their use of Te Rito is consistent with the Privacy Act. For example that information is only shared with authorised individuals who have a need to know, and that it is used for purposes as defined in school enrolment forms or privacy statements etc.

The Master Services Agreement stipulates that Edsby must comply with the Privacy Act in the performance of providing the Te Rito service. Edsby have one sub-contractor, Hubspot, who provide customer support functions. Hubspot is within Edsby's ISO27001 scope, with Edsby responsible for handling of personal information in Hubspot.

2.3 The privacy role of supporting systems

This PIA relies on supporting systems having performed similar privacy analysis for their own purposes.

The most recent PIA's and security risk assessments for Digital Identity for Online Learning (**DI4OL**), e-Assessment Tools for Teaching and Learning (**e-asTTle**), Early Learning Information (**ELI**), **ENROL**, Funding Information Regulatory System Technology (**FIRST**), National Student Index (**NSI**), Progress and Consistency Tool (**PaCT**), Te Waharoa Ararau (**TWA**), have all been reviewed to ensure implications for this Te Rito analysis are considered.

When additional integrations are being investigated, e.g., other Ministry funding systems, a review of their current privacy and security status will be undertaken.

2.3.1 Student|ākonga login

Student|ākonga login to Te Rito will be federated from their school's identity provider, Microsoft 365 for Education or Google Workspace for Education. The Ministry also has the DI4OL federation broker platform, which went through a PIA review in 2021. The scope of the DI4OL PIA has been extended to different age cohorts ready for Te Rito production use. The Te Rito PIA assumes that any future updates of the DI4OL PIA will remain consistent with the desired outcomes for Te Rito in providing access to school students|ākonga of all ages.

2.3.2 Staff login

Staff login to Te Rito is via the Education Sector Logon (ESL) service. Where privacy recommendations are identified as relevant to the ESL, the Ministry's Digital Identity team is responsible for delivery. It is assumed that information collected by ESL has been in accordance with the Privacy Act.

2.3.3 Other systems connected to Te Rito

Where data is sourced from other systems, including a school's Student Management System (SMS), or Ministry systems such as e-asTTle or PaCT, this PIA assumes that the original collection of information, along with use and purpose has been through a PIA or equivalent review to ensure compliance with the Privacy Act.

Proactively released

3 Methodology

This Privacy Impact Assessment (PIA):

- has been completed by the Ministry of Education, following OPC[2] guidance
- uses the definition of Personal Information (PI) in the Privacy Act, OPC's PIA Toolkit, and elaborated in *Privacy ABC for Schools* as "*It has to tell us something about a person. It needs to identify that person*."
- is an input to the Certification & Accreditation and Authority To Operate (ATO) processes
- includes substantial updates and replaces the previous PIAs:
  - *Student Information Sharing Infrastructure Student Management System Early Stage Rollout Privacy Impact Assessment* (**SISI SMS ESR PIA**) 2018
  - *Learning Support Register PIA* (**LSR PIA**) 2019
  - *Te Rito Data Analysis ESR PIA* 2019
  - *Te Rito high level discovery phase PIA* 2021
- considers the privacy analysis performed for SMS Data Exchange Service (SDEX) in 2006
- considers the SENSITIVE security classification, aggregation of disparate sources of information and the impacts to privacy of that classification
- uses controls deliberately aligned with the Ministry's security risk assessment process to ensure ongoing management of risk and monitoring of controls.

3.1 Review of previous findings

The IPP analysis and risk assessment from the PIA's listed above have been reviewed in detail to ensure that the previous recommendations are reflected in the current service design. Almost all of the recommended controls (116 of 128) are being implemented as part of the current Te Rito service. See Appendix C for a summary analysis, and the supplement to Appendix C for full comparative traceability.

3.2 DPUP

The Ministry has adopted and is in the process of implementing the Data Protection and Use Policy (DPUP) developed by the Social Wellbeing agency. The principles of the DPUP have also been considered in this assessment where appropriate.

3.3 Sources of information

To complete this PIA, information has been collected and reviewed from the previous Te Rito PIAs, the Te Rito project team, Ministry Privacy, and Information Management specialists, Ngā Rau Whakatupu, and the Te Rito vendor (Edsby) to ensure accuracy. Advice has also been provided by external stakeholders including the Office of the Privacy Commissioner (OPC) and the Government Chief Privacy Officer (GCPO). This assessment has been completed on the most current documentation and information available.

3.4 Additional analysis and assurance

Beyond the analysis against the 13 Information Privacy Principles, this PIA has also considered independent Privacy analysis and assurance of Edsby from the US Common Sense Privacy programme. Edsby has been successfully assessed by the Safer Technology for Schools (ST4S) programme used in Australia and New Zealand. Self-assessment of Te Rito against the UK ICO's Age Appropriate Design Code (AADC) has been performed. This additional assurance is presented in section 5.14 on page 55.

[2] Refer to the OPC's PIA Toolkit for more information - Office of the Privacy Commissioner | Privacy Impact Assessment Toolkit

Proactively released

4 Summary of findings

4.1 Summary of privacy risks

A total of eighteen (18) privacy risks were identified through the PIA. These are described in Table 1 below. One of the medium rated risks (P-04) is specific to schools, rather than Te Rito.

Nine risks from previous PIAs were medium-level risks after implementation of recommended controls. Of these nine:

- four risks continue to be assessed as medium-level in this PIA (one relates to P-04, three relate to P-03)
- five risks previously rated as medium risks are low risk after the mitigations in this PIA.

Further elaboration of the prior PIA's, their risks and recommendations is provided in Appendix C - Previous PIA risks, privacy responses, and recommended controls on page 89.

The overall assessment of risk in this PIA is consistent with the Ministry's *Enterprise Risk Management Frameworks* Receptiveness to risk in the 'Strategy Design and Delivery', 'Service Design', and 'IT Functionality' categories. The level of preventative controls in place is consistent with being averse to risk in the 'IT Security' category.

The previous version of the Ministry's risk framework had a category for 'Trust and Confidence'. The work of the Te Rito team with Ngā Rau Whakatupu on governance, design and deployment is consistent with the cautious appetite for risk in this previous category.

Analysis against the UK ICO's Age Appropriate Design Code (AADC) shown in Table 15 on page 70 identified no additional privacy risks.

The residual level of privacy risk is consistent with an overall aversion to risk for Te Rito.

Table 1: Summary of privacy risks

Initial risk rating	Risk description	Residual risk rating after controls
High	**P-11** Te Rito may retain personal information for longer than operationally necessary. Increased exposure and impact from a breach.	Medium
Medium	**P-04** Schools have ineffective or insufficient safeguards to protect kaimahi credentials or ensure the integrity of data stored in SMSs. Data in Te Rito is compromised as a result.	Medium
	P-03 Personal Information is exposed to an unauthorised third party. This is due to the Te Rito solution not implementing effective or sufficient safeguards to ensure the security of PI. PI is disclosed, the Privacy of multiple individuals is breached with potential to cause serious harm.	Medium
	P-15 Schools may be sharing personal information to other schools which is outside of the specified purpose for which it was collected. Schools may not identify on enrolment forms that information will be shared with a student's next school, or consent to do so is not sought. Te Rito facilitates this.	Low
	P-10 A school pre-enrols student|ākonga in their SMS, resulting in the principal or administrator for that school being able to see additional information in Te Rito about a student who is not currently attending the school.	Low
	P-14 Kaimahi authorised to access Te Rito, uses or discloses (inadvertently or deliberately) sensitive personal information that is inappropriate with the potential for serious harm.	Low

Proactively released

Initial risk rating	Risk description	Residual risk rating after controls
	P-02 Schools are insufficiently transparent with students or parents about their use of Te Rito to collect and share personal information, whether at point of enrolment or at point of opting into Te Rito.	Low
	P-08 An authorised user of Te Rito accesses, uses or discloses personal information that is inappropriate or outside identified purposes.	Low
	P-07 A technical fault in Te Rito leads to an authorised user being able to see personal information that they have no purpose to see.	Low
	P-13 Scope, function, or purpose creep in Te Rito may lead to new Privacy risks not being identified and mitigated. Including schools or other Governance stakeholders not being aware of changes in progress.	Low
	P-09 An individual is able to be identified from a number of aggregated or anonymised data sets, or through unique identifier such as their National Student Number (NSN).	Low
	P-01 Excessive items of personal information are collected for no clear purpose.	Low
	P-18 The Capture app is used to upload photos, audio, and/or video of young children to Te Rito. Young children lack the capacity to genuinely consent to this or comprehend the implications of their likeness being captured and stored in Te Rito. A Privacy complaint may arise over reasonableness, or meaningful consent.	Low
Low	**P-05** Requests for access or correction are not adequately processed by schools, or Statements of Correction made visible in Te Rito.	Low
	P-12 Students or parents may not understand the use and purpose for collection and storage of information in Te Rito, this results in a privacy complaint.	Low
	P-17 A student is unable to exercise their Privacy rights given the mandatory nature of school enrolment and attendance, and the school being a custodian of student information. A Privacy complaint may arise over issues such as purpose, meaningful consent, opt-in, scope of data held.	Low
	P-06 Personal information is used or disclosed outside of the specified purpose for which it was collected and stored in Te Rito. Specifically, Ministry staff access Te Rito to obtain information not otherwise accessible to the Ministry.	Low
	P-16 A student uses Te Rito to publish to a school wide group personal information about another student without permission or content that is not age appropriate.	Low

The Ministry will use its existing security risk monitoring and tracking tool, SimpleRisk, to manage the privacy risks, evaluate the effectiveness of existing controls, and continue to monitor the implementation and effectiveness of all controls. This will ensure that the privacy risks identified in this PIA are managed by the same processes that manage Ministry security risks.

The effectiveness of privacy controls and resultant risk levels will be reviewed and updated through discovery work with different schools. Through this process, additional controls may be required, and some controls may be determined to be unnecessary.

Proactively released

4.2 Summary of privacy enhancing controls

A total of twenty-eight (28) privacy enhancing controls specific to Te Rito were identified as either being currently in place, or as work in progress that are due for completion before national onboarding activity (these are highlighted in orange). These controls reduce either the likelihood or the impact of the identified privacy risks. The 'control reference' numbers are from the Ministry's Information Security Controls Catalogue. The relevant IPP numbers refer to the Privacy Act's Information Privacy Principles.

Table 2: Privacy enhancing controls

Control Reference	Control Description	Linked Risks	Relevant IPPs
PRI-01.6	Privacy by design including data minimisation, transparency, user centric thinking.	All risks	All IPPs
PRI-02	The Privacy statement applicable to Te Rito is publicly published, in plain language, in Te Reo, is summarised for students, and an age-appropriate format for students aged under 12 will be developed. Te Rito T&Cs for adults are in plain language, publicly published and an age appropriate acceptable use guidelines have been written for students.	All risks	All IPPs
PRI-08	OPC's PrivacyABCs for Schools is available as privacy training for all school Kaimahi. Privacy touch points are included in overall Te Rito user training guides.	All risks	All IPPs
DCH-22	Automatic Data Quality and Validation checking is performed by Te Rito during data ingestion	P-04, P-10	5, 11
GOV-01	Compliance requirements – Ministry information security and Privacy requirements and recommendations are articulated to other parties. In some cases are embedded in contracts (**TPM-08** SLAs and Contracts).	P-03, P-13	4, 5, 10
GOV-03	Te Rito Data Kaitiakitanga Group provide assurance over access to and use of Te Rito data. Ethics review process will be defined.	P-03, P-06, P-13, P-17	4, 5, 10, 11
GOV-05.2	Operational and business reporting of key risk indicators.	P-03, P-06, P-07, P-08, P-10,P-11, P-13	1, 4, 5, 9, 10, 11
HRS-03	A comprehensive *Engagement and Communications Plan* has been implemented to ensure that all stakeholders are informed about Te Rito deployment and use.	P-01, P-02,P-05, P-06, P-12, P-15,P-17, P-18	1, 3, 4, 6, 7, 10
HRS-09.4	Te Rito automated deprovisioning of kaimahi access based on SMS update	P-03, P-10, P-11, P-14	5, 9, 10, 11
IAC-07	Formal user registration and de-registration process that governs the assignment of access rights.	P-03, P-04	5
IAC-08	Role Based Access Control – All access to Te Rito (kaimahi, students) is managed by RBAC.	P-03, P-06, P-07, P-08, P-10, P-11, P-14	1, 4, 5, 9, 10, 11, 13
IAC-13	Alternative methods of authentication under specific circumstances for young children.	P-08	10, 11
IAC-15.8	Student Usage Guidelines for Te Rito have been defined for students. They are made available for schools to use as appropriate.	P-03, P-08, P-16, P-18	1, 4, 5, 10, 11

Proactively released

Control Reference	Control Description	Linked Risks	Relevant IPPs
IAC-17	Periodic review of the privileges assigned to users to validate the need for such privileges; and reassign or remove privileges, if necessary, to correctly reflect school business needs.	P-03, P-06, P-07, P-14	1, 4, 5, 10, 11
IAC-20	Principle of 'least privilege' is enforced by RBAC and linking of student records to their current school and teachers	P-03, P-04,P-08, P-10, P-14, P-17	5, 10, 11
IAC-22	ESL enforces a limit for consecutive invalid login attempts by a user and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	P-03, P-04	5
IAC-24	Session lock initiated after a period of inactivity, or on receiving a request from a user and retain the session lock until the user re-establishes access using established identification and authentication methods.	P-03, P-14	5, 10, 11
IAC-25	Automated mechanisms exist to log out users at the end of the session or after a defined period of inactivity.	P-03, P-14	5
PRI-01.2 & PRI-01.3	Te Rito specific engagement and communications is made publicly available through multiple channels for students and parents. Clarifying Te Rito information use, purpose and storage.	P-12, P-13,P-15, P-17, P-18	3, 4, 10, 11
PRI-03	Guidance will be documented and communicated for schools to review enrolment forms and privacy statements for specific requirements	P-01, P-02,P-10, P-12, P-15,P-17, P-18	1, 3, 4, 10, 11
PRI-03.1	Completed: Te Rito will record 'consent to share' with next school	P-02, P-08, P-10, P-15, P-17	1, 3, 10, 11
PRI-04	Existing school business processes address collection of information about young children from parents with parental consent.	P-01, P-02,P-15, P-17, P-18	1, 3, 10, 11
PRI-06	Personal information permission – students & school staff have access to review some information stored about them in Te Rito.	P-01, P-12	1, 3, 4, 10
PRI-06	Access to Information – process to be defined for Right of Access to data in Te Rito post-school.	P-05	6, 7, 8
PRI-08	Te Rito specific Privacy training is available.	P-03, P-06, P-07, P-08	1, 3, 4, 5, 6, 7, 8, 10, 11
PRI-08	Role Based Access Control (RBAC) testing is conducted	P-03, P-07	5, 11
PRI-10	Guidelines issued to ensure the quality, utility, objectivity, integrity, and de-identification of Personal Information.	P-01, P-03, P-09, P-11, P-13	1, 4, 5, 9, 10, 11, 13
PRI-14	Privacy-related audit records. Privacy related reporting to internal senior management, as well as external oversight bodies as appropriate, demonstrating accountability with privacy requirements.	P-13	4, 10
SEA-09	Input Validation. Automated processes validate information output from SMS sync to ensure that the information is consistent with the expected content.	P-01, P-03,P-04, P-08, P-10,P-11, P-13, P-14	1, 4, 5, 9, 10, 11
Additional controls identified not directly related to Te Rito			

Proactively released

Control Reference	Control Description	Linked Risks	Relevant IPPs
HRS-03	Advice and guidance are provided to school Boards and kaimahi about their responsibilities for Privacy and Security of school information and systems.	All risks	All IPPs
PRI-01 & PRI-02	Schools have existing privacy policies; these may need updating in line with the purpose for storing info in Te Rito. Completed: A sample of enrolment forms and privacy policies of 700+ schools has been reviewed to assess whether further guidance from the Ministry to schools may be needed.	All risks	All IPPs
PRM-01	In the Ministry's overall digital strategy are several initiatives to help schools with their cyber security including Te Mana Tūhono, Cyber Security and Digital Support for Kura and Schools programme (CSDS), Network for Learning (N4L), Safer Technology for Schools (ST4S).	All risks	All IPPs
IAC-15	User Account Lifecycle Management – the Cyber Security and Digital Support for Kura and Schools programme is undertaking work to document guideline recommendations for schools	P-03	5
PRI-01.5	The ETA identifies specified users and specified purposes for use of the NSN, with an offenses provision defined.	P-09	10, 11, 13

A further twenty-eight (28) controls specific to Te Rito were identified as either being currently in place or as work in progress due for completion before national onboarding activity (these are highlighted in orange). These additional security controls in Table 3 below reduce the likelihood or impact of identified risks. There are also 4 controls that are not specific to Te Rito included at the bottom of the list.

Table 3: Additional security controls

Control Reference	Control Description	Linked Risks	Relevant IPP
GOV-01	Compliance requirements – inc. Certification and Accreditation (C&A) of the Te Rito solution and end to end service.	All risks	All IPPs
GOV-03	Information security & privacy reviews – Perform a risk assessment, in concert with major changes of scope, solution capability.	All risks	All IPPs
GOV-03	Privacy control and risk review – Evaluation and discovery work with schools will provide feedback to confirm which controls are effective or ineffective, updating the risk level. Identification of new effective controls.	All risks	All IPPs
GOV-03	Periodic reviews – The Te Rito project will engage an independent auditor to perform project IQA.	All risks	All IPPs
GOV-03	Information security reviews – The Ministry reviews Edsby assurance documentation and will assess the reliance of assurance that can be placed on the Edsby evidence.	All risks	All IPPs
IAO-05 & PRI-14	Operational Assurance Plan. In concert with the assurance requirements identified of supporting or integrated services, the Ministry will agree a formal assurance plan covering the end-to-end Te Rito service.	All risks	All IPPs

Proactively released

Control Reference	Control Description	Linked Risks	Relevant IPP
PRI-01 & PRI-02	Information security and Privacy policies – Existing Ministry and Edsby information security and privacy policies, practices, processes, education and awareness training, applicable for all staff involved in the design, operation, and management of the end-to-end service.	All risks	All IPPs
VPM-07	Security testing – Perform security testing, remediate findings to an acceptable risk level.	All risks	All IPPs
CHG-02	Configuration management – integral with change control are technical configurations implemented to prevent sharing, export or download of PI except where appropriate and managed by RBAC.	P-03, P-08, P-09, P-14	5, 10, 11, 13
CPL-01	Due Diligence – Ministry expectations for Assurance reporting to be articulated and a framework established to enable reporting. Including RACI matrix to clarify shared responsibility obligations.	P-03	5
CPL-01	Service Agreement between schools, the Ministry, Edsby.	P-03, P-04, P-08, P-10, P-14, P-15	3, 5, 10, 11
CRY-03	Transport Layer Security – all data is encrypted in transit from external connections to Te Rito.	P-03	5
CRY-05	Storage data security – all information and data are encrypted at rest and in storage.	P-03	5
IAC-02	Central Authentication, Authorisation of Te Rito users and processes acting on behalf of organizational users.	P-03	5
IAC-03	Central Authentication, Authorisation of third party users and processes accessing Te Rito.	P-03	5
IAC-10.1 & 10.4	Password complexity requirements	P-03	5
IAC-11	Error messages during authentication provide minimally useful feedback	P-03	5
IAC-15 & 15.8	Terms & Conditions of use for Te Rito are enforced for staff (ESL) users. Including Professional Code of Conduct obligations.	P-03, P-06, P-07, P-08, P-09, P-10, P-14	1, 4, 5, 10, 11, 13
IAC-18	ESL requires users to follow accepted practices in the use of authentication mechanisms.	P-03	5
IRO-04	Sector facing cyber and privacy Incident Response Plan (IRP).	P-03, P-04, P-07, P-08, P-11, P-14	5, 9, 10, 11, 13
IRO-10	Process exists to report incidents to applicable: Internal stakeholders; Affected schools; Governance bodies; and Regulatory authorities.	P-03, P-04, P-08, P-09, P-14	5, 10, 11, 13
MON-01.12	Automated mechanisms exist to alert incident response personnel of inappropriate or unusual activities that have security incident implications.	P-03	5
MON-02	Logging and Auditing – Te Rito has full logging of all system and user events. Logs automatically feed in to monitoring and alerting tools.	P-03, P-04, P-06, P-08, P-11, P-14	1, 4, 5, 9, 10, 11

Proactively released

Control Reference	Control Description	Linked Risks	Relevant IPP
MON-02.3	System monitoring and alerting – Te Rito is monitored, and alerts generated using existing tools.	P-03, P-06	1, 4, 5, 10, 11
MON-02.3	Security Incident and Event Management (SIEM) – in addition to creation of anomaly reporting criteria in monitoring tools. Work in progress: Ministry SIEM solution will receive alerts.	P-03	5
NET-04	Firewalls inc data flow access control lists	P-03	5
NET-08	Network Intrusion detection	P-03	5
OPS-03	Service Management RACI & SoPs to be established.	P-03	5
Additional controls not directly related to Te Rito			
IRO-04	Incident response plan – Ministry incident response plans cater for information security and privacy incidents, including escalation, communications, notification to effected parties.	All risks	All IPPs
IAC-28	Staff (ESL) users are required to provide Evidence of Identity (EoI) for ESL account setup. Staff are also required to perform Identity Verification in the workforce safety checks under the Childrens' Act.	P-03	5
SAT-02	Security awareness training – the Ministry's Cyber Security and Digital Support for Kura and Schools programme (CSDS) has a specific workstream for awareness raising in the education sector.	P-04, P-06, P-07, P-08, P-15	3, 4, 5, 10, 11, 13
SAT-02	There is extensive engagement in the education sector from NZ organisations such as Netsafe, NZ Police, OPC, CERT NZ on basic cyber security and privacy awareness applicable to children.	P-04	5

Proactively released

4.3 Recommended additional privacy enhancing controls

Through the PIA, additional controls were identified that are currently being implemented. In Table 2 and Table 3 above a few controls are identified that are currently work in progress and will be in place before national onboarding of users takes place.

Five (5) additional controls are recommended shown in Table 4. These will need investigation and elaboration in greater detail to determine their likely effectiveness in further reducing the privacy risks identified. They do not have a committed plan to implement before national onboarding commences and are therefore not considered in the assessment of residual risk. The Te Rito project is committed to investigating and evaluating these recommended controls.

Table 4: Recommended additional controls

Control Reference	Control Description	Linked Risks	Relevant IPP
IAC-06	Multi Factor Authentication (MFA) – All ESL users with access to student information should be required to use MFA.	P-03, P-04	5
PRI-05	Retention requirements – agree an approach to retaining PI in a 'lifelong learning' context. Implement differing retention periods.	P-01, P-11, P-18	1, 9

Control Reference	Control Description	Linked Risks	Relevant IPP
PRI-05.2	Need to consider whether a two stage access model (request, confirm) can be implemented.	P-03, P-08, P-10, P-14, P-15, P-17	1, 3, 5, 10, 11
PRI-05.7	Define and implement data handling and protection requirements for specific categories of sensitive Personal Information.	P-09, P-11, P-12, P-14, P-15, P-17	3, 4, 9, 10, 11, 13
PRI-09	Schools to perform privacy brief analysis focused on the use of Te Rito. (Tangentially related to P-01, P-16)	P-02, P-08, P-10, P-12, P-14, P-15, P-17, P-18	1, 2, 3, 5, 10, 11

- **IAC-06** multifactor authentication is dependent on ESL implementing the required capability.
- **PRI-05** retention of data in Te Rito potentially beyond a student's mandatory education, is subject to further consideration with Archives NZ and the agreement of a disposal authority or schedule specific for Te Rito.
- **PRI-05** also needs to consider the ability to implement differing retention periods for different types of information, particularly for more sensitive or time limited information.
- **PRI-05.2** being a two stage or confirmation process for a new school to access a student's Te Rito record. This is implemented in the Ministry's existing SRTS. For Te Rito this functionality may rely upon information in ENROL to enable additional data quality checking and act as enforcement point. Or it could be implemented with a consent field in Te Rito with business logic then determining school access.
- **PRI-05.7** relating to the handling and retention of more sensitive information is part of the discussion with Archives. In addition, more detailed analysis may be required to gain assurance of school information collection practices and subsequent storage of information in SMSs and Te Rito. Specifically related to Health and Medical information, in alignment with the Health Information Privacy Code (HIPC).
- **PRI-09** Privacy good practice recommends that schools perform their own (brief) privacy analysis on the use of Te Rito. Potentially including considerations as they relate to Te Rito for Collection, Use, Purpose, and Sharing as articulated on enrolment forms or in Privacy Statements.

All recommendations and associated activities from the PIA are tracked by the Te Rito project team through Jira.

Following distribution of a final draft of this PIA, three actions have been completed. The Te Rito Incident Response Plan, a programme IQA, and the implementation of a consent field within Te Rito for sharing student information to the next school. In addition analysis has taken place of a representative sample of 700+ schools (~28%), their enrolment forms and privacy statements. This has resulted in risk P-15 being mitigated to Low based on available evidence.

Proactively released

5 Assessment part 1 – Te Rito system information

5.1 Key stakeholders

Business Owner (Risk)	Stuart Wakefield, Chief Digital Officer, Ministry of Education
Project Owner (System)	Craig Haywood, Manager, Sector Products & Services Mark Brumby, Te Rito Programme Manager
Other Stakeholders and Service Providers	Te Rau Whakatupu Māori and Auraki (collectively referred to as Ngā Rau Whakatupu), sector working groups for Māori & English medium, including the main education sector peak bodies[3] Te Rito Data Kaitiakitanga Group (Data Stewardship group), Te Uru Puia (Te Rito Steering Committee), Schools, Students, Parents, OPC, GCPO, Edsby

5.2 Te Rito overview

Te Rito is guided by a whakatauāki gifted to the programme by Te Rau Whakatupu Māori:

"Me tiaki te mana o te tamaiti me tōna whānau – Protect the mana of the child and their family"

Te Rito is a national information-sharing platform that enables information about ākonga and students to follow them in a secure and accessible manner throughout their education – Te Rito's purpose. Te Rito offers a range of features to support teaching, learning, parent and whānau engagement, and classroom administration. Use of Te Rito will be in the best interests of ākonga and students, to support the objectives and benefits elaborated on the following page. Te Rito is being co-designed, co-governed and co-delivered with the education sector via two sector working groups, Te Rau Whakatupu Māori and Auraki. Working group members speak highly of the level of trust and collaboration with the Ministry as they work together to deliver Te Rito in the best interests of ākonga and students.

Authorised users of Te Rito can access and use student's education-related information from one place. This ensures that when a student moves to a new school, their educational records are available to that new school. This is particularly important for transient students and students who have support needs, as it ensures the new school has the information available to minimise any delay in providing continued support. Te Rito will ensure that a school has the most accurate and up to date information about the student across multiple sources of information.

The clear vision for Te Rito is that the student's record is owned by the student, with the Ministry and their school a custodian of the information. Access is then based on the student's enrolment status with a school. As the Ministry has the contractual relationship with Edsby, the Ministry is responsible for ensuring that Te Rito is managed and operated in a safe and secure manner. The Ministry is ultimately accountable for providing Te Rito to schools and all users.

The Te Rito Early Stage Rollout (ESR) is already used by thirty three (33) ECE's and thirty six (36) schools. Four PIA's have previously considered both the ESR and LSR. The Te Rito deployment in 2024 will be a progressive rollout for additional groups of schools, users, and functionalities. Initial access to Te Rito is for school principals (including deans, deputy principals or others who hold delegated roles such as the school administrator or manager) and teachers. Students and other kaimahi will gain access as decided by their schools. A pilot group of students from Ko Taku Reo|Deaf Education NZ started in 2024. Parents and whānau will gain access later. There is more information about Te Rito on the website here.

[3] NZAIMS, NZEI, NZPF, NZPPA, NZRASLA, PPTA, SEPANZ, SPANZ, and Te Akatea.

Proactively released

5.2.1 Te Rito objectives and benefits

An overview of the problems, objectives, and benefits of Te Rito is summarised below:

"The New Zealand education data ecosystem is characterised by three problems:

1. *Access: Learners, whānau, educators, providers and government do not have access to information when and how they need it to make the best decisions.*
2. *Collection: Data gathering and entry is labour intensive, error prone and often duplicated, leading to gaps in data, poor quality data and high costs for education providers and government.*
3. *Use: Low skill levels and awareness, few incentives and cultural resistance are leading to lower use of information than desired*."

"Key stakeholders identified four main investment objectives…:

1. *Children and young people, their whānau, teachers, education providers and government have better information to support children and young people to fulfil their learning potential.*
2. *Robust high quality data on all children and young people in the education system is available alongside a view of how they access education services.*
3. *Quality information is sufficient to enable effective and timely policy and investment decision making to best support teaching and learning.*
4. *The administrative burden is lower for everyone who uses the system*."

These investment objectives were supported with the following rationale:

"Investment rationale

- *Learner information does not follow learners as they progress through the education system.*
- *No commonly agreed interoperability standards used by education providers [or their vendors].*
- *Data resilience is variable across the sector with no common system to provide back-up.*
- *There is no secure, common system to enable education providers to share education content and data. This makes it difficult to collaborate safely.*
- *No common platform to implement tools and systems to support teaching and learning (e.g. learning support and the proposed Record of Learning)."*

"Benefits

- *Increased use of student information by teachers to improve their practice and make evidence-based decisions affecting learning.*
- *Increased learner information available to schools and kura enabling more timely support.*
- *Students records travel with them as they transition school to school. Transient children are identified quickly, and information is passed to support them – targeted deployment.*
- *Reduced administrative burden for schools and kura.*
- *Trends for individual learners and cohorts such as Kāhui Ako can be tracked.*
- *Increased amount of quality information about learners is available to parents, learners, schools, and education agencies in a more timely and complete manner.*
- *Reduction in cost to manage information at schools.*
- *Data Quality"*

"[Te Rito] will create a national repository of learner data that will allow a child or young person's information to be available wherever they are enrolled, and is added to in real time by education providers to create a learning record. This will:

- *make it possible for learner information to be accessed in a secure way by children and young people, education providers, and parents, and to be shared with education agencies, under the appropriate permissions*

Proactively released

- *allow a child or young person's unique education record to be available to them throughout their education journey. It will make it possible for children and young people, including those with learning support needs, to be provided with more timely and targeted support over time".*

"Our tamariki are our taonga and the information collected and held about them is also taonga. It is critically important to protect the privacy and security of our learners' information whilst ensuring that the right people have access to it, for the right purpose, at the right time."

5.2.2 Te Rito data guardianship

As Te Rito is implemented, a data guardianship or stewardship function is required. The Te Rito Data Kaitiakitanga Group comprises a range of stakeholders from Ngā Rau Whakatupu and the Ministry, who will advise on how Te Rito data is accessed or used. The role of the Te Rito Data Kaitiakitanga Group in providing advice to schools and kura, and a continuing role overseeing the appropriate access to and use of Te Rito, is being developed as part of the Terms of Reference.

The draft Terms of Reference for the Te Rito Data Kaitiakitanga Group provides a more privacy / data-centric view aligned with the objectives and benefits for Te Rito:

"*Te Rito will enable data held in SMSs to be exchanged with a national learner repository so that the information is available to support the learner/ākonga, their whānau, and educators. Te Rito will improve the quality of data used to improve learning outcomes.*

Te Rito has the potential to bring considerable benefits to children, young people and teachers by:

- *protecting learner and ākonga information from cyber-attack and privacy breaches*
- *improving the transfer of learner and ākonga information between kura and schools so they have access to that information from day one*
- *reducing the need for teachers to reassess newly enrolled learners and ākonga*
- *providing more timely information to support learners/ākonga with additional learning needs*
- *storing information securely and making it more accessible to those who have the appropriate permissions*
- *supporting collaboration and improving the flow of information within and between kura and schools."*

The purpose, scope and mandate of Te Rito Data Kaitiakitanga Group is aligned to the principles of the Toi Hou Tangata Social Wellbeing Agency's Data Protection and Use Policy (DPUP). In DPUP, the principle of kaitiakitanga is to work as a guardian and steward of information, ensuring that it is protected and kept safe, and can be used and shared to add value in ways that are inclusive and transparent. As the Te Rito Data Kaitiakitanga Group will represent the interests of multiple stakeholders, any authority to agree or approve access to information (e.g. for research purposes) on behalf of students and schools will need to be established.

The Te Rito Data Kaitiakitanga Group have already agreed that any research request to access aggregate information in Te Rito will only be considered for anonymous information which cannot be identified to an individual student, or small cohort of students. Where identifiable information is requested, this would be an OIA request for each individual school to handle. How requests are assessed will need careful consideration, especially to ensure that the research objectives are not detrimental to students. A process similar to the Ministry's Ethics review process will likely be developed.

Proactively released

5.3 Te Rito scope

5.3.1 Scope introduction

The scope of this PIA is the full national rollout of Te Rito, data stored in Te Rito and accessed by the education sector workforce (kaimahi) at New Zealand schools and kura, along with a pilot of student access ahead of a national rollout to students. A national rollout will take a number of years. Different approaches to deployment will be evaluated with small groups of schools, reflecting differing needs and priorities for different regions, types of schools, and special cases.

This PIA is deliberately wide, covering the different types of information that have been identified by Ngā Rau Whakatupu as necessary information to help student's education, especially during changes of school or teacher. Not all the identified information will be stored in Te Rito immediately from all schools for all students.

Beyond the practicality of working with SMS vendors and groups of schools to map data fields to equivalent Te Rito data fields, subsequent discovery and evaluation work using data in Te Rito will be required to qualify and consider whether the identified information is useful, necessary, and beneficial. By necessity this work can only be done with schools using real information about students to confirm the anticipated benefits. We anticipate that Ngā Rau Whakatupu and the Te Rito Data Kaitiakitanga Group would review the outcomes of evaluation work and could recommend that Te Rito discontinues storing information that was not found to be useful. This meets the criteria defined by OPC for a proportionality test.

Similarly, all of the potential uses of information relating to educational delivery are not known at this time. Schools may use Te Rito for education purposes related to sports lessons, or official school sports teams, or opt-in sports groups outside of school hours. These are all school activities.

Te Rito currently only stores basic biographic, attendance, enrolment, and limited assessment information about students. Through the discovery and evaluation work *some* schools will start storing in Te Rito *some* of the information identified in the following sections. Successful scenarios will likely lead to more groups of schools following the same approach.

In brief the data scope comprises:

- student data, school years 1-13, normally ages 5–18
- adult students and learning support students, aged 19 or older
- school staff data, primarily principals and teachers, potentially all kaimahi
- parent data, primarily in the context of a student contact relationship
- data primarily from SMSs, additional data will come from other Ministry systems such as ENROL.

A high-level summary of the student data in scope is shown in Figure 4 on page 30. Student, parent, and kaimahi data in Te Rito is elaborated in the section on Information types starting on page 36. All attributes stored including all data about users is detailed in Appendix E - Te Rito All data attributes on page 92.

With all planned activity there is associated assurance work, including this PIA. As part of the Ministry's Certification & Accreditation (C&A) process Edsby has been successfully assessed by Safer Technology for Schools (ST4S). Assurance documentation has been received from Edsby for their ISO27001 Certification and the results of the Common Sense Privacy program evaluation. Review of third-party assurance is discussed later in the section on Additional analysis and assurance on page 55.

This PIA does not address the anticipated future changes for Te Rito identified on page 28; any such changes would require further privacy assessment prior to implementation. It also does not consider information about the school (e.g., physical address, year levels taught) as that is publicly available information and not personal information.

Proactively released

5.3.2 Te Rito current scope

Te Rito is provided as a service by Edsby, who host Te Rito in Microsoft's Azure data centres in Australia. Data is primarily sourced from Student Management Systems (SMSs) operated and managed by individual schools. Additional data is sourced from a variety of Ministry systems including ENROL, Pourato, e-asTTle and other assessment tools.

Access to Te Rito is authenticated by the existing Education Sector Logon (ESL) service that is already used by staff at all schools. A student access pilot is being performed with Ko Taku Reo|Deaf Education NZ. This will authenticate students with the Identity Provider (IdP) that their school uses, typically Microsoft 365 for Education or Google Workspace for Education.

Te Rito does not include any built-in functionality that does analysis of historical data to make predictions about future outcomes. E.g. A student's past assessment results to predict future assessment results or NCEA achievements.

The scope of Te Rito centres on the progressive national roll-out of the Te Rito service, which supports a range of value streams. The current deployment shown in Figure 1 below includes:

- access for principals, teachers, and other specialist roles at existing ESR schools
- access for principals, teachers, and other specialist roles at Ko Taku Reo (KTR)
- core Te Rito functions referred to as Teacher Collaboration and Student Panorama
- integration with three SMSs (Edge, eTAP, KAMAR) to receive basic biographical information, Assessment and Attendance/Enrolment data
- integration with the Ministry's Funding Information Regulatory System Technology (FIRST) application, to obtain organisational only information. No funding data would be used.
- A Data Analysis ESR which enables data held in multiple existing SMS systems used by the schools in a Kāhui Ako to be displayed in Te Rito for business intelligence and data analysis
- A standardised Learning Support Register (sLSR), only available to existing ESR schools and Early Childhood Education (ECE) providers. The sLSR is outside of the scope of this PIA, though does benefit from the controls identified in this analysis.

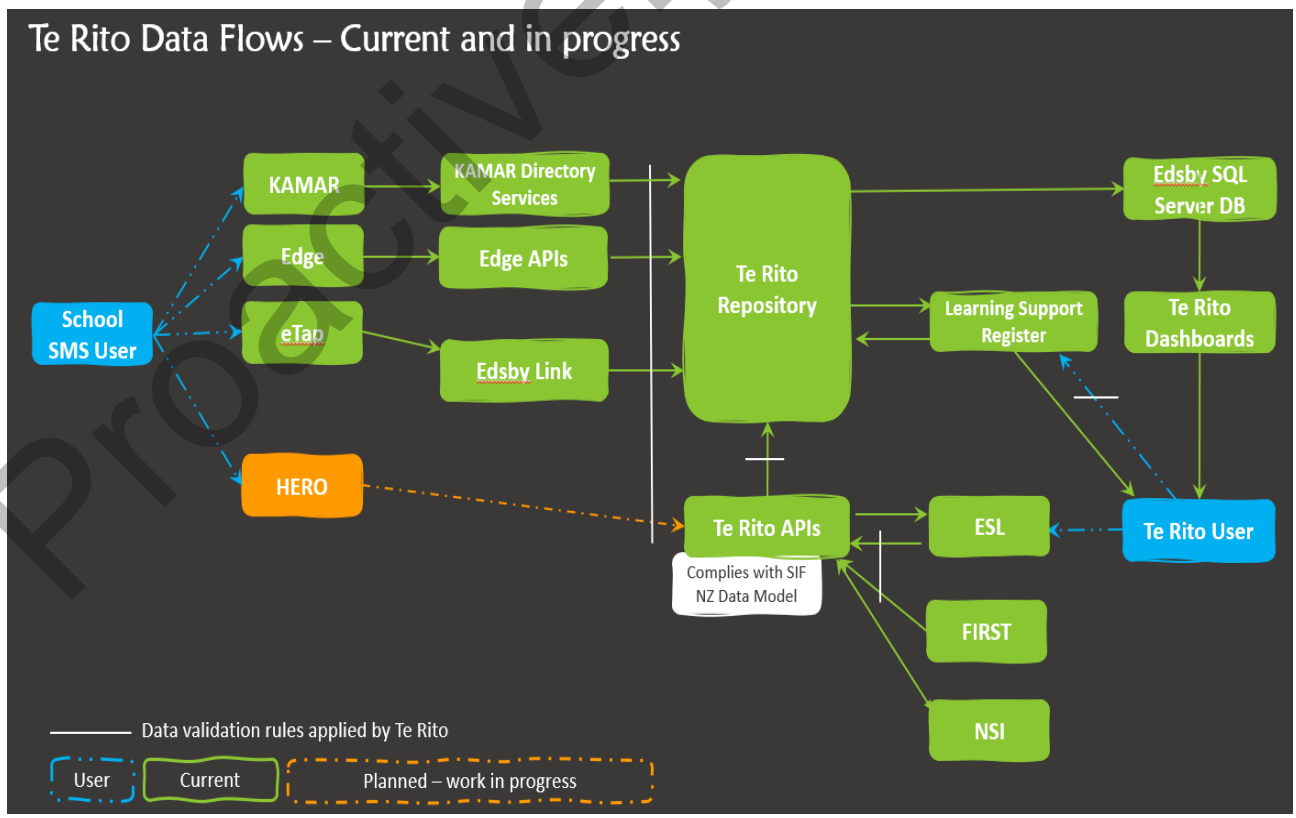


Figure 1 Te Rito current state - including data flows

Proactively released

5.3.3 Te Rito planned scope

The 2023/24 deployment stage includes User Access and Technical Connectivity described below, all in scope of this PIA.

5.3.3.1 User Access

- A planned deployment at a regional level starting with schools and kura from Ngā Rau Whakatupu and their associated Kāhui Ako Cluster schools and kura, progressing to Whangārei and Te Tai Tokerau
- General availability of Te Rito to early adopter schools or kura on an opt-in basis
- Enabling access for principals and teachers to core Te Rito functionality and cross school collaboration groups
- Enabling access for all kaimahi at a school, subject to individual school practices
- Enabling core Te Rito functionality including Community Engagement, Learning Management, Assessment & Reporting, Analytics, Student Well-Being. Plus use of the Edsby & Edsby Capture apps on iOS & Chrome devices (see Figure 2 and Table 5: Edsby functionality mapped to Te Rito Service Roadmap below)
- Enabling access for ~170 Ko Taku Reo (KTR) students for a pilot
- Subject to outcomes from the KTR pilot, opening up access to Te Rito for students and ākonga at schools and kura that choose to enable student access
- Edsby to provide full end user support, including service desk and ticketing functions.

The features and functions at a product level are represented in Table 5 and Figure 2 below. A full description of features and functions is available on the Edsby website Features-Edsby.

Table 5: Edsby functionality mapped to Te Rito Service Roadmap

	Community Engagement	Learning Management	Assessment & Reporting	Analytics	Student Well-Being
2023	• Ministry, CoL & class news • Groups for Clubs & teams • Messaging • Real time notifications	• Content builder • Google G-Drive / Microsoft OneDrive integration • Course modelling • Learning object repositories • LTI support • Import support	• Standards based reporting	• Dynamic drill through dashboard • Role-based delivery • Advanced privacy controls • Enrolment dashboard • Attendance dashboard • Custom dashboards	• Panorama view • Shared observations • Learner support register
2024	• Timetable & calendar	• Blended/Hybrid distance learning • Progress tracking	• Advanced gradebook • Formative assessment • Standards based assessment • Online rubrics • Online quizzes • Schedule conflict checker • Online report card • Question banks online • Content mark-up	• Standardised testing dashboard	• Monitor group • Portfolios • Student alerts
2025	Not in scope of this PIA parent accounts, parent teacher scheduling, parent teacher conference scheduling.				

Proactively released

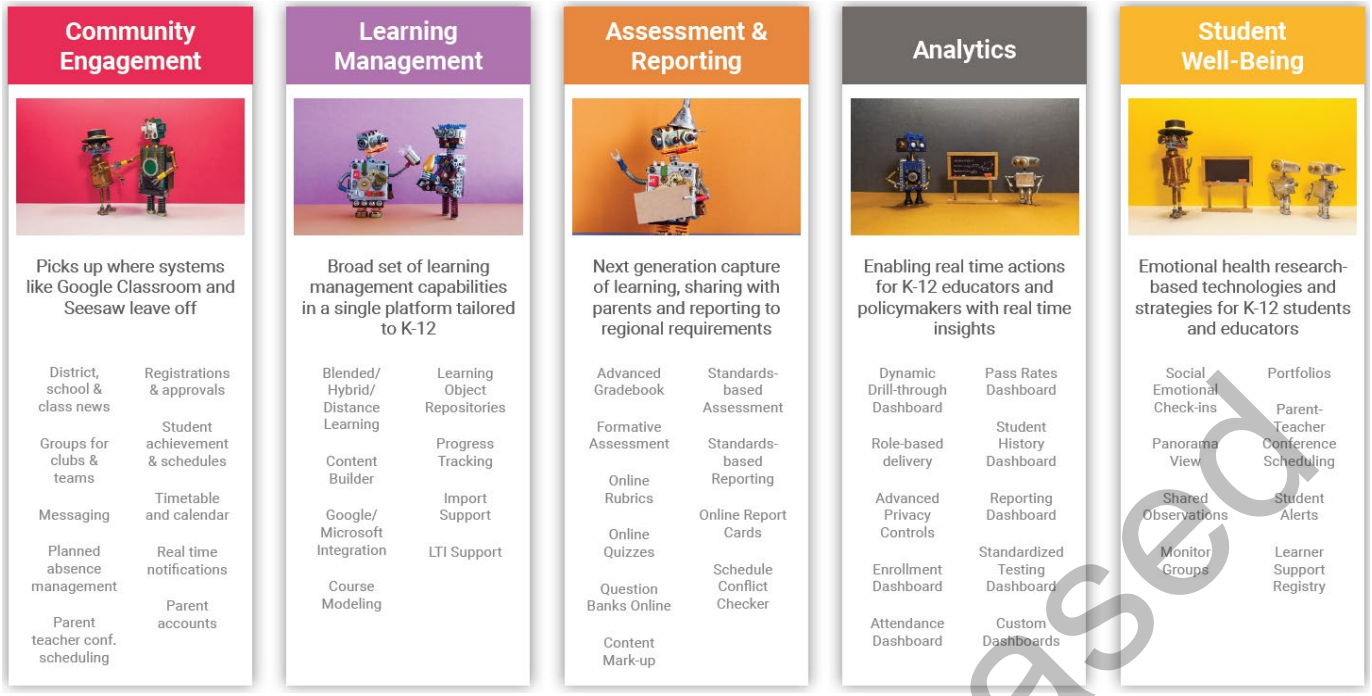


Figure 2: Edsby features & functions

It is not possible to explicitly identify which particular features or functions of the Edsby platform a school may, or may not, use for particular purposes. This PIA therefore considers the general use of the Edsby platform and the data within it for educational & administrative purposes by schools. Schools remain responsible for ensuring that their use of Te Rito is consistent with the Privacy Act.

5.3.3.2 Technical Connectivity

- Connectivity for SMSs to Te Rito and synchronisation of data, ahead of user-focused onboarding and training
- Publishing a Systems Interoperability Framework (SIF) based API for SMS integration, Hero will be the first use case[4]
- Receiving additional data from Student Management Systems (SMSs) and other school sources including additional biographic information relating to Medical conditions, additional assessment & achievement data, attendance/enrolment data, pastoral data[5]. Pastoral data is further sub-divided (for detail see Appendix D and Appendix E) into categories for:
  - positive behaviour & participation including individual plans
  - teacher to teacher transition notes
  - support and interventions, including health needs relating to education
- Integrating with the Ministry's National Student Index (NSI)
- Integrating with and receiving data from the Ministry's Electronic Enrolment Management System (ENROL), Early Learning Information (ELI), Pourato data warehouse
- Integrating with and receiving funding specific data from Ministry systems including English for Speakers of Other Languages (ESOL), Learner Business Data Store (LearnerBDS), Ongoing Resource Scheme (ORS), Resource Teachers of Literacy (RTLit), Specialised School Transport Assistance (SESTA).
- Integrating with and receiving data from assessment tools including Electronic-Assessment Tools for Teaching and Learning (e-asTTle), Progress and Consistency Tool (PaCT), Te Waharoa Ararau (TWA)
- Integrating with NZQA's NCEA Record of Achievement (RoA) or LearnerBDS for NCEA data.

[4] Integration with additional SMSs may include COMPASS, INTEGRATOR, PCSchool, Synergetic

[5] Some pastoral data is already required to be shared by schools with the Ministry

Proactively released

The above scope is represented in Figure 3 below.

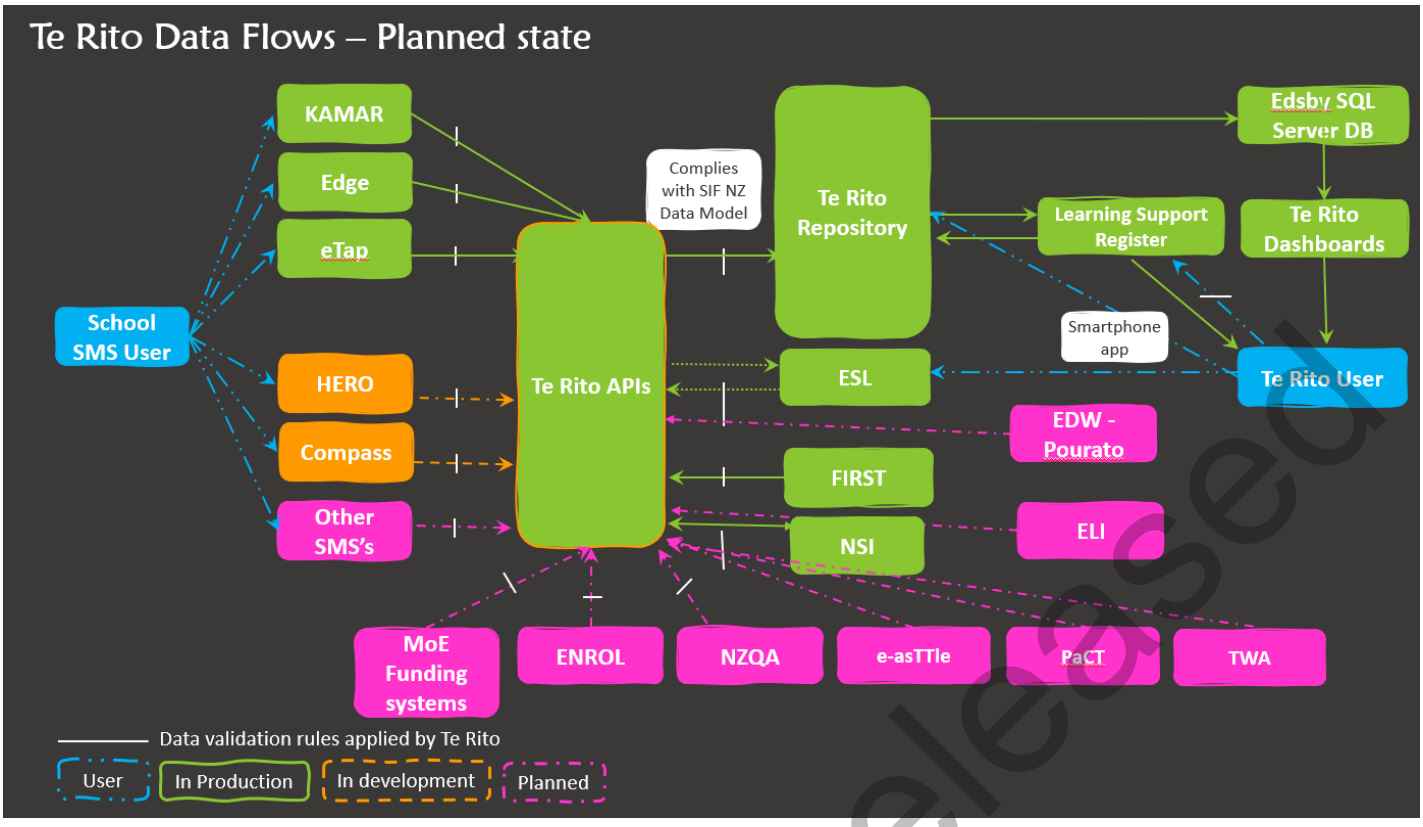


Figure 3: Te Rito planned scope – inc data flows

5.4 Anticipated future changes for Te Rito

Foreseeable changes that are outside the scope of this PIA and would require further privacy and security review include:

- parent access to Te Rito
- members of a school's Board of Trustee's accessing Te Rito
- inclusion of Pastoral: Behavioural Incidents information in Te Rito
- integrating with and receiving data from additional assessment tools including Progressive Achievement Tests (PATs), Supplementary Test of Achievement in Reading (STAR)
- integrating with to receive data from other MoE systems
- extending the deployment of Te Rito to ECE providers beyond the ESR's 33 ECE's
- enabling the sLSR for additional schools beyond the scope of the original ESR – noting that the existing sLSR users and data benefit from all the controls identified in this PIA
- extending Te Rito to include educational data from the Tertiary sector
- A lifelong record of learning data capture and exchange capability, i.e., continued access to Te Rito for students as 'lifelong learners' post-secondary school
- integration with, or receiving data from, other organisations or government agencies, such as Te Whatu Ora for Before School Check (B4SC) information
- any integration that may involve Te Rito sending data outside of the Te Rito solution, e.g., two-way transfer to SMSs.

Some of the above future changes are briefly mentioned in this PIA where it is contextually important to the current analysis. For example, information visibility for parents in the future. Potential changes that are not in plan for Te Rito and would be a major material scope change are:

- any direct use of biometrics by Te Rito
- use of Stand-downs, Suspensions, Exclusions or Expulsions (SSEE) data.

Proactively released

5.5 Te Rito data

The main benefit for students and kaimahi using Te Rito will be as a single access point to student information that is stored in multiple systems. This will help kaimahi ensure that a student's learning needs, progress, approach etc. are known and easily available when there is a change of teacher or school. Te Rito will also improve students' visibility of the information that the Ministry and schools hold about them, currently in disparate systems that students do not have access to.

This PIA is deliberately wide, covering the different types of information that have been identified by Ngā Rau Whakatupu as necessary information to help student's education during changes of school or teacher. Not all the identified information will be stored in Te Rito immediately from all schools for all students.

Discovery and evaluation work will be required to consider and qualify whether the identified information is useful, necessary, and beneficial. By necessity this work can only be done with schools using real information about students to confirm the anticipated benefits. Through the discovery and evaluation work *some* schools will start storing in Te Rito *some* of the information identified in the following sections. Successful scenarios will likely lead to more groups of schools following the same approach. This meets the criteria defined by OPC for a proportionality test.

System and data integration decisions are co-designed, co-governed and co-delivered with the education sector by the Ngā Rau Whakatupu working groups. Priorities for data are decided by Ngā Rau Whakatupu, while the technical integration is agreed and implemented by the Ministry and Edsby.

The full description of data planned to be in Te Rito is included in Appendix E - Te Rito All data attributes on page 92.

5.5.1 Data sources and flow

As the central repository, Te Rito will store and make accessible information:

- received from systems including school SMSs, Ministry systems such as ENROL, and potentially from other agencies in the future
- directly uploaded by students or school staff.

Figure 1 on page 25 provides an overview of current integrations and data sources, with Figure 3 on page 28 providing an overview of planned integrations in scope for this PIA.

The integration with other systems will:

- ensure that the single view of the student presented in Te Rito is accurate and up to date
- improve school staff visibility of student information, without having to access multiple different systems
- reduce the need for school staff to manually transfer information between systems.

Information in Te Rito is already collected or available to school staff through their SMS, other school IT systems, and Ministry systems that schools submit information to. Te Rito does not provide access to any additional information in source systems. Other information in Te Rito is uploaded or saved directly by students and kaimahi, for example portfolio or learning stories.

Kaimahi information within Te Rito is primarily sourced from the school's SMS. Some teacher information will come from assessment tools, where their name may be associated with specific assessments or specific student's results. Other teacher information, most likely their name, would be part of the Pastoral information about students and in teacher-to-teacher handover notes.

Proactively released

Figure 4 below gives a more detailed view of Figure 3, identifying the categories of information that are received from specific applications. Data does not flow out of Te Rito to other systems.

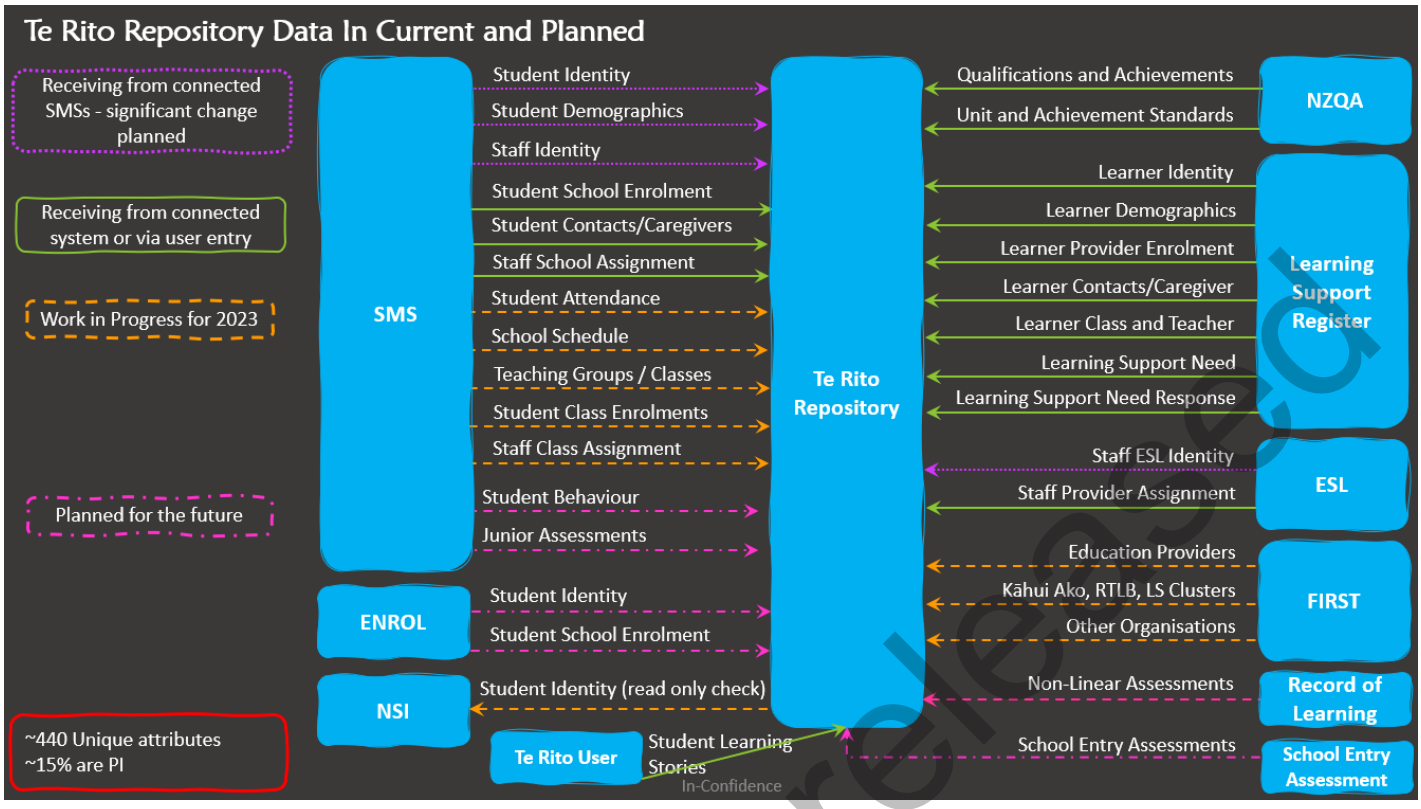


Figure 4: Te Rito Data flows – categories from source

By necessity Figure 4 does not show all attributes from each system, the detail of which attributes are in which groups is given in:

- Information types on page 36
- Appendix D - Te Rito Summary of student data categories on page 90
- Appendix E - Te Rito All data attributes on page 92
- Appendix F - Logical architecture view on page 93

An important distinction to highlight is that the students Te Rito record is not 'shared' or 'transferred' to the new school. A new school is granted authorised access to the students record in Te Rito on the basis of a valid enrolment. A parent or student must provide the new school with the student's Official name, Date of Birth and NSN. An SMS supplying these attributes to Te Rito requires an exact match, before Te Rito then grants access to the student's information in Te Rito. 'Access to previous records' may have been explicitly consented on an enrolment form. Otherwise, access to the student's information from a previous school is directly related to one of the purposes for the original collection, being delivery of education.

Whether school enrolment forms or privacy statements may need updating for Te Rito purposes is being considered. In terms of the Privacy Act, a new school being given access to the students record in Te Rito that includes information from their previous school may be considered a 'disclosure' or 'sharing'. However, this access is authorised with the knowledge of the student (or their parent) by the action of the student being officially enrolled. This is consistent with Te Rito being the student's record and owned by the student, with the Ministry or a school being custodians, and access is based on the student's enrolment status with a school.

The sections on Collection of personal information below and Dual attendance on page 51 elaborate how access to Te Rito records is managed during the enrolment process.

Proactively released

5.5.2 PII and non-PII attributes

Of the 485 attributes currently stored in Te Rito, per Table 6 below, 440 are unique. ~15% (10% excluding the LSR) are Personally Identifiable Information (PII) about students, their parents, or kaimahi. The remainder are non-PII, e.g. date of first attendance, year level, class assignment. Some attributes may be Personal Information (PI) in unusual cases, e.g. starting school mid-term, in that it tells us something about the individual, although it does not directly identify them. Given the possibility that free form fields may contain PII, some of these are counted as including PII based on field name. The planned additional integrations and data from SMSs will bring the total to ~1,000 attributes.

Table 6: Te Rito attribute totals – approximation

Attribute approx. count	Student / Parent	LSR specific	Kaimahi	School/org	Duplicates	Total
PII	20	40	15	0	15	90
Non-PII	100	60	75	130	30	395
Total	120	100	90	130	45	485

The PI stored by Te Rito is summarised in Appendix D Te Rito Summary of student data categories on page 90, elaborated in section 5.6.5 Information types on page 36, while all attributes stored about all users is detailed in Appendix E - Te Rito All data attributes on page 92.

In an EU General Data Protection Regulations (GDPR) context some Te Rito information is considered special category data. This includes; racial/ethnic origin, which may also imply religious beliefs; health; sexual orientation (or gender identity). For teachers there may also be union membership noted or visible e.g. through meetings showing in a calendar, though union membership is not stored by Te Rito as structured data. Consideration of GDPR controls potentially applicable for Te Rito is elaborated in section 5.6.5.15 on page 44.

5.5.3 Information volumes

At the start of drafting this PIA, there were ~11,500 student records in Te Rito, of which ~8,900 represent current students in Te Rito connected schools and kura. The remainder are for students no longer at Te Rito connected schools and kura. In addition, there are ~820 teacher records. The planned deployments will add student and teacher record volumes per Table 7:

Table 7: Approximate numbers of Te Rito users

Selected region	**schools| kura**	**students| ākonga**	**teachers| kaiako**
2023 active Te Rito users (excluding ECE)	36	8,900	820
Users to be added 2024 (excluding opt-in early adopters)			
Ngā Rau Whakatupu	11	6,300	590
Ngā Rau Whakatupu associated cluster schools and kura	89	32,500	2,840
Whangārei (1st group)	37	10,730	935
Northland|Te Tai Tokerau (inc 20 in 2nd group for Whangarei)	116	20,500	1,800
Ko Taku Reo (all teachers and full-time students)	1	170	400
Total users being added	**254**	**70,200**	**6,500**
Total users after this stage	290	81,700	7,320
Total once all schools connected	2,550	831,000	73,000

Proactively released

It will be a schools' decision as to whether only necessary kaimahi (principal and teachers) are given access, or whether other kaimahi, such as teaching assistants, office administrators, and other support staff will also be given access. As teachers are necessary to build class schedules, we have used that as the minimum.

Numbers are approximate as not all schools or kura may choose to adopt Te Rito. Those that do opt-in may not initially meet all requirements for SMS connectivity, user access, or may choose to send SMS information before onboarding kaimahi and student users at a later date.

In total the current planned deployments for 2024 will add ~70,200 student and ~6,500 teacher records, giving an estimated total of ~81,700 student and ~7,400 teacher records in Te Rito across ~290 schools. This is equivalent to ~10% of the NZ school sector[6].

The general availability of Te Rito to other schools, whether as early adopters or through subsequent regional deployments, will naturally add additional student and teacher records. This PIA considers the risk arising from full national use. In the future with all ~2,550 schools using Te Rito total records could comprise:

- ~831,000 student|ākonga records, growing at ~63,000 records per year over a seven (7) year retention cycle.
- ~73,000 teachers|kaiako including tumuaki|principals, growth likely static overall. Statistics on teachers entering and leaving the profession are equivalent.
- ~50,000 other kaimahi, inc teacher assistants, school administrators, other support staff
- ~1,200,000 unique parent records, growing ~93,000 records per year over a seven (7) year retention cycle (estimate based on StatsNZ household composition).

5.5.4 Unstructured information

A key challenge for Te Rito will be receiving the significant quantities of unstructured data from schools and presenting it in a consistent and reliable manner. Unstructured data will come from various sources including emails, shared folders or files, school network file storage, cloud document storage, documents attached within an SMS and so on. This is anticipated to be a particular issue for pastoral information, teacher to teacher transition notes, and possibly some health or medical information.

Learning Stories are an example of unstructured information that is associated with a student. A Learning Story may be formal, submitted by a teacher or student and associated with an assessed class activity. Or may be informal, submitted by the student or their parent through the main user interface of the Capture app, and stored as part of the Student Portfolio (see Figure 8 on page 39).

How unstructured data from various sources can be consolidated will be evaluated and tested with schools, with feedback sought from stakeholders on the actual value or benefit gained. A semi-structured approach, defining templates within Te Rito for specific types of information or particular business purposes, may be one approach. Encouraging SMS vendors to update their products to allow schools to store information in a more structured manner may be another approach. The context (including timeliness) and purpose of the information will need to be made clear in Te Rito, along with ensuring that the absence of unstructured data is not perceived as negative.

[6] The full breakdown of demographics including age cohorts for students, and teacher numbers in each education region is available on the Education Counts website.

Proactively released

5.5.5 Te Rito data access

Access to the information in Te Rito is based on which school a student is enrolled with, and:

- only specific kaimahi (principal, deputy principal and equivalent roles, current class specific teachers) at a student's current school can access a student's detailed information
- when a student moves schools, access for their former school is automatically removed when the student enrolment is marked as 'finished' in the SMS
- parents retain access to Te Rito when their child moves school through a re-authorisation process applicable to the child moving school.

Within a school, limits at a class level are enforced by Role Based Access Control. This provides flexibility for schools depending on how teacher and class assignments are handled, which will depend on how large the school itself is. Assignment of Teacher status to a class can include automatic deprovisioning on a specified date, which would apply for substitute or day relief teachers. The principal and deputy principal (or those holding equivalent roles such as a school administrator or dean) at a school can see all students and information associated with them. Only the Principal and school administrator, or kaimahi delegated those roles within Te Rito, can view and manage staff information.

Some non-identifiable information is shown in dashboards for Kāhui Ako (Communities of Learning), where principals and deputy principals of other schools in a Kāhui Ako can see aggregate data.

Figure 5 below provides an overview of the information visible to different kaimahi roles in Te Rito. Kaimahi such as a Dean may be assigned the Deputy Principal role, a decision for each individual school to make. Students can only see their own information, and basic information about other students in their class. The standardised Learning Support Register (sLSR) is included here for completeness, though is not in scope of this PIA.

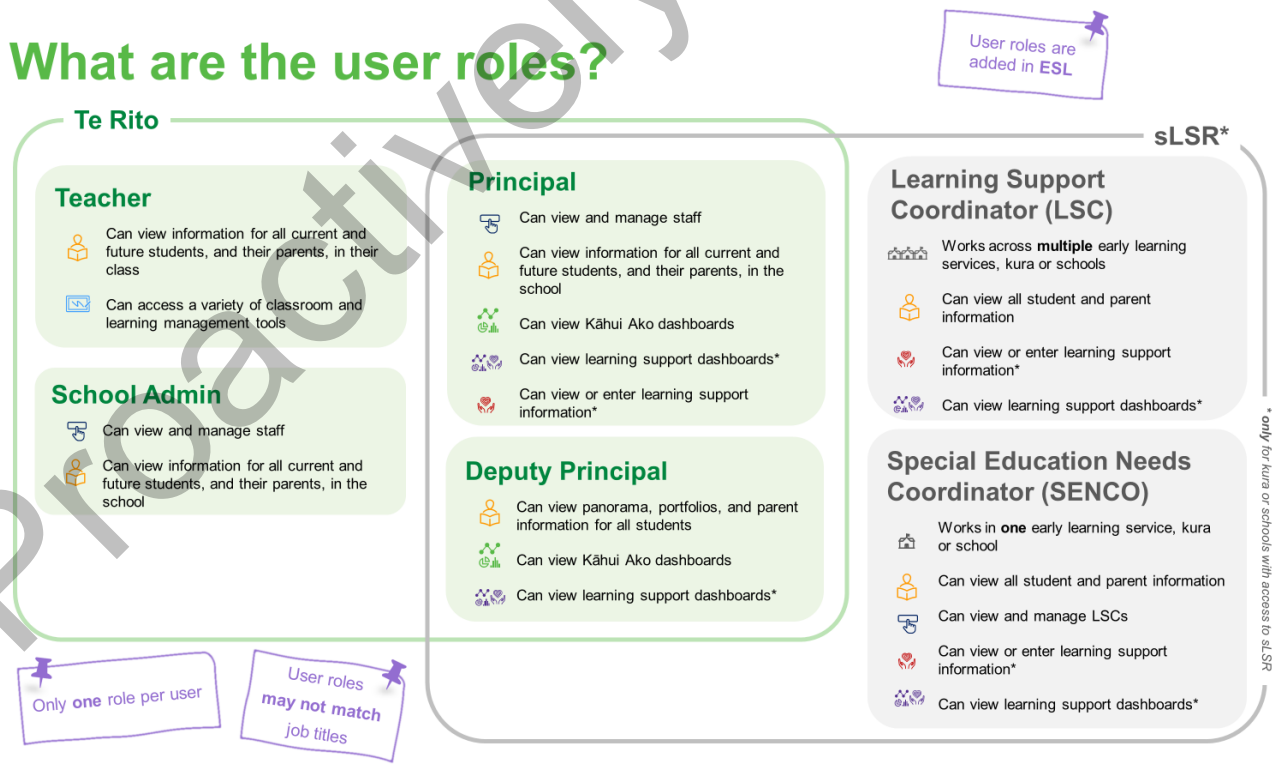


Figure 5: Te Rito user roles and access

Proactively released

5.6 Collection of personal information

Schools and the Ministry collect extensive information about a student at enrolment time and subsequently throughout their learning journey. There are nineteen (19) different Ministry systems that store or process information relating to enrolments. Throughout a student's journey through the education system information could be stored in up to thirty-five (35) different Ministry systems, along with each individual school's SMS and other digital education or administrative systems used. It is not the purpose of this PIA to describe the flow of data through the education ecosystem during the student's educational journey. Transparency by schools of the different school IT systems and Ministry systems that student information is stored in, is variable. Information tends not to be accessible to students outside of a Privacy Act access request. The detail of what personal information about students, parents and kaimahi is in Te Rito is elaborated in section 5.6.5 on page 36 onwards and the Te Rito Privacy statement.

Parental expectations of what age their children can share their personal information are trending down from 14+ to just over 12 years old. (see References on page 96 Table G3 *Australian Community Attitudes to Privacy Survey*, and LSE papers). Te Rito can identify whether consents have been obtained from the student or their parent.

Final wording of the Privacy Act amendment to address indirect collection may require comms. Either by the Ministry publicly notifying indirect collection, or further clarifying Te Rito's status as a schools' system not a Ministry system. Thus does not represent an indirect collection by the Ministry, or by subsequent schools.

5.6.1 Ministry as agent for schools

Per guidance published on the NZBA website directly about Te Rito, "*Boards are the accountable agency for Privacy in their school*".

The Ministry provides Te Rito as a service to schools and does not have access to Te Rito. With the exception of Ministry staff providing technical support to ensure data integrity, security & safety. Similarly Edsby is acting as an agent for schools, managing the information that schools store in Te Rito. Neither the Ministry nor Edsby process the data, per Privacy Act §11(3), within Te Rito for their own purposes.

While the Ministry is accountable in the public eye or from an education sector perspective for Te Rito, it is acting as an agent and service provider to schools. Similarly Edsby are responsible for operational management as agents for schools. In that regard, neither the Ministry nor Edsby, is collecting information for their own purposes. Schools are choosing to store in Te Rito:

- information that they have already collected from students and kaimahi, or
- upload information from other educational activities into Te Rito.

Use of 'Service Provider' in communications to the education sector for the Ministry's role in Te Rito has been to build trust and confidence. Reflecting that the Ministry has not mandated use of Te Rito. Service provider terminology has resulted in extensive discussion with OPC that ultimately was not resolved. This may effect risks P-06 and P-13 in the future. OPC have requested the following statement be included;

"*The Privacy Commissioner was consulted on the Te Rito PIA and does not agree with the Ministry of Education's assessment that it is acting as an agent for schools. The Privacy Commissioner considers that the Ministry of Education is the responsible agency under the Privacy Act for system level breaches*."

The Ministry agrees that it would be the responsible agency for notifying OPC of a potential privacy breach with Te Rito, irrespective of the material cause or extent of a breach. Elaboration of anticipated roles and responsibilities for incident management are included in section 5.13 Incident Management on page 54.

Proactively released

5.6.2 School collection – IT systems

Current school enrolment forms or privacy statements tend not to identify even the high level types of IT systems that a school uses and therefore where student, parent, or teacher information will be stored. By the action of delivering educational services, Schools collect substantially more information about students than is provided on enrolment forms, yet this is not made clear.

Analysis in 2022 showed that only five (5) schools out of a sample of 200 identified some of the specific IT systems that those schools used. In some of those examples only high level types of IT systems were mentioned. In other cases they still omitted the mandatory Ministry systems such as ENROL that all schools are required to use. The average school has twelve (12) different teaching applications and twenty (20) different administrative applications of an IT nature. The Te Rito project is performing further analysis of a nationally representative sample of schools. This will inform whether additional advice or guidance to schools about the content of enrolment forms or privacy statements may be required.

Schools do not offer an opt-in or opt-out decision for parents or students about whether their data can be stored in school IT systems used for educational delivery or school administration. Even if any opt-out choice were to be offered to parents or students, it is unlikely that would be meaningful given the foreseeable detrimental impact to the student's education, their participation in class, or attendance at school. Student attendance at school is mandatory.

5.6.3 School collection – business process for students

As with other school IT systems, the main purpose for a school collecting information about students and their parents is to enable and support the student's education. Te Rito directly relates to this broad purpose when using both administrative and educational delivery features.

The collection of student information by a school/kura starts at pre-enrolment time, which could be years before a student joins a school when their parents express an interest with their child being put on a wait list. Information is provided by parents, or in secondary schools may be provided by the students themselves. Collection of pre-enrolment information for cohort entry at the start of a new school year in January, will typically start in October-November of the prior calendar year. Where SMSs have a pre-enrolment flag on a student's record, Te Rito recognises this and discards the record from being stored or updated in Te Rito. Where SMSs do not have a pre-enrolment flag, Te Rito inspects the 'first attendance date' field to determine whether the date is in the past (a student is currently enrolled), or in the future (the student is not yet enrolled). Where the enrolment date is in the future, again Te Rito discards this information. In either case where Te Rito discards the update, the information would remain in the school's SMS and the school remains unable to access any information about the student in Te Rito.

Class specific data may be received from a secondary school SMS before students are confirmed as enrolled (first day of attendance) given the need to build the school's class schedule in the SMS. However, that does not equate to the school accessing a student's information in Te Rito. How far in advance schools populate their class schedules is a matter for schools, noting that full access to student information in Te Rito is still controlled as described above. In practical terms completion of an enrolment form provides consent for the school to store information about a student. Schools have a grace period for completing mandatory returns in ENROL, which is necessary to reflect actual student attendance from day one at school.

At subsequent enrolment points, i.e. starting a different school, the new school's SMS will send to Te Rito the student's official name, DoB and NSN information from the school's enrolment form. Te Rito will then match this record with existing Te Rito records for the same student. Matching is based primarily on the NSN, checked against other attributes including name and DoB.

Proactively released

Consents sought through enrolment forms are most commonly about the use of a student's photo or name on school social media feeds, websites, or newsletters.

Initial analysis of enrolment forms and Privacy statements for 700+ schools shows that 71% have explicit consent in their enrolment form, or a specific purpose in their Privacy statement that covers the sharing of student information with the student's next school. Thus use of Te Rito by schools with automated sharing to the next school is already agreed by parents. With further analysis we expect this result to trend to 92% of schools having either explicit consent sought or a privacy statement identifying sharing as a purpose.

5.6.4 School collection – business process for kaimahi

Schools collect staff information at commencement of employment with the full knowledge of the staff for the purposes of their employment and role within the school. Whether schools specify which educational delivery or administration systems kaimahi information will be stored in at the time of collection or subsequently, is a school decision. Given the relative flexibility that teachers have to use education delivery tools that they are familiar with, it is likely that most schools do not have a complete list of all educational delivery applications used by kaimahi.

Detailed personal information about staff in the SMS and thus Te Rito is limited, per section 5.6.5.12 on page 44 and the Te Rito Privacy statement. As shown in Table 6 on page 31, most information about teachers in particular relates to their classes and is not personal information.

5.6.5 Information types

This PIA is deliberately wide, covering the different types of information that have been identified by Ngā Rau Whakatupu as necessary information to help student's education during changes of school or teacher. Not all the identified information will be stored in Te Rito immediately from all schools for all students.

Discovery and evaluation work will be required to qualify whether the identified information is useful, necessary, and beneficial to be in Te Rito. By necessity this work can only be done with schools using real information about students to confirm the anticipated benefits.

Through the discovery and evaluation work *some* schools will start storing in Te Rito *some* of the information identified in the following sections. Successful scenarios will likely lead to more groups of schools following the same approach.

In the future Te Rito will contain some particularly sensitive information discussed in the sub-sections below. In Te Rito particularly sensitive information, such as Behavioural or Health information, would not be visible to either students or their parents when they do access Te Rito. This represents a default high privacy and high safety by design consideration. Health information may be generally known by family and friends at school, e.g. eczema, or may be highly private, e.g. diagnosis of a serious illness. To preserve both safety and privacy, this information is only visible to limited Kaimahi roles. This avoids the risk of disclosure due to students leaving computers unlocked, shoulder surfing in class, or parents having access to their child's computer for home internet safety purposes. Parents and students retain a right of access to their own information, which would have to be facilitated by their school.

Some sensitive information relating to learning needs is part of the Pastoral or Behavioural information in Te Rito. Sub-categories of data include; Resource Teacher's for Learning and Behaviour Support (RTLB), Resource Teacher's for Literacy (RTLit); teacher transition notes; health conditions; High Health Needs (HHN). The sLSR benefits from all the existing controls identified in this PIA.

Proactively released

5.6.5.1 Biographic data

The Student Admin part of Te Rito stores the core biographic information about a student, name DoB, NSN, preferred names etc. as shown in Figure 6 below. Only the Principal, Deputy Principal and school administrator have access to all the biographic information, teachers do not. This is the primary source for the profile photo used in Te Rito.

The student admin section also includes parental information, elaborated in more detail in section 5.6.5.11. Basic information about the students learning support needs, additional information on their strengths and free form notes is also included. The History view provides a full audit trail visible to the Principal and Deputy Principal(s) of the changes made by Kaimahi or the student to the information stored in Te Rito about the student.

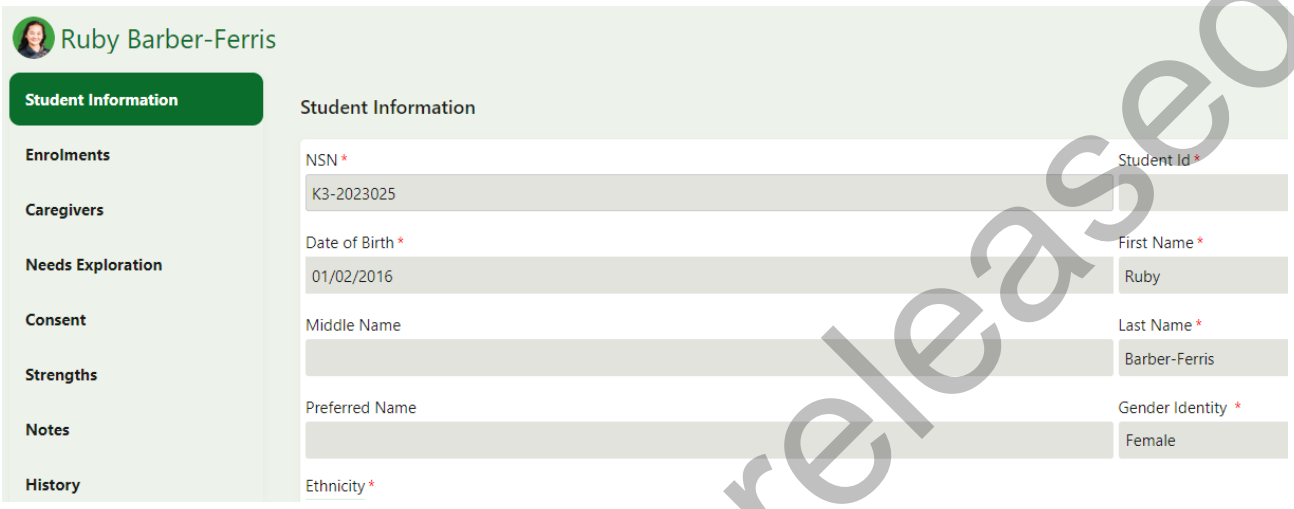


Figure 6: Student Admin profile view

5.6.5.2 Consent information

Te Rito currently stores basic consent information. In Figure 7 below consent has been provided for Ruby's information to be shared (anonymously) with the Kāhui Ako cluster. Consent has also been provided for Ruby to receive Learning Support services. The right hand column records whether consent was provided by the student or their parents. Consent has not been provided for Ruby's former ECE to share any learning support information with her school. Under the Education and Training Act learning support information can be shared between schools, however between ECE's or from an ECE to a school, consent to share is required.

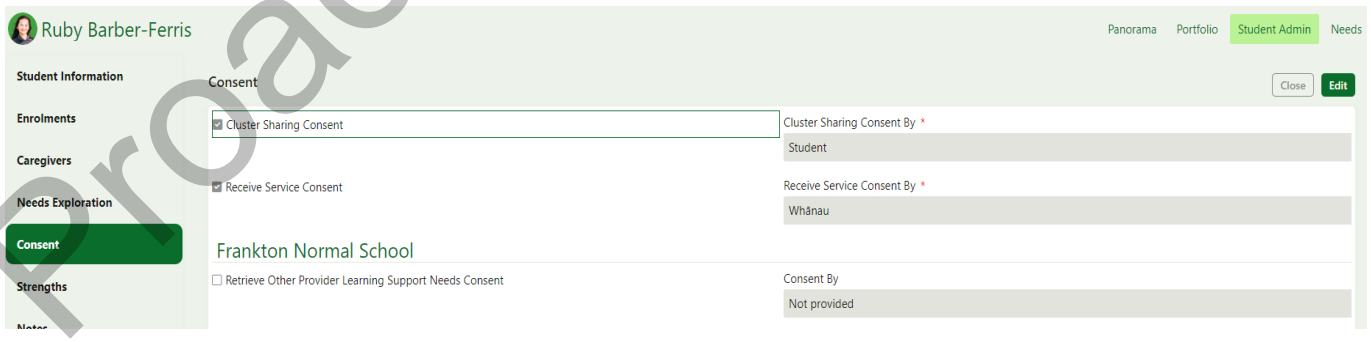


Figure 7: Consents in Student Admin page

Recording of consent to share student information with their next school has been implemented. This will help resolve any ambiguity about access to the student's record in Te Rito by their next school and can be recorded directly in Te Rito even if school enrolment forms or SMSs are not updated accordingly. Additional consents may be included in the future based on feedback from schools.

Proactively released

5.6.5.3 Enrolment data

The Ministry's core application collecting student enrolment and core biographic data is known as ENROL. Data from ENROL will be used by Te Rito to identify which school a student is enrolled with. ENROL is the authoritative source for this information within the Ministry and should match information supplied directly by schools from their SMS. This will be particularly important in validating claims from an additional school that a student is dual-attending, thus has authority to access the student's information.

In the future additional data quality checking may be performed to implement a control enforcement point. Where a school's SMS has been updated with an enrolment, until such time as that is confirmed via ENROL access to data in Te Rito about that student could be limited.

5.6.5.4 Attendance data

Te Rito is currently collecting data on a student's attendance in compulsory schooling from a school's SMS. Attendance is captured in half-days for primary and intermediate schools and per period for secondary schools. Te Rito receives;

- date of attendance,
- period or half day, period name (if available), start and end times per half-day/period,
- attendance code (present, absent, justified absence etc.).

In the future, Te Rito may receive data supplied by schools to the Ministry's Attendance Service Application (ASA). Attendance services is a Ministry run national service that works with any child who is enrolled that has not been attending school, to understand the reasons for the poor attendance and to remedy them where possible. It is unclear what specific data Te Rito might receive, but at a minimum it is likely to be the reasons for the poor attendance and actions in place the resolve this.

There is no plan to include Stand-downs, Suspensions, Exclusions or Expulsions (SSEE) data in Te Rito. Inclusion of SSEE data would be a material change to this PIA.

5.6.5.5 Assessment information

While the specific data received from each assessment tool is slightly different, assessment tool data will include the following of which only NSN and teacher name is unambiguously PII:

- **NSN** (Plus in some assessments, **student name**, **DoB** for data integrity checking)
- assessment tool name, assessment name, assessment type
- test questions and answers - (answers may be PI)
- test analytics
- assessment number (unit and achievement standards)
- year level, subject code, year assessed, level
- credits
- assessment result, raw score, scale score, total score - (results may be PI)
- competency
- stanine
- error margin
- assessment date and time
- school assessed by
- **teacher assessed by.**

Assessment tools enable schools to comply with their obligations under the ETA on assessing capability and measuring progress, alongside reporting to the Ministry and parents. Assessment

Proactively released

results alone may not be sensitive, however if particularly good or poor assessment results were publicly known this could cause emotional harm to a student or give rise to bullying.

5.6.5.6 Student content

In addition to the information from a school SMS or other Ministry systems integrated to Te Rito, students themselves are able to contribute their own information. Functionality within Te Rito provides an 'about me' or 'student voice' section where students can provide information about themselves that they wish to share with their teacher or classmates. The Te Rito default is that 'about me' is only visible to the principal and teachers for a student, not visible to other kaimahi or students. This avoids the free text field being mis-used by students to publish inappropriate information to the whole school.

A key function of Te Rito is the Student Portfolio, where students can upload or save evidence of informal learning as they are comfortable with, or formal submission of class assignments. More formal Teacher curated submissions are termed as 'Learning Stories', though may be materially no different from a portfolio story. All information is retained within the walled garden that is Te Rito.

An example of 'about me' and portfolio information is shown in Figure 8 below. Screen shots are taken from the Te Rito demo environment, which consists of entirely fictional information.

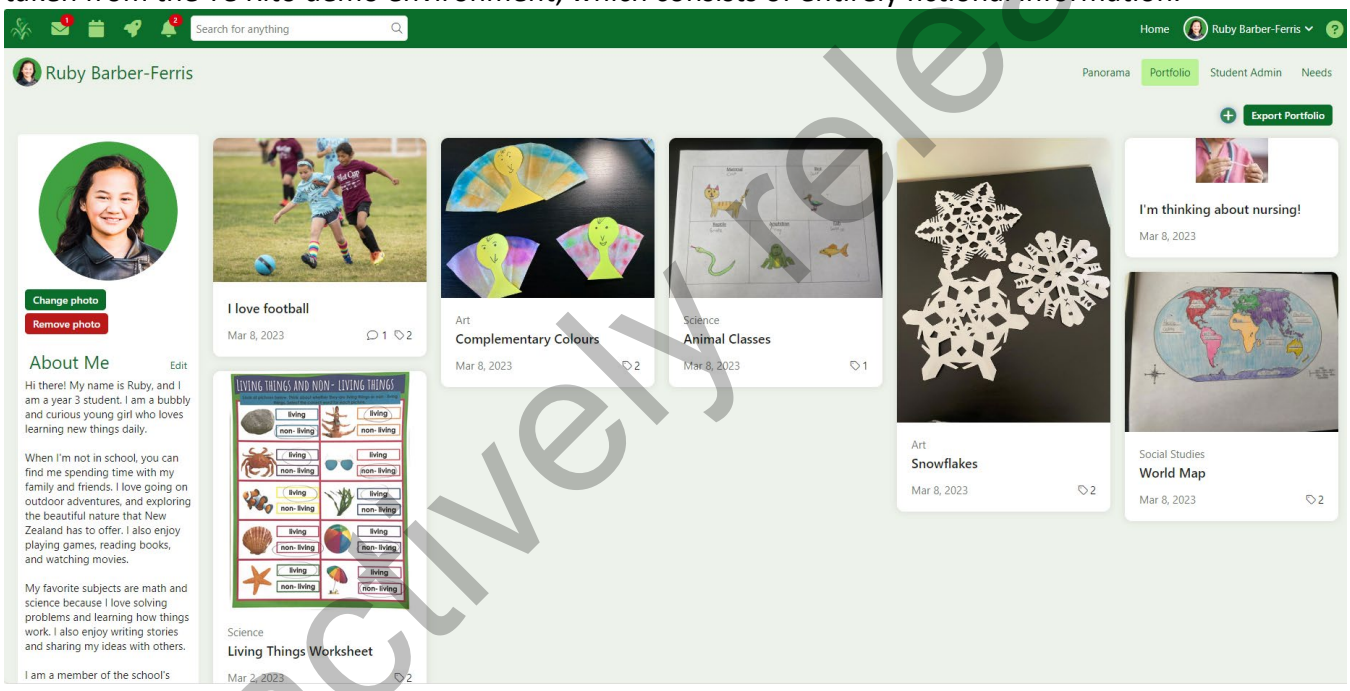


Figure 8: Student About Me and Portfolio

The student voice section of Te Rito allows a student to articulate in their own words their interests, ambitions, goals, career aspirations, or roles and responsibilities that they hold in the school or wider community. None of this information is mandatory.

When students participate in a school collaboration group, the information they submit to the group is accessible to all group members. Detailed information about a student is not available by default, only their name and school profile photo are available. As shown in Figure 9 for a group that Ruby is a member of, Ruby is unable to see any 'about me' or portfolio information for Kaihautu.

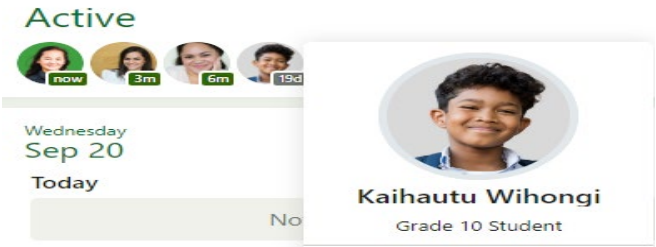


Figure 9: Student profile visibility to other students

5.6.5.7 Pastoral - Student behaviour information

Currently behavioural information within Te Rito is limited to the sLSR, which does not adequately distinguish between positive or negative behavioural information. The sLSR would not be visible to

Proactively released

students or parents through their own Te Rito login if those logins were enabled. Parents and students retain a right of access, which would have to be facilitated by their school.

Principals and kaimahi holding equivalent deputy principal roles such as Learning Support Co-ordinator (LSC) or Special Education Needs Co-ordinator (SENCO) have access to sLSR information. Teachers only have visibility of a tick box indicator, which would prompt them to follow up with their Principal for the specific detail.

Inclusion of positive behaviour information, outlined below, will need a data model defining for any structured approach to information being stored and made visible in the core Te Rito service. As discussed above, students may still supply some of this information in their About Me profile.

The positive behaviour and participation information categories are:

- student strengths
- positive behaviour event
- student awards
- roles and responsibilities
- gifts and talents.

Templates will likely be needed for more freeform observational information; tags can be defined to provide some structure aligned to learning outcomes or curriculum objectives. How this could work will be evaluated and tested with schools. Feedback will be sought from stakeholders on the actual value or benefit gained, ease of use, where the information should be visible and to who (e.g., Student Admin, limited to principals; or Student Panorama, visible to student, parents and their teacher etc.) Whether this information could be supplied by the students themselves or parents, is also something that will be evaluated.
A common trend in education and the workplace is to shows 'badges' which are associated with awards or achievements. These are optional to show, typically as part of a student profile, e.g., team captain, prefect.

Additional pastoral participation information has been identified by Ngā Rau Whakatupu as highly useful. This includes:

- conditions affecting student
- events impacting student (E.g., death in family, refugee)
- diagnosed learning or behaviour condition (E.g., ADHD, ASD)

Qualifying how necessary this information is and direct relevance to a student when they change schools or there is a new teacher, is something that will be evaluated in a small scale school pilot. It is likely much of this information will be unstructured information. Naturally there is some cross over with health and medical information.

5.6.5.8 Student health and medical Information

Health or medical information will be stored in Te Rito where it has direct relevance to a student's safe participation in education at school. Enrolment forms commonly ask for health and medical information to varying levels of detail. Whether health and medical information is collected from parents or older students directly will be for the school to determine in each individual case. How much of the information is stored in the SMS or Te Rito will also be decided by the school.

Once the health and medical information is within Te Rito, then this reduces the need for students or parents to repeatedly provide the same information to a new school. It also mitigates the risk of forgetting something at the time of enrolment that may be important. Some health or medical information is more pastoral in nature, use of pastoral or health categories is not mutually

Proactively released

exclusive nor easily separated for unstructured data. Categorisation of unstructured information may not neatly fit definitions used for structured data.

Health information within Te Rito is not visible to students or parents. This represents a high safety high privacy by default configuration. Otherwise, the reality of students not following good information security behaviours, locking their PC's, logging out of applications etc. means that people who are unauthorised (other students) or unintended (other people at home), may be able to access otherwise sensitive information that may not be public knowledge. Principals have access and very limited information is visible to teachers. Parents and students retain a right of access, which would have to be facilitated by their school.

There is some cross over between basic biographical information and health information. The health and medical information that Te Rito may receive is subject to further discussion and validation with school sector representatives. For the purposes of this PIA, limited health or medical information may be stored in Te Rito to explore how useful the information may be, how it can be safely managed, the possible application of different retention periods etc. Initial candidate health and medical information from SMS's includes:

- Medical condition, action required, medicine details (see examples in Table 8 below)
  - In some cases, this may have a safety aspect e.g., asthma, diabetes, eczema, haemophilia. In other cases, e.g., ADHD, it is pertinent to learning & education.
  - At enrolment time if the school decides that a medical condition isn't pertinent, the information shouldn't be recorded in the SMS and thus would not be in Te Rito.
  - The risk of receiving any 'not pertinent' information that the school has recorded in their SMS, should not exclude all the other necessary and pertinent information that is recorded from being received. This represents a safety by default approach that may lead to storing some unnecessary information in Te Rito.
- Allergy, action required, medicine notes
  - In many cases this has a safety aspect, e.g., nut allergy.
- Medical centre name, doctor name, medical centre phone, doctor phone
- Immunisation status / details
  - There tends to be little of this in SMS's, discovery work relating to B4SC is underway. B4SC information is outside the scope of this PIA.
- High Health Needs (HHN)
  - Directly necessary for participation in education and at school. This cohort of students tend to have information shared between schools, partly because of funding, partly because the student can't participate in school without help to meet their needs.

Table 8: Example Medical condition information

Condition	Medical Action Required	Medicine Details
Asthma	Give Ventolin Inhaler. If breathing improves, keep an eye on the student until recovered. If breathing does not improve call an ambulance.	Ventolin Inhaler
Haemophilia Mild case.	No contact sports. Do not give aspirin or ibuprofen. If bleeding starts and does not stop, call the student's parents. If they are unreachable call an ambulance.	No medicine
Epilepsy	In the case of a seizure, when the student falls to the ground, remove anything around them that could cause them injury, place something soft under their head. Once seizure is over, roll them on their side and reassure them till they recover. Ring the parents. If they had food or fluid in	No medicine

Proactively released

Condition	Medical Action Required	Medicine Details
	their mouth at the start of the seizure roll them onto their side immediately. If the seizure lasts for more than 2 minutes call an ambulance and the parents.	

5.6.5.9 Support and interventions (funding information)

The data category called 'support and interventions' includes funding for those support and interventions. The focus for Te Rito is on the funding aspect, to enable schools to plan for helping students. Not necessarily storing the detail of the need within Te Rito, which would be part of Pastoral data. A school that currently receives funding clearly knows of and stores information about this funding. One purpose of Te Rito is to clearly identify to a prospective or actual new school that a student has support needs and there is funding already available. It is likely that some funding information would be shown under pre-enrolment scenarios. Funding information related to behavioural issues may not be visible pre-enrolment. Evaluation work will be performed with schools to confirm what is necessary and proportionate.

Situations where a new school only needs the funding information will be considered first. Where the support need may require the additional 'detail of need' information, how this may be stored in Te Rito or the sLSR will need further consideration. Irrespective, this PIA highlights that such discovery work will take place, and similar to Health or medical information, some evaluation work is required with students and schools to confirm how little or how much information is necessary.

Funding services provided by the Ministry are quite broad and cover many education-related areas such as ESOL, ongoing resourcing, teacher aide or specialist teacher, SESTA. The Te Rito project is prioritising which funding systems to integrate with based on Ngā Rau Whakatupu input and guidance of student need and relative impact in supporting a student's education. At a high level the data received from the different systems can be described as:

- Student name & contact details (possibly of parent)
- Funding Initiative/Service Name
- Funding Need – what the student needs the funding for
- Funding Term – how long the student is funded for
- Funded Hours – the number of hours a day/week covered
- Funded For – what is covered by the initiative/service, e.g., teacher aide
- Funded At – what school(s) receive the funding for the student (not all funding follows the students as they move schools)
- Any supporting plans, strategies, and goals for the student.

Depending on the specific funding system, additional information may be stored. For example, SESTA stores a home address specifically for the purposes of transportation.

Some learning support information would be considered pastoral information, again, the categorisation of unstructured information may not neatly fit definitions used for structured data.

5.6.5.10 Transition notes

Feedback from multiple sector representatives articulates that exchange of teacher-to-teacher transition notes, especially between schools, is ad-hoc and unstructured. As noted above, students with high health needs tend to be one cohort of students where there is a structured transition approach. Many other students with support needs are adversely affected by a lack of any handover notes. This has a particularly detrimental impact for transient students, or students who suddenly change school without prior notice to their former or new schools.

Proactively released

One of the purposes for Te Rito is to establish a structured and secure mechanism for the exchange of transition notes. Ensuring that all students benefit from some form of handover from one teacher to another, one school to another, allowing new teachers and schools to start getting to know a student before teaching them. Transition notes would only be visible to new schools at confirmation of enrolment and not visible under pre-enrolment scenarios. Though this does not preclude that the same information may be exchanged by other means pre-enrolment. Class placement recommendations which may include in class achievement beyond formalised assessment results, are identified as particularly helpful.

Initially transition notes may be received from SMS's, in the future templates for transition notes may be defined in Te Rito. It is likely the information would be added directly to Te Rito, pending possible updates by SMS vendors in their products to align with the new fields.

Providing the functionality and capability to create transition notes does not mean this will immediately happen in a consistently professional manner. Training or guidance for teachers will likely be required in the use of any standard forms developed, or to establish a common terminology and taxonomy. A focus on specific pastoral information may help guide templates or expected content in transition notes. The categorisation of unstructured information within transition notes may not neatly fit definitions used for structured data.

5.6.5.11 Parent information

As noted previously, minimal information about parents is stored in Te Rito and always in the context of their relationship to their child as a student at a school. This includes the parents name, email address and other contact details that a school would collect via enrolment forms. Figure 10 below shows a parent profile, identifying related children and recording any free text observations about the parent.

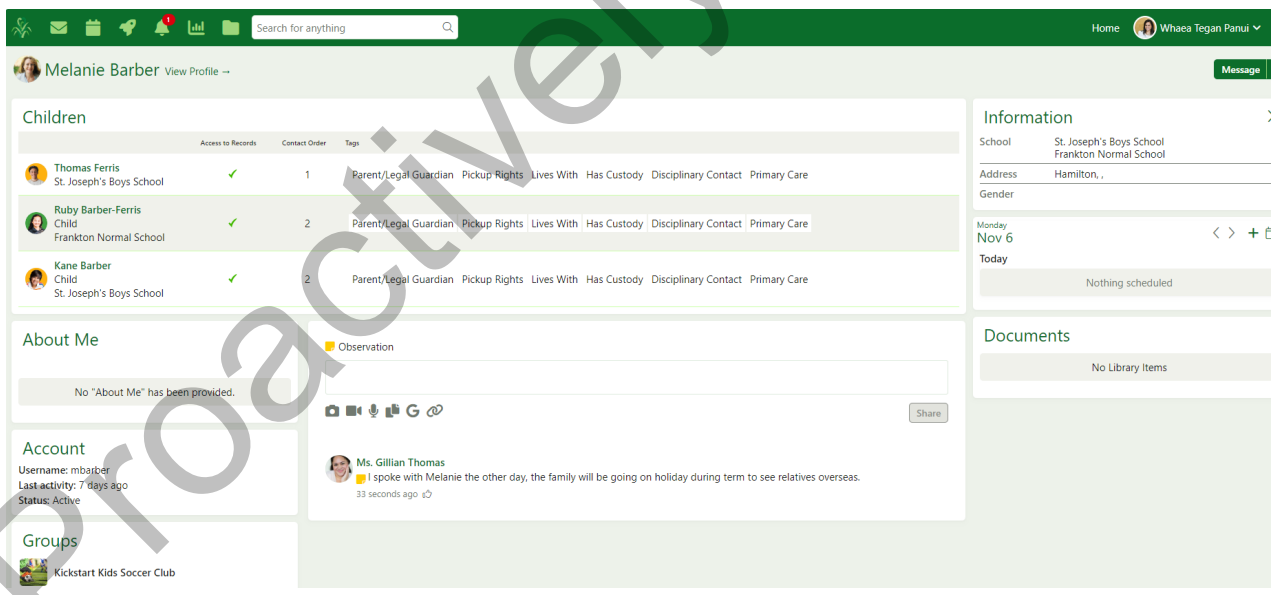


Figure 10: Parent profile view

Additional information such as a profile photo would be optional for parents to submit to the school or update themselves in Te Rito. Observations are visible to the teachers of the associated students, as shown above from the demo environment where Gillian as the Principal has made an observation that is visible to Tegan as Ruby's class teacher.

An 'access to records' filter can also be applied in cases where a parenting or custody orders exist. Ensuring the parental relationship is correctly identified, while preventing the non-custodial parents' access to information in Te Rito about an individual child. Additional tags are available for contextual purposes e.g. 'pick up rights' 'lives with', being important for kaimahi to be aware of.

Proactively released

Formal court orders will not be stored in Te Rito. They may be legally privileged documents or contain sensitive information, beyond common knowledge of a child's parents being divorced or living apart. Instead freeform parenting notes can be written in the Student Admin view, per section 5.6.5.1 Biographic data.

Te Rito provides a parent portal which is not currently enabled. In the future it will allow parents or guardians a single interface to view information about their children irrespective of which school they attend. This is naturally dependent on the school using Te Rito.

5.6.5.12 Kaimahi information

As noted previously, the PII in Te Rito directly related to kaimahi is minimal. Their names, legal and preferred, school email address, a profile photo is all publicly available on school websites or other sources. Biographical information about kaimahi can be added by kaimahi themselves in Te Rito, or by a school administrator to the SMS or Te Rito with kaimahi consent or at their request. Biographical information includes gender, preferred language and contact details. As with students, 'about me' information in Te Rito is optional.

There is no field to store health, ethnicity, or religious information about kaimahi, although languages spoken may infer ethnicity. Kaimahi may choose to include ethnicity or religious information as part of their 'about me'. All other kaimahi information is related to their role in the school and class. See Appendix E under Te Rito Education Sector Employee Data and Te Rito Teacher Collaboration Data.

5.6.5.13 Adult students

Some Learning Support Students may remain in secondary school after their 19th birthday, potentially up to the age of 21. It will be for the student and school to decide whether storing parental information is appropriate given the students maturity or relative level of independent living. This would determine whether their parents continue to have access to Te Rito.

Adult students are permitted in secondary schools to support achievement of minimum numeracy and literacy levels, and appropriate NCEA qualifications. Adult Students may be asked to agree to Terms of Use applicable to them, these would be written for a reading grade 8 (age 13), which is consistent with working towards NCEA level 1. From a Te Rito perspective, adult students are otherwise no different from any other student.

5.6.5.14 Young children's ECE attendance information

ECE providers use ELI as their enrolment management reporting tool to the Ministry. Te Rito receiving some attendance data from ELI is being investigated. This is helpful for schools in the context of supporting a young child's transition to, and participation in, full time school education. Another need has been identified relating to schools supporting parents with applications for specialised school transport assistance. A purpose directly related to attendance and participation at school. Data from ELI may constitute another pre-enrolment scenario.

5.6.5.15 GDPR and special category data

As the *Data Analysis PIA* made a number of references to the possible applicability of GDPR, commentary is included below. The risks and controls identified in this PIA were cross checked against controls that are recommended as part of the GDPR to identify any applicable controls that may be useful. The conclusion of this analysis identified no additional controls.

Proactively released

Data held by schools about individuals within NZ is likely not considered within scope of GDPR. Primarily as schools are performing a core government function of providing mandatory education within New Zealand. In GDPR terminology this would equate to 'substantial public interest' 'statutory and Government purposes'. This PIA may be considered suitable as an 'appropriate policy document' supported with additional process documentation.

Where students are EU or UK citizens, this may be identified as structured data within Te Rito. However, as roll returns do not necessarily identify dual-citizenship status, additional business logic is not applied in the handling of information in Te Rito. Citizenship may also be noted in freeform text, including for parents or kaimahi.

All Te Rito data is protected with consistent high security/privacy by design defaults and controls. These are consistent with the controls expected by GDPR. As identified in the prior sections, the principle of least privilege is applied to the level of information that kaimahi are able to view.

In a GDPR context some Te Rito information would be considered special category data;

- racial/ethnic origin, which may also imply religious beliefs;
- health;
- sexual orientation (or gender identity).
- teachers' union membership may be visible e.g. meeting showing in a calendar, though union membership is not stored in Te Rito explicitly.

For students, storing information about ethnic origin or religious beliefs (by implication) is entirely optional and driven by the information provided to a school by the student or their parents and stored in the SMS. Religious information is not explicitly stored in Te Rito. Basic demographics relating to gender identity is collected by schools in the SMS, and currently represented in Te Rito as Male, Female, Gender Diverse, Transgender. Te Rito has an option to record 'decline to answer'. Whether SMS's have a similar option will vary, as will a schools' policy on needing to record an answer.

Given that teachers are interacting with their students on a day to day basis it is highly likely that a teacher would know a student's racial or ethnic origin, their gender, and may have knowledge of religious beliefs. It is also likely that teachers would know important health information, to ensure the students safety in their class.

Additional protection is provided in Te Rito for health information by enforcement of the principle of least privilege and attribute based access control. Only Principals and school administrators are able to see all information about students, parents or kaimahi. Teachers are not able to see all information about their students or colleagues. Storage of health information is discussed in section **5.6.5.8 Student health and medical Information** on page 40.

Within Kāhui Ako dashboards ethnicity and iwi affiliation can be used as a filter where the information is available. Gender identity can be used as another. All information in the dashboards is anonymous.

Other than for health information, no material risk is identified for special category data that may require additional controls beyond the high level of protection already implemented.

5.6.5.16 Information about all users

Additional transactional information relating to all users will also be stored as part of Te Rito, ESL and the school's IdP. This will include computer TCP/IP address, non-PI device details including type and versions of OS and browser. This information is stored in the audit logs for the different applications and is necessary as part of providing an internet based service. It is used as necessary for service support and security purposes.

Specific geolocation information about Te Rito users is never collected or stored by Te Rito.

Proactively released

5.7 Use of personal information

The purpose for using information in Te Rito is discussed in section 5.2 Te Rito overview on page 21 and elaborated in section 5.6.5 Information types above. In summary:

- Te Rito is a national information sharing platform that enables information about ākonga and students to follow them throughout their education.
- One of the purposes for schools collecting student information is to enable and support a student's education.
- Sharing the information with a subsequent school is directly related to that purpose
- Te Rito facilitates the access to a student's information in a secure, safe, and reliable manner.

Te Rito also provides schools a backup capability for educational business continuity. Ensuring that critical information from their SMSs or other key systems, is held securely and remains available in the event of an outage of school IT systems.

It is not possible to explicitly identify which particular features or functions of Te Rito a school may, or may not, use for particular purposes. This PIA therefore considers the general use of Te Rito and the data within it for educational purposes by schools. Schools remain responsible for ensuring that their use of Te Rito is consistent with the Privacy Act.

5.7.1.1 Use of student information

From a Privacy Act perspective, Te Rito's use of information is consistent with IPP 10 (1)(a). Being directly related to one of the purposes for which the information was collected by a school - to enable the student's education.

Student information stored in Te Rito is used to improve the transition process for students moving schools at any time of the year, moving up a year (cohort entry), or when there is a new teacher. Building a digital portfolio about a student requires regular and continual information update, ensuring accuracy and currency. Te Rito will ensure that student learning needs are identified as early as possible, that schools can receive information about the student and what works best for them. Te Rito will ensure that information about students is managed and shared in a secure and reliable manner. Te Rito will be able to facilitate greater engagement by students in their education, particularly when students cannot physically attend school for various reasons.

Collaboration groups are anticipated to be created by schools for students, both within their school and across-schools as required. PII is naturally involved in a collaboration group by virtue of a name and profile photo being showing in the list of group members. Whether any other PI may be involved in a group will depend on the nature of the group.

5.7.1.2 Use of parent information

The use of information within Te Rito about a child's parents is directly linked to the child's attendance at school. This use and purpose are directly related to the school's original collection and use of parent information at enrolment time.

5.7.1.3 Use of kaimahi information

Use of personal information about kaimahi is in the context of their role in the school relating to educational delivery. For example, Te Rito does not store HR records relating to kaimahi, nor include kaimahi medical information, salary etc. Therefore the information is not in Te Rito in the first place.

Proactively released

To enable cross school collaboration all kaimahi are visible in a Te Rito directory. Kaimahi can search this directory by name to establish contact via Te Rito message with kaimahi at other schools. Principals can add Kaimahi from another school as a Teacher of a class at their school, which is particularly helpful for distance learning providers such as Kōtui Ako, NetNZ and Te Kura. Kaimahi can opt-out of being listed in the Te Rito directory.

The Teaching Council website includes a public register of all teachers in NZ. Most schools also publish a list of staff on their websites, often with a contact email address. Based on this information being publicly available and feedback from Ngā Rau Whakatupu, explicit consent (opt-in) from kaimahi will not be sought before they are added to the directory. Opt-out is available.

5.7.1.4 Young children's use of Te Rito

Although Te Rito will store student information for all school years 1-13, it is unlikely that students in years 1-4 (ages 5-9) at primary school will be directly accessing Te Rito. Beyond the complexity of remembering a user id and password, the digital fluency skills in using a keyboard reliably may prevent meaningful educational use. It will be for schools to decide when it is appropriate for their students to start using Te Rito as an educational application. Guidance on this is available from Edsby based on experience with other customers. There is anecdotal information indicating some schools use Hapara or Seesaw with year 2 students.

The year 1-4 age cohort can engage with Te Rito on Chromebooks or iPads via the Edsby Capture app. The Capture app provides a one way upload of a learning story to Te Rito, without requiring the individual uploading to have a Te Rito logon, or use the full function user interface.

Authentication for the Capture app is via a QR Code unique for each student. The QR code can be printed for ease of use in the classroom or at home. Thereby providing parents with the ability to save informal learning stories to Te Rito without requiring a login.

Young students using the Capture app would likely be assisted by kaimahi or parents. Those adults can take photos of schoolwork adding a short written or audio description and upload to Te Rito. Young students or parents uploading video or audio content will be stored in the student portfolio. For teachers this may be saved as a formal teacher curated learning story.

Interacting with Te Rito via the Capture app is more age appropriate for younger students to interact with Te Rito. They gain familiarity and understanding in a low engagement channel without providing them full access to Te Rito. The vast majority of year 1 students are familiar with the taking of photos and uploading of work to ECE tools such as Storypark. Specifically for the purpose of sharing those stories with their parents. Tools like Storypark also provide ECE kaimahi with the ability to tag curriculum learning progress and objects, demonstrating a student's learning. Te Rito has equivalent functionality through the Edsby capture app. Parental access is then a natural progression that young children will understand from tools such as Storypark used in ECEs.

Proactively released

5.8 Storage of personal information

The Te Rito service is hosted in Microsoft's Azure datacentres in Australia. In a subscription managed by Edsby with an instance dedicated to the Ministry. The Te Rito project team have reviewed assurance documentation from Microsoft. This assurance documentation includes the most recent and past SOC2 Type2 reports, ISO27001 & ISO27701 Certifications, and Australian government Information security Registered Assessors Program (IRAP) audit reports. The different assurance processes and practices provides a high level of assurance that Microsoft has effective information security and privacy practices in place.

Edsby hold ISO27001 Certification for their Information Security Management System. This independently audited industry standard certification provides a significant level of assurance, above and beyond attested privacy pledges. Edsby has also been successfully assessed by ST4S, as elaborated in section 5.14 Additional analysis and assurance on page 55.

Edsby has signed the most recent version of the US student privacy pledge Signatories 2.0 – Pledge to Parents and Students (studentprivacypledge.org). The use of Te Rito also meets the requirements of the pledge. This makes clear that information in Te Rito, including information about students, will not be re-sold, aggregated, or shared for commercial purposes irrespective of whether there is a direct payment or not.

Access to information in Te Rito requires login via Ministry ESL for kaimahi, or school identity providers Microsoft 365 for Education or Google Workspace for Education for students. Role Based Access Control (RBAC) is further enforced to limit the information that an authenticated user is able to access. Storage and access controls are discussed further in analysis of IPP5.

Proactively released

5.9 Disclosure and sharing of personal information

Te Rito does not facilitate or enable any additional disclosure or sharing that is not otherwise already permissible or authorised by schools. Schools exchange information for necessary purposes by other less secure or reliable means today.

Te Rito does provide improved ease of access to a student's own information. When parent access is enabled, they too will benefit from this improved ease of access. A parent would either be exercising a right of access on behalf of their children or authorised to access educational information via their role as a guardian. The limited parent access to student information in Te Rito is unlikely to constitute an unauthorised disclosure.

5.9.1 Access to information

Information in Te Rito is held by schools as custodians for students. Business processes schools are responsible for and formalised with the Ministry, e.g. enrolment, then facilitate the 'access to' or 'sharing of' student information. The Ministry does not own, nor access the data within Te Rito.

As identified in the SDEX PIA;

"*There is no question of the Ministry's legal authority to collect the information* [in SDEX]*, as it is a perfectly legitimate role for the Ministry to facilitate information flows across other agencies in the sector*."

The SDEX PIA identified no need for any additional regulatory response. The SDEX use case of facilitating and sharing student information was assessed as legal in 2006.

In the more modern construct of Te Rito, the Ministry is facilitating the access to information about students for schools. In the same way that the current Student Record Transfer Service (SRTS) facilitates the information flow. From a Privacy Act perspective sharing is consistent with IPP 11 (1)(a), being directly related to one of the purposes for which the information was collected by schools - to enable the student's education.

While the vision of Te Rito is that students own their record within Te Rito, in practice and practical terms other organisations and individuals are responsible custodians managing access to information, updating it, ensuring it is kept safe and secure. All in the best interests of the child. Parents are responsible for providing consent on behalf of their child. A school's access to information about a child held by the Ministry (e.g. ENROL, NSI), or the wider education ecosystem (other schools, other education agencies such as NZQA), is directly related to the original purpose for which the information was collected – being the delivery and administration of education to the student.

All of this happens without a student being able to exercise agency. They may simply be too young to understand there is a decision they can make. Older students may understand there is a theoretical decision that could be made; however, it is not a practical or meaningful decision given that attendance at school is mandatory for children aged 5-16. Students are expected to follow school rules, policies, and processes. Irrespective of any decisions that may be offered to a student, fundamentally there remains a power imbalance between principals and teachers as adults in a position of trust and authority; and the students themselves. Finally, even if a choice were to be offered, it would likely not be meaningful given the potential adverse impact on the student's education.

5.9.2 Student information

Schools collect data from a student, or students and teachers upload information directly to Te Rito. The Te Rito service maintains that student record which different schools are granted access to. When enrolling at a school the student will be aware that the new school is being granted access to their information within Te Rito. Particularly when students have Te Rito access.

Proactively released

There is no explicit agency or autonomy for students to subsequently decide who in the school has access to their main student record information in Te Rito. This is already the case with all other school IT systems. Access to information is managed by school organisational rules and role based access control. In Te Rito students do have the ability to decide whether their portfolio information is accessible to only themselves, or in addition to their teacher(s) or parents. They may also choose to post information to an open school group.

As noted elsewhere in this PIA, enrolment forms and privacy statements of early adopter schools are being reviewed to identify whether consent to share information with a student's next school is explicit, or whether the school relies on notification of purpose. The review will identify whether improvements could be made to school enrolment form(s) or privacy statements, to ensure that they are consistent with using Te Rito. Whether a school updates their enrolment form or privacy statements will be a decision for the schools to make, consistent with the level of detail they provide to students and parents.

Initial analysis of 700 schools shows that 71% have a specific purpose in their Privacy statement or explicit consent in their enrolment form, that covers sharing of student information with the next school. With further analysis we expect this result to trend to 92% of schools having either explicit consent sought or a privacy statement identifying sharing as a purpose.

While changes in privacy maturity progress, further reliance could be placed on;

1. From a Privacy Act perspective use is consistent with IPP 10 (1)(a) and sharing is consistent with IPP 11 (1)(a), both being directly related to the purpose for which the information was collected in the first place to enable the student's education. Sharing records to the next school enables a student's education. Similar guidance has been published by OPC in *Privacy in Schools*.
2. The existing schools focussed view of student information. In that the student record is a school record managed by a school. The purpose of Te Rito is thus to enable schools to share information about students with other schools as necessary to support the student's education, and to facilitate the sharing/disclosure of this information in a secure manner in the best interests of the child. This is consistent with Principal's obligations under section 237 of the Education and Training Act 2020. Which requires Principals to share information about a student with the next enrolled school.
3. The Ministry specifically advises parents that "*Once your child is enrolled at a new school, all their personal records will be sent from the previous one"* [sharing ref 1]. So there may be a common and reasonable expectation by parents that schools share student information as necessary when a student changes school, as part of providing education.

In the context of Health or Medical information, ensuring that accurate information is available to (shared with) new schools is critically important for schools to ensure that they are able to keep a student safe. A new school could rely on HIPC Rule 10 subrule (1)(b) or HIPC Rule 11 subrule (1)(c) – both related to the purpose of collection, or HIPC Rule 10 subrule (1)(d)(ii) or HIPC Rule 11 subrule (2)(d)(ii) – both relating to lessening a serious threat to the health of the individual.

Having collected information about a student during their time at school, there is a balance required. Between sharing too little (or no) information, as is the case for many transient or disadvantaged students today, compared with sharing too much information. Either can be detrimental for a student. Te Rito's purpose is to provide timely access to the critical contextual information, that enables kaimahi to help students in school and with their education. This informs improved responsiveness to student needs, better decision making by schools, producing better outcomes. Currently, outside of the Te Rito context, the judgement on what information to share is made by Principals. Te Rito will enable a more reliable and systematic approach to identifying the necessary information and in what circumstances it is necessary to be shared.

Proactively released

The Te Rito service has a full audit record of all actions and views that take place. If there is a Privacy Act request from a parent wanting to know who or how many school staff looked at their child's information, then this could be responded to with assistance from Edsby. School staff do not have access to the view audit log.

Anonymised student information in Te Rito will not be shared with or disclosed to third parties by the Ministry, including internally within the Ministry, except by request to the Te Rito Data Kaitiakitanga Group. An ethics review process will need to be established, alongside clarification of the authority for the Te Rito Data Kaitiakitanga Group to act for schools as a collective in considering any requests for data from multiple schools. See the previous section 5.2.2 Te Rito data guardianship on page 23 for discussion of their role.

5.9.3 Dual attendance

In considering the stated purposes for using Te Rito where a student is attending more than one school, both schools would have access to the common biographic and demographic information about the student. Each individual school would have access to the information relating to specific classes at the school. In both cases, data from each school's SMS will indicate a 'first attendance date' in the past, and Te Rito would honour updates from SMSs and provide access to the student's common information in Te Rito.

As additional data is added to Te Rito, the necessity and proportionality of this being visible to both schools will be considered and reviewed with Ngā Rau Whakatupu before implementation.

Te Rito is unable to distinguish between a valid dual attendance update, and an invalid claim of enrolment by another school if both 'first attendance date' fields are in the past. An invalid claim of attendance would be visible in Te Rito to the principal and teachers at the correct school, and ultimately the student themselves when student access to Te Rito is enabled. A correction would need to be requested by the valid school to the school making an invalid enrolment claim.

In the future additional data quality checking may be performed to implement a control enforcement point. This may include a consent field in Te Rito with business logic to allow (or deny) access to a student's Te Rito record to another school depending on parent or student consent. This could solve the 'two stage' access approval recommendation identified as **PRI-05.2.**

5.9.4 Dashboard information

Although the sLSR is out of scope for planned Te Rito deployments, existing ESR schools retain access to the Kāhui Ako dashboards. Dashboards contain only anonymous information, aggregated at the Kāhui Ako level. This will thus contain information about students from more than one school, but only between the schools within an approved Kāhui Ako.

As illustrated in Figure 5 on page 33 only the Principal and Deputy Principal roles in Te Rito have access to the Kāhui Ako dashboards. A deputy principal role might be granted to a teacher working across schools in a Kāhui Ako to enable their work, this is a role assignment decision for Principals.

When filtering is applied which would mean that information about less than five students would be in a results cohort, the dashboard returns a null (-1) result as opposed to zero (0). This prevents filtering by data attributes which return a zero result from being used to refine other filter results.

5.9.5 Kaimahi information

In the context of kaimahi information, this is available in Te Rito to other kaimahi at the school and would not be a new disclosure or sharing of that information. Basic kaimahi biographic information (name, school) is disclosed in Te Rito via the directory search capability. As noted above in section 5.6.5.12 Kaimahi information, various sources exist that publicly disclose kaimahi contact details.

Proactively released

5.10 Retention and disposal of personal information

5.10.1 Student information

The record of information about a student attending school will be retained for the duration of their schooling. For most students that is for up to thirteen (13) years. Te Rito then retains information for a further seven (7) years, in alignment with the *Schools Records Retention and Disposal Schedule* (SRRDS). As the student is not enrolled with a school, no schools have access to the information in this 7 year period. During the seven year period students or parents have a right of access to the information and would need to contact the Ministry to exercise this right. After seven years the information is deleted within Te Rito, though is retained in the backups for a further seven years. Only a few Edsby administrators with a role relevant to backup and recovery have access to the operational backups.

Where data is deleted from the source SMS, it is deleted in Te Rito. Short term information retention in Te Rito is thus dependent upon good information management practices at source within schools.

Although out of scope at this time, the ability for students or parents to directly access Te Rito after completion of secondary school is a consideration for a 'lifelong record of learning'. Options exist to allow students or parents to access Te Rito via personal logins not associated with any school. No policy or design decisions have been made on whether this will be enabled.

Te Rito performs an annual archive process, so that information directly available to students is only about their current classes and school year. Information about previous school years and classes is stored in the archive for seven years. Principals and teachers in the current school retain access to the archive.

Discovery work is progressing to consider options to provide different retention periods shorter than the default seven years. This may be applied to more sensitive information, or to more transient information such as the student portfolio or transition notes.

Although the sLSR is outside the scope of this analysis, it is intended that sLSR specific information is retained for only three (3) years as live data. On the basis that sLSR information is highly specific to current needs and older information would not be useful or accurate.

5.10.2 Kaimahi information

Retention of identifiable information about kaimahi in Te Rito is driven by their employment status with a school. Where kaimahi have left a school, their information would be updated (deleted) in the SMS and propagated to Te Rito. Some information would remain in the seven year archive, mostly likely in the context of class related activities.

5.10.3 Information in Te Rito and the Public Records Act

All state and state integrated schools are required by the Public Records Act 2005 to create and maintain processes to develop and manage their school records.

The status of Te Rito in the context of the Public Records Act is currently unresolved between the Ministry and Archives NZ. While school obligations exist to retain information about former students for up to seven (7) years, or while still operationally useful, Te Rito is not the system of record for schools. Also, once a student leaves a school, that school no longer has access to the student's information in Te Rito. As part of considering the longer term for student access to Te Rito, the status of their information will need agreeing. For example, it may be that Te Rito records are discharged to the student themselves at the point they leave school. Thus they are no longer under the auspices of the Public Records Act.

Proactively released

5.11 Transparency

Helping students and their parents understand that information collected by their school is stored in Te Rito, used by their schools, and shared with other schools as required will rely on transparency and communications in an understandable manner. Delivery in plain language that is understandable by students and plans for age appropriate formats for differing age cohorts, are a component part of the comprehensive *Te Rito Engagement and Communications Plan*. This is key to building trust and confidence with stakeholders. The high level principles for all change activity are shown in Figure 11 below from the *Change Management Strategy*.

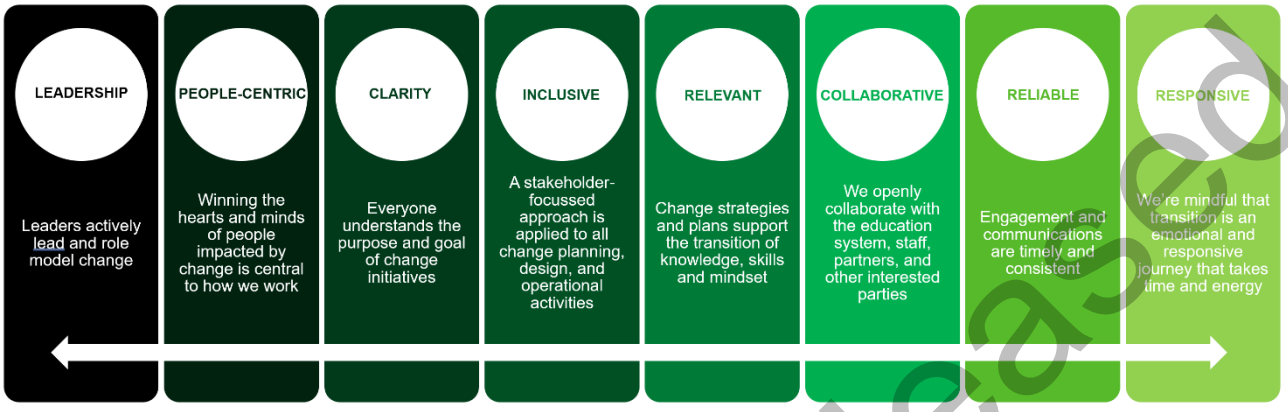


Figure 11: Change Principles

Schools will remain responsible for directly informing students and parents about Te Rito in a manner that is appropriate and consistent with existing communications. The school has the direct relationship with students and parents; and engagement with the wider school community.

The Ministry will make template material available for schools to use through multiple channels as they see fit, depending on the audience. An over focus on Te Rito as one specific digital education system, while not mentioning the other educational delivery or administrative digital systems that a school uses, may not be appropriate. Available information shows that an average primary school has ~12 educational delivery and ~20 administrative digital systems.

As noted elsewhere, enrolment form(s) and privacy statements for early adopter schools are being reviewed to identify recommendations for improvement. This may identify a need for greater clarity or transparency. Overall recommendations will inform generic guidance for future Te Rito connected schools to consider.

Irrespective of any direct school communications, the Ministry will publish information about Te Rito on the Te Rito and Ministry websites, through newsletters and other communications channels as appropriate for students, parents, and kaimahi. Beyond being in plain language and in Te Reo, other language translations of Te Rito information may be undertaken. Age appropriate formats for engaging with students of various ages will also be developed with student feedback proactively sought as part of the development. To date student feedback has helped improve the Te Rito *Privacy Statement* and *Student Acceptable Use Guidelines*. Further feedback will be sought on the plain language summary of this PIA, along with feedback from Te Reo speakers on the content of the Te Reo versions of the same documents.

The Te Rito Privacy statement will be updated when new integrations are completed, or when additional information is received from SMSs, in accordance with the content of this PIA.

By enabling Te Rito to be accessible to students, we will improve their visibility of some of the information that a school holds about them. As noted in prior sections, not all information is visible and this represents a high privacy high safety by design decision.

Proactively released

5.12 Security classification of personal information

As the information in Te Rito is predominantly about students and kaimahi and is collected by schools, no formal classification of the information is conducted at source by schools. The agreed information classification in July 2021 of Te Rito being a system holding SENSITIVE information remains valid.

This ensures that appropriate management practices and controls are implemented considering the risk associated with the significant aggregation of information in Te Rito. Aka the 'one up' principle for classifications. This is consistent with other Ministry systems that Te Rito sources data from, such as PaCT. See Assessment part 5 – GCSB Information Classification for elaboration.

This is also consistent with OPC's view that information about a child is considered sensitive (small s), and that the breach of a child's privacy would result in serious harm.

5.13 Incident Management

The Ministry has documented an Incident Response Plan (IRP) for Te Rito, augmenting Edsby's Te Rito specific IRP. The Ministry's Te Rito IRP aligns to the wider education sector cyber incident response plan that has been established to help schools with a range of security or privacy incidents. Management of a security or privacy incident may involve Edsby, the Ministry, or multiple schools depending on the nature of the incident. From a Ministry perspective any incident involving two or more schools is considered a 'major incident'. Resulting in escalation within the Ministry and potential involvement of external agencies to help.

In practical terms the Ministry would lead investigation and resolution of an potential privacy incident involving Te Rito. Including notification to OPC of the incident in the first place, so that schools are not obliged to notify OPC. Stakeholder communications would be made to schools, within the Ministry, and to external stakeholders such as OPC, National Cyber Security Centre (NCSC), NZ Police, Netsafe, IDCARE etc. Using the NCSC categorisation of incidents, a large scale compromise of Te Rito would probably be categorised as a C4, perhaps a C3 incident. The Ministry would also lead any public notifications and communications relating to the incident.

Schools would be responsible for directly notifying any effected staff, students or parents. Primarily because schools hold the contact details for those individuals, it would be impractical for the Ministry to individually notify effected individuals in a timely manner. Secondly, schools hold the day to day relationship with staff, students and parents. Beyond public notification and communications by the Ministry, it is appropriate that schools advise their communities in a manner and to a level of transparency to address concerns.

A small incident may involve the compromise of the email account for a member of school staff. Email account compromise within a school context would be the school's responsibility to notify OPC, if it reached the threshold for a notifiable privacy breach. This sort of incident would not be known by the Ministry or Edsby unless the school notifies either party. Once notified, the Ministry and Edsby would investigate whether email account compromise subsequently resulted in a breach of privacy of information held within Te Rito.

Responsibilities between schools and the Ministry are clearly and succinctly described in the *Te Rito Privacy Statement*. The most important step being advising the other party of a suspected incident so containment actions can take place. Further detail is elaborated in the *Te Rito Terms of Use* and *Te Rito IRP*.

Proactively released

5.14 Additional analysis and assurance

5.14.1 Safer Technology for Schools assessment (Australia & NZ)

Pending formal assessment of Edsby by Safer Technology for Schools (ST4S), Te Rito had been reviewed by the Ministry against the ST4S readiness check to determine alignment with the required criteria for its functions and service tier. Of the sixty-five (65) questions in the readiness check, nineteen (19) are specifically about privacy considerations. A number of other questions relate to privacy, e.g. information security controls that would relate to IPP5.

Edsby has now been successfully assessed by ST4S and joined the ST4S Product Badge Program as of August 2024. This provides assurance against an independent benchmark that Edsby has appropriate controls in place for its purpose. Edsby is considered a Tier 1 service for both the data stored and functionality offered.

5.14.2 Common Sense Privacy Programme (US)

The US based Common Sense Privacy programme assesses education technology against good privacy and security practice. Edsby was last reviewed in February 2023, with a Pass in the Basic evaluation with a score of 95%. Edsby – Privacy Evaluation (commonsense.org).

The comprehensive review scores Edsby at 65%. Edsby – Full Privacy Report. A perfect privacy score of 100% is not achievable as the Edsby service complies with legal requirements (responding to lawful warrants), performs identity verification checks, is intended for use by students under the age of 13, and students can upload their own content. These factors, and others, result in not achieving a perfect privacy score of 100%. It is debatable whether any system could achieve a 100% perfect privacy score, especially given a legal need to comply with lawful warrants.

The comprehensive review has some gaps which represent a lack of information in Edsby's publicly available security and privacy policies, while other gaps represent the semi-automated nature of Common Sense's assessment of publicly available information. All of the gaps have been reviewed, none of them are a concern for the Ministry or education sector using Te Rito. E.g., in the full report section 8.8, Common Sense are unclear about security compliance audits, yet Edsby hold an ISO27001 Certification which includes audits. In section 10 Advertising, Common Sense note uncertainty about filtered advertising, yet Edsby are clear in multiple different statements including their Services Privacy Policy there is no advertising to students.

5.14.3 Age Appropriate Design Code (UK & International)

The UK ICO's Age Appropriate Design Code (AADC) represents a generally agreed standard of best practice when dealing with services likely to be used by children, that is increasingly being used as the foundation for new legislation in numerous countries. The Institute of Electrical and Electronics Engineers (IEEE) has defined an industry standard based on the AADC, IEEE-2089 *Standard for an Age Appropriate Digital Services Framework*. The only formal certification available against the AADC at this time is for age verification technology used on websites.

In lieu of an independent assessment option, the Ministry has reviewed the AADC and associated Children's code self-assessment risk tool, to self-assess whether Te Rito would likely meet AADC requirements. The full analysis is described in section 6.1.2 *Age Appropriate Design Code analysis* on page 70.

The main area of partial compliance relates to data minimisation. The objective of Te Rito is to aggregate in one system the disparate information held about students in numerous other, often inaccessible, systems. And to ensure that information remains available to a student through different schools. Co-design with Ngā Rau Whakatupu is identifying the most important information for school kaimahi to help students in their best interests.

Proactively released

6 Assessment part 2 – Privacy Principles' analysis

6.1.1 IPP Analysis introduction

This assessment is of Te Rito against the 13 Information Privacy Principles (IPPs) in the Privacy Act 2020. The Information Privacy Principles are summarised in Appendix A. Te Rito's objective is succinctly described as:

> *"It is critically important to protect the privacy and security of our learners' information whilst ensuring that the right people have access to it, for the right purpose, at the right time."*

In achieving that objective there is a balance required between having too little (or no) information, as is the case for many transient or disadvantaged students today, compared with collecting, sharing, or retaining excess information. Either can be detrimental for a student. Te Rito seeks to provide timely access to the critical contextual information that enables Kaimahi to help students in school and with their education. This informs improved responsiveness to student needs, better decision making by schools, producing better outcomes for all. As identified previously, the judgement on what information to share is currently made by Principals. Te Rito will enable a more reliable and systematic approach to identifying which information is appropriate for sharing.

This PIA is deliberately wide, covering the different types of information that have been identified by Ngā Rau Whakatupu as necessary information to help student's education during changes of school or teacher. Not all the identified information will be stored in Te Rito immediately from all schools for all students. The IPP analysis below considers the range of information currently and planned to be in Te Rito, relying upon source systems having performed their own analysis for collection in the first place.

Discovery and evaluation work will be required to qualify and consider whether all the identified information is useful, necessary, and beneficial. This work will meet the criteria defined by OPC for a proportionality test. By necessity evaluation work can only be done with schools using real information about students to confirm the anticipated benefits. Through the discovery and evaluation work *some* schools will start storing in Te Rito *some* of the information identified in the following sections.

Data minimisation, only collect the minimum information that you need for well defined purposes, is a core privacy by design principle. Schools necessarily collect significant quantities and varieties of structured and unstructured information about students for broad purposes described as educational delivery or school administration. Te Rito implements input filtering so that only specific mapped fields of data from an SMS are stored in Te Rito. This is effective for fully structured data and will always be less effective for unstructured data such as freeform notes fields or attachments.

Te Rito also implements comprehensive Role Based Access Control to ensure that only the right people have access to information in Te Rito, related to their role in the student's education, at the time they are involved in their education. Training is being provided to Kaimahi in how to use Te Rito safely and effectively. Beyond authorised users, Te Rito implements robust information security protections minimising the risk of technical issues leading to a privacy or security breach. Te Rito has been assessed against multiple different assurance frameworks, including formal certification against ISO27001. It will continue to be assessed against evolving frameworks, such as the Age Appropriate Design Code.

Proactively released

Table 9: Privacy principles related to collection of information

IPP	Assessment against Privacy Principles	Compliance	Risk[7]
IPP1	Information should be collected for a lawful purpose; You should only collect the personal information that you need		
	Under the authority of the Education and Training Act 2020 (ETA) and other legislation, schools collect a wide variety of information about students for approved educational purposes. Most of this information is stored in Student Management Systems (SMS), and in associated Ministry systems such as ENROL. As part of day-to-day collection of information schools have a variety of optional assessment tools available, such as e-asTTle and PaCT, where collected data is also stored. In addition, schools collect and submit to the Ministry applications for funding relating to additional support students may have, e.g., reading recovery, resource teachers for literature or maths, English for Speakers of Other Languages (ESOL). Schools similarly collect information about parents, in the context of their relationship to the students, and kaimahi in the context of their employment. Parents are able to decline to give a school some information, such as multiple contact details, although basic information such as home address and an emergency contact are necessary. Information stored in Te Rito about kaimahi is minimal and in context. E.g., HR information is not stored. Te Rito stores information that is already being collected by schools, either in an SMS or other IT systems, or directly uploaded by Teachers or Students. The purpose for which school boards will use the information in Te Rito is to support the student's education. This purpose is consistent with one of the purposes for collection by schools. This purpose will need to be transparently communicated by schools and the Ministry to students and parents, preferably at the point of collection by the school. By aggregating information originally from multiple schools into a single national repository, some over collection (or retention, see IPP9) may happen compared with the information being simply left in the former school's SMS and not shared with a new school when a student changes schools. Te Rito's purpose is to prevent useful and necessary information from being inaccessible to new schools, which currently has a detrimental effect on students. A core assumption in this analysis is that school Boards ensure their schools are following guidance provided by the Ministry and peak bodies including New Zealand School Trustees Association (NZSTA), NZ Principals Federation (NZPF). That schools are collecting PI in a manner consistent with the Privacy Act and the ETA. That students & parents are appropriately informed of the purpose and necessity to collect information; processes to collect the information are not intrusive; and that forms (online or paper based) and school Privacy policies or statements clearly articulate these topics. The majority of school enrolment forms seek consent to share student records when they change school, or rely upon a Purpose statement in their Privacy policy. Beyond sharing student information to subsequent schools being an expected and lawful purpose. The Ministry specifically advises parents that *"Once your child is enrolled at a new school, all their personal records will be sent from the previous one"* [sharing ref 1]. There is likely a reasonable expectation by parents that schools simply do this as part of providing education. Given the disparity in labels/fields that different SMSs apply to attributes, and each school's use of different labels/fields, Te Rito performs a data mapping to ensure that attributes are consistently displayed in Te Rito. If schools are collecting excess information in their SMS, Te	**Compliant**	**P-01** **P-10**

[7] Risks TR-xx are risks identified in the information security risk assessment; risks P-xx are risks identified in Part 3 of this PIA.

Proactively released

IPP	Assessment against Privacy Principles	Compliance	Risk[7]
	Rito has the ability to filter out unnecessary attributes from being retained in Te Rito. There is a risk that a common field is used inconsistently, thus unnecessary or excess information is retained in Te Rito from some schools. Privacy risk **P-01**. Where SMSs have a 'pre-enrolment' flag or future enrolment data associated with a student record, Te Rito recognizes this and does not populate or currently make visible the information in Te Rito for that student to the school claiming a pre-enrolment. Where SMSs do not have a 'pre-enrolled' flag, and schools pro-actively add students with a current enrolment data who are not currently enrolled, then this pre-enrolment scenario may appear as a dual enrolment in Te Rito. Privacy risk **P-10.**		
IPP2	You should collect information directly from the person (unless an exception applies)		
	Te Rito will receive information that the school has already collected directly from the student, or their appropriate representative (e.g., parent, guardian, kaimahi). Some information collected by schools from students or their parents is already shared with the Ministry for a number of purposes that are mandated by the Education and Training Act. It is common sense that parents or guardians often act for children that they are responsible for, and as stipulated in law under Care of Children Act 2004 Section 17 *Child's father and mother usually joint guardians*. Parents are often consenting to collection of information on behalf of their child. Where the child is unable to understand their own privacy interests, the parent can make an informed decision on whether information sought about the child is necessary for the purposes identified by the school, has their consent, is non-intrusive, is accurate and kept up to date. Obligations under the ETA stipulate that a parent or guardian are responsible for ensuring records that schools and the Ministry hold about their child are correct at the time of enrolment. Schools or the Ministry are responsible for keeping this information up to date and accurate, per IPP7. Beyond the common-sense that parents often act for their children, it is possible from a Privacy Act perspective IPP2 exception (2)(a) or (f) could apply to collection of information. This is consistent with previous analysis for SDEX in 2006, which identified that "*to avoid duplication* [within the education ecosystem, schools sharing information via the Ministry] *is unlikely to prejudice the interests of the person concerned*". Te Rito will receive other information directly uploaded (saved) by the student themselves. Which might otherwise be saved in the schools IT Services such as Microsoft 365 for Education or Google Workspace for Education. Saving information in Te Rito is, of itself, not a new collection of new information by the school. Schools will collect information about parents directly from one or both of the parents. Principals or teachers may also add other freeform text, e.g. about extended whānau or guardians. Schools will collect information from kaimahi directly related to their employment by the school. Only a necessary sub-set of that information is stored in Te Rito. No material Privacy risk was identified in relation to the collection of information by schools that would be stored in Te Rito. There is a touch point with risk **P-02** – Schools transparency with students.	**Compliant**	**P-02**

Proactively released

IPP	Assessment against Privacy Principles	Compliance	Risk[7]
IPP3	You should let people know that you are collecting personal information, what will be done with it, and what their rights are		
	Use of Te Rito is opt-in for schools. Schools or the Ministry will not be expressly seeking consent from each student, their parent, or kaimahi as it will not be practical for schools to seek explicit consent for the purpose of storing or saving information in Te Rito. This would qualify under IPP3 exceptions (3) or (4 (a) & (d)). Te Rito stores information that is already being collected by schools, and information that is directly saved. Te Rito is used by schools for the purposes of educational delivery and school administration, just as schools use other IT services for the same purposes. Irrespective of an IPP3 exception applying, the Purpose for storing the information in Te Rito is directly related to the original purpose for collection. Depending on the outcome of the Privacy Act amendment to address indirect collection, the Ministry may need to further clarify (on behalf of schools) Te Rito's status as a schools' system not a Ministry system. Thus, does not represent an indirect collection. Schools may also need to notify the onward sharing of collected information to other schools, the 'front loading' approach. A comprehensive *Engagement and Communications Strategy* and *Plan* has been developed, articulating the benefits that use of Te Rito will bring for students, kaimahi, and schools. Once a school expresses an interest to opt-in further onboarding specific communications and planning will be conducted with the school. This will include templated communications that can be shared with stakeholders such as students, parents, School Board of Trustee's etc. Schools will be able decide what is appropriate for them to share with students, parents and their communities in a manner consistent with existing school communications. Communications will ensure that the school and Ministry are transparent with all stakeholders on the purposes for using the information stored in Te Rito. Even though this is information that the school already holds and, in many instances, shares with the Ministry for other purposes. The planned Privacy Brief analysis for schools, will likely identify recommendations to schools that they actively inform students and parents on the use of Te Rito. For the deployments during 2024, the Te Rito project team is reviewing enrolment forms and Privacy statements for early adopter schools. This will identify any recommendations for improvement or clarity. Analysis of over 700 schools has identified that 71% of schools identify sharing to the next school within their privacy statement, or on their enrolment form with explicit consent to this provided by parents. Further analysis is expected to see this trend to 92% of schools. Recommendations for improvement may include being more explicit about consent on the enrolment form, rather than relying upon purpose statements in additional privacy policies; Or seeking explicit consent for the new school to access the student's Te Rito information; Or a need to clearly articulate the schools choice to store information in Te Rito (which may also address the proposed Privacy Act changes relating to indirect collection); Or potentially elaborate the schools use of Te Rito beyond general 'educational purposes'. The project team will provide specific guidance to early adopter schools and develop more generic guidance applicable to any school. Specific guidance will include whether existing school enrolment form(s), Privacy statement(s) or policies may need updating. Generic guidance will be included as part of an onboarding readiness checklist, as part of the engagement and communications plan. Whether a school updates their enrolment form(s) or privacy statements will be a decision for the schools to make, consistent with the level of detail they provide to students and Parents. Privacy risk **P-02**, **P-12, P-15, P-17.** A Privacy brief analysis template focussed on Te Rito will be developed to help schools in assessing their specific Privacy controls, and approach to informing parents & students about the use and sharing of information via Te Rito.	**Compliant**	**P-02** **P-12** **P-15** **P-17**

Proactively released

IPP	Assessment against Privacy Principles	Compliance	Risk[7]
	The use of information in Te Rito is consistent with the purposes for which the information was collected by schools through enrolment processes and day to day education delivery. A Privacy risk (**P-02**) was identified in relation to schools informing students, parents and staff in a transparent manner at the time of collection about the storage of information in Te Rito and future sharing with the next school (**P-15, P-17**). If a school does not socialise in a transparent manner that information stored in Te Rito is accessible to a new school at pre-enrolment time or after a change of school, then students, parents or staff may feel they have not been appropriately informed on one of the uses for which schools store information (**P-12**).	**Schools potentially non-compliant**	
IPP4	Information should be collected lawfully, and in a fair and reasonable manner		
	Existing purposes for schools collecting information are lawful in terms of the Education and Training Act 2020. Existing business processes for education providers to collect information, either at time of enrolment or during day-to-day educational delivery, will not change. Schools' opt-in to use Te Rito, therefore schools are actively choosing to store the information with the Ministry and Edsby as an agent. Per IPP2 above, collection of information at school enrolment time will either be from parents, who are acting on behalf of their children and are able to make an informed assessment of the relevance of information sought; or from older children who may provide this information themselves. Students may themselves directly upload information to Te Rito, it is implicit that this is reasonable otherwise the students would not engage or participate. To avoid unnecessary re-collection from the student directly, sharing of the information from a school's SMS and Ministry systems is fair and reasonable given that one purpose for collecting the information about students in the first place is to support their learning and engagement in the education system. The existing collection is also with a trusted figure of authority in a school, rather than via an anonymous webform with no trust relationship or of questionable provenance. Schools are, obviously, experienced with gathering information about children either directly or from parents in a manner that is fair and reasonable. Education providers have varying levels of openness and transparency when collecting information as to the intended purpose and use. Few education providers give specific detail (e.g. exactly which third party applications they use and thus information is stored with, whether information sharing is mandatory or optional). The majority of education providers only provide higher level purposes for use (e.g., education purposes, school administration, communications, measuring student achievement, sharing with the Ministry). Potential use of the Capture app, as a low friction option for younger students, could result in more likenesses of young children being stored than the mandatory school profile photo. Young children are unlikely to understand potential privacy consequences. Teachers should be using professional judgement as to when to use the Capture app and what to save to Te Rito. Potential risk **P-18**. This is a decision by each education provider as to what is appropriate or reasonable for their students and parents. At no point is biometric information required to be collected by education providers to use Te Rito. A profile photo is supported in Te Rito for students, parents and staff. It is a school decision as to whether that is shared from the SMS or not. Though everyone would have the ability to opt-out. Te Rito does not collect anonymous information to build a profile of any users.	**Compliant**	**P-18**

Proactively released

Table 10: Privacy principles related to protection of information

IPP	Assessment against Privacy Principles	Compliance	Risk
IPP5	Information should be protected from loss, unauthorised use, access, and disclosure		
	A comprehensive security and risk review of the current state Te Rito solution is part of the Ministry's Certification and Accreditation (C&A) process being performed for the 2023/24 deployments. This PIA is part of that review. **P-03** is representative in this PIA of the risk of ineffective or insufficient security management. The C&A scope includes policies, processes, procedures, and technical security controls relating to Te Rito and obtaining assurance of the same from Edsby for their service management functions. Edsby hold ISO27001 Certification for their Information Security Management System. This independently audited industry standard certification provides a significant level of assurance, above and beyond attested privacy pledges. There is always a risk of a technical fault, **P-07**. As part of the overall service management plan, reporting will provide assurance to Ministry stakeholders that Edsby are operating Te Rito to the required standard. Business reporting will provide all stakeholders including Ngā Rau Whakatupu, education providers and peak bodies, assurance that overall service metrics are meeting objectives as well as providing an overview of service utilisation. Key security metrics have been identified and will be included in operational and business reporting. The Education Sector Logon (ESL) service is the only authentication mechanism to permit Kaimahi to access Te Rito. ESL is a common platform that supports multiple education applications. ESL identifies which school an individual is associated with and in some cases identifies their role (principal, teacher, etc.). Role Based Access Control (RBAC) is managed down to the individual field level by Te Rito, with permissions to view or update information about staff and students assigned to specific roles. RBAC is enforced at the class level, so teachers can only view information about students in their classes. RBAC can be assigned for temporary Teachers, with automatic deprovisioning of access. Te Rito performs automatic kaimahi deprovisioning based on updates from the schools SMS. Role assignment is performed by each school's Principal or delegated administrator. Role assignment in Te Rito will be monitored by business reporting. This will identify any deprovisioning in ESL that may be required for staff that leave a school. ESL access administration is performed by schools. Each software release performs RBAC testing as part of the test suite, this is checked by the Ministry to ensure no unforeseen permission changes to any role. Te Rito implements real time server-side access control validation, so that if any user's role (or active status) changes including during a session, the prevailing access permissions are enforced for each view or update transaction. Full audit logging is enabled in Te Rito. This tracks all updates made by any users, with some updates then being visible to students and parents under 'notifications' e.g., where a teacher posts a test result. Other updates from the audit log are only visible to the Principal of a school in the Student profile Admin view, e.g., teacher changed a grade. This audit log also provides Edsby privileged administrators with logging data about all 'user views', e.g., which students a teacher has viewed information about. The 'user view' log is not accessible to any school staff.	**Compliant**	**P-03** **P-04** **P-07** **P-08** **P-09** **P-14**

Proactively released

IPP	Assessment against Privacy Principles	Compliance	Risk
IPP5 cont.	For student access, federated authentication from each school's own identity provider is required. The Microsoft 365 for Education or Google Workspace for Education that students use on a day-to-day basis to access their school network and applications. To use Te Rito adult users must agree to abide by the Terms of Use. These are presented as a 'tick to accept' option at first time login. They are also available in English and Te Reo on the Te Rito website Terms of use|Te Rito. Terms of use for students have been developed, more akin to an acceptable use agreement or digital citizenship agreement promoted by Netsafe for schools. A Service Agreement for schools (as an organisation) to accept in addition to individual user acceptance of Terms of Use will be provided to ensure that schools are clear on their different roles and responsibilities compared with the Ministry or Edsby responsibilities. School (and any MoE) staff accessing Te Rito are expected to complete the Te Rito Privacy training module. This is made available on the Education Sector and Ministry internal Learning Management Systems (LMS). Completion will be tracked and reported on to Te Rito Data Kaitiakitanga Group at an aggregate level to inform key risk indicators. The Te Rito training module is also publicly available on the Education Sector LMS for students and Parents to access. There is no obligation for students or Parents to complete the Privacy training module. Work is underway to include OPC's *PrivacyABCs for Schools* training module in both LMSs, which will have completion reporting in place. Further planned work includes the concept of 'Privacy touch points' in Te Rito user training guides. The Ministry is not directly responsible nor accountable for all the information security protections in Schools or School IT systems. School systems may not have equivalent or sufficient information protections **P-04**. Te Rito does contribute to risk reduction, by reducing the sharing via email or cloud storage of student information. Reducing instances of human error or the use of email are positive outcomes to prevent privacy breaches. Despite codes of professional conduct, Terms of Use, or training, there is always a risk that an authorised user performs unauthorised actions **P-08, P-14**. This could include exporting identifiable student information. In Te Rito export or download of a partial or full student record is prevented. Specific aggregated datasets (e.g., all assessments) that may include identifiable student information (e.g., NSN) is possible. Even where an export is only of structured data and does not include identifying biographical information, storage of the NSN as part of student records could make an otherwise de-identified data export identifiable if correlated with other systems **P-09**. E.g., the NSI is searchable on the NSN alone. Alerting for anomalous or suspicious activity is being established for Te Rito. Though malicious intent cannot be identified from valid and authorised activity. In the Ministry's overall digital strategy are several initiatives to help schools with their cyber security including Te Mana Tūhono, Cyber Security and Digital Support for Kura and Schools programme (CSDS), Network for Learning (N4L), Safer Technology for Schools (ST4S), Assurance Framework for Schools. Some initiatives implement preventative controls that protect information, others will implement detective or responsive controls to identify and help mitigate a security incident impacting education providers should that happen. In practical terms the responsibility will remain with Schools to implement appropriate protections and follow guidance.		

Proactively released

Table 11: Privacy principles related to accessing and correcting information

IPP	Assessment against Privacy Principles	Compliance	Risk
IPP6	An individual should have access to their information		
	Schools are responsible for handling requests for access to personal information held in school systems, including Te Rito. The business process for this and how timely schools respond may be a risk **P-05**. In the future students will have access to Te Rito and will be able to view more of the information that schools currently hold about them in disparate systems, along with basic demographic information held about their parents. This represents an improvement on the current limited direct access to information held. In Te Rito particularly sensitive information, such as Behavioural or Health information, is only visible to limited Kaimahi roles and is not visible to either students or their parents. This represents a default high privacy and high safety by design consideration. Health information may be generally known by family and friends at school, e.g., eczema, or may be highly private, e.g. diagnosis of a serious illness. Parents and students retain a right of access, which would have to be facilitated by their school. Where a student is no longer at school and requests access to their information from their most recent schools, that school would need to request assistance from the Ministry and Edsby to provide a copy of information held in Te Rito. In Te Rito some subjective information such as teacher observations, will not be visible to students unless they are included in a formal progress report. This partial visibility of subjective or evaluative information is part of the access request risk **P-05**. Noting that this is an existing consideration for schools where not all information is currently accessible to students, nor necessarily stored in an SMS. School staff will have visibility of information held about them in Te Rito. While some school staff who do not have access to their school's SMS may have access to Te Rito, thereby increasing their visibility and access.	**Compliant**	**P-05**
IPP7	Information should be corrected if a person tells you that it is wrong		
	Information in Te Rito sourced from a schools SMS will need correcting at source by the school if there are any inaccuracies. This applies for students, parents, kaimahi. Where the SMS may not support a correction, corrections could be made directly within Te Rito by the Principal. Information in Te Rito sourced from Ministry systems will bring improved visibility to students, who can then request updates as appropriate via their school or with the Ministry. Information directly uploaded or inputted to Te Rito by schools would need updating in Te Rito. Once student or parent access is enabled, the improved visibility of information for students and parents will enable more timely correction of inaccurate information. Where there is disagreement about subjective information, a Statement of Correction may be added by the school in the SMS as free form text or an additional attached document. Where a free form text field is separate from the related structured data in the SMS, Te Rito may discard the freeform notes or an associated attachment as the structured data they relate to is not obvious. This is a high safety high privacy by design aspect, to avoid potentially sensitive data in a freeform notes field from being inadvertently disclosed to a wider audience. However, Te Rito would thus not present to users the requested correction and the reasons for it not being made, **P-05**. A Statement of Correction can be saved directly in Te Rito under student related documents, ensuring it is accessible to the next school. Use of freeform notes fields in SMSs and Te Rito, along with handling of attachments from SMSs requires further analysis.	**Compliant** **Partially Compliant**	**P-05**

Proactively released

Table 12: Privacy principles related to relevance and retention of information

IPP	Assessment against Privacy Principles	Compliance	Risk
IPP8	Personal information should be accurate, complete, up to date, relevant and not misleading before you use it		
	By providing a single view of the student in Te Rito comprised of information from multiple different systems, the most complete, up to date and accurate information is available to Te Rito users. This will help schools to identify when information is missing, e.g. funding for additional teaching support. This removes potential gaps that might otherwise be detrimental for the student or may result in detrimental outcomes for students. Te Rito will perform data quality and integrity checks against Ministry systems including ESL and NSI, to ensure accuracy of information about kaimahi and students. As noted for IPP7 Schools will remain responsible for ensuring that information about students and parents is kept up to date in SMSs and synchronised to Te Rito. It is an existing risk that schools do not perform updates in a timely manner, or that updates to various Ministry systems are not synchronised. As discussed in IPP9 - from a school's perspective in Te Rito and in dashboard views, a deceased person would be treated as if they have left the school. Their information would not be displayed even in de-identified form. Te Rito will rely on matching with DIA's register of Births, Deaths and Marriages performed by NSI, and updates to the SMS by schools, to update information about deceased students. No material Privacy risk was identified in relation to Te Rito holding accurate, complete or up to date information, beyond the existing risk relating to schools not keeping accurate records.	**Compliant**	**n/a**
IPP9	Personal information should only be kept for the period for which it is required		
	Existing Schools Record Retention and Disposal policies set by the Ministry and Archives NZ apply to Te Rito. Core student biographic information is retained throughout a student's journey through the education system, usually up to thirteen (13) years plus seven (7) years further retention. Other information relating to classes, such as assessment results, is retained for the time they are considered operationally useful by a school and by default no longer than seven years. Where information is deleted in the SMS, it would be deleted in Te Rito. Te Rito retains a backup copy for up to seven years after deletion. For information directly related to classes, the 7 year archive +7 year backup retention duration may be more than is strictly operationally necessary **P-11.** This is a Ministry accountability to manage for Te Rito. Note schools do not directly 'retain' the student record in Te Rito, their access to student records in Te Rito is determined by whether a student is enrolled with the school or not. Te Rito currently has little flexibility in automatically managing for how long different types of information are retained. While manual deletion is possible, this also introduces a risk of human error. Work is underway to explore different retention periods for different types of information.	**Compliant**	**P-11**

Proactively released

IPP	Assessment against Privacy Principles	Compliance	Risk
IPP9 cont	By aggregating information originally from multiple schools into a single national repository, over retention may nominally be seen compared with the information being held only by the former school and being inaccessible to the new school. Existing practices mean that necessary and relevant information is not reliably transferred to a new school. While being retained by the former school in their SMS for up to seven years. This has a detrimental impact on students. Te Rito's purpose is to ensure necessary information is available in a timely manner to schools. There will always be a balance between retaining useful information and disposing of unnecessary information. Too much or too little information can both be detrimental or harmful. Te Rito performs an annual archive process, so that information directly available to students is only about their current classes and school year. Information about previous school years and classes is stored in the archive for seven years. Principals and teachers in the current school retain access to the student's information in the archive. Another Te Rito nuance to be considered is the status of a student's class specific information after seven years. Irrespective of archiving processes, should information be 'discharged' to a student every year? With guidance provided to export (download) a copy of the information they want to keep. Core biographic and achievement information is retained within Te Rito while a student is at school. Should students retain direct access to Te Rito after school or if they have moved abroad? A Disposal Authority that considers the nuances of Te Rito needs to be developed and agreed. Retention of information about deceased people, especially children, is a very sensitive topic where different families will have differing expectations. Parent choices will be actioned by the school and updates will flow to Te Rito. Te Rito has flexibility to not display information about deceased children to parents if that is their decision. Parents may not wish to see a deceased child's photo when dealing with schooling for other children. Information about kaimahi will only be retained within Te Rito as long as they are employed by the school. Automatic deprovisioning of access to Te Rito driven by SMS updates takes place, which actions deletion.		

Proactively released

Table 13: Privacy principles related to use and disclosure of information

IPP	Assessment against Privacy Principles	Compliance	Risk
IPP10	Personal information should only be used for the purpose for which it was collected, unless an exception applies		
	Per IPP1 analysis of this IPP is noted as Compliant given that education providers already collect personal information for the main purposes of enrolment, provision of education to students, and other purposes including sharing necessary information to the next school a student attends. Te Rito's purpose is to enable the information about ākonga and students to follow them throughout their education in a secure and accessible manner. Where onward sharing or access is not explicitly consented or identified as a purpose by schools, reliance could be placed on IPP10 (1)(a). Where one of the purposes for collecting information is to enable the student's education, and sharing the information with a subsequent school is directly related to that purpose. Parents may consider the information collected by schools is implicitly necessary for education purposes, expecting it to be shared when their child attends a new school. The Ministry specifically advises parents that "*Once your child is enrolled at a new school, all their personal records will be sent from the previous one*" [sharing ref 1]. So there is likely to be a common and reasonable expectation by parents that schools simply do this as part of providing education. As discussed in IPP11 below and in section 5.9 Disclosure and sharing of personal information on page 49, the majority of schools include sharing of information when a student changes school as one purpose to which the collected information will be used. Some schools are not this explicit (Risk **P-15**)**.** A Privacy brief analysis template focussed on Te Rito will be developed to help schools in assessing their specific Privacy controls, and approach to informing parents & students about the use and sharing of information via Te Rito. Whether schools clearly articulate to students and their parents the purpose for collecting information, or how much is mandatory for enrolment purposes vs. necessary for broader educational purposes, is ambiguous and outside the scope of this PIA. Risks **P-01, P-02**. A Service Agreement for schools (as an organisation) to accept in addition to individual user Terms of Use will be established to ensure schools are clear on their roles and responsibilities. Per IPP3 and section 5.11 on Transparency the *Te Rito Engagement and Communications Plan* includes publication of information about Te Rito in the public domain to resolve possible gaps or clarify potential ambiguity. Per IPP5 there is always a risk that an authorised user performs unauthorised actions **P-06, P-08, P-14**. Ministry staff do not have access to Te Rito, with the exception of staff providing technical support to ensure data integrity, security and safety. Any Ministry staff access would be subject to audit review and part of regular reporting to the Te Rito Data Kaitiakitanga Group.	**Compliant**	**P-01** **P-02** **P-06** **P-08** **P-14** **P-15**

Proactively released

IPP	Assessment against Privacy Principles	Compliance	Risk
IPP11	Personal information should only be disclosed for the purpose for which it was collected, unless an exception applies		
	Analysis of this IPP is noted as Compliant given that education providers already collect personal information for the purposes of enrolment (administration), provision (delivery) of education to students, onward sharing to the next school, and other purposes. Information handling within a school that relates to the purpose for collection does not constitute a disclosure. Te Rito will not change that. When enrolling at a school a student or their parent is providing consent for that school to access the student's information in Ministry systems such as ENROL and the NSI. Thus receiving a disclosure. This business process may be opaque to students or parents. Or students and parents may have an understanding of education business processes from various sources of publicly available information. Part of this business process is for the school to then store additional information about the student in school systems, along with updating Ministry systems. Schools use multiple different systems, and it is not practical for a school to offer a choice about which systems will store student information. Te Rito is no different. There is no unauthorised disclosure or sharing by the student's former school to their new school in the Te Rito context, since access is authorised by the business process of enrolment. A use for onward sharing is identified. Use is directly related to one of the purposes for which the information was collected, thus exception IPP11(1)(a) applies. The same as happens with ENROL or the NSI. Analysis of a sample of enrolment forms and privacy statements from ~700 schools shows that 71% of schools already address their Privacy Act obligations in the context of sharing information. Further analysis is expected to see this trend to 92% of schools. Guidance for schools in the context of access to a student's record within Te Rito will be developed. A Privacy brief analysis template focussed on Te Rito will be developed to help schools in assessing their specific Privacy risks and controls, including approach to informing parents & students about the use and sharing of information via Te Rito. This will help further mitigate risk **P-15**. In lieu of explicit purpose statements or consent on enrolment forms about schools sharing or being granted access to the Student's Te Rito information, application of IPP11(1)(a) exception, reliance could be placed on: a) Principal's obligations under section 237 of the Education and Training Act 2020. Which requires Principals to share information about a student with the next enrolled school, or b) Public information from the Ministry specifically advising parents that "*Once your child is enrolled at a new school, all their personal records will be sent from the previous one*" [sharing ref 1&2]. In any case, there is likely a common and reasonable expectation by parents that schools share necessary information with the next school as part of providing education. Whether the legal basis for existing information sharing by schools needs clarification, Te Rito being a part of that, will be considered by the Ministry. Risk **P-17**. Te Rito enforces access controls so that kaimahi who have no specific need to see detailed information in Te Rito about students do not. Teachers will have visibility of detailed information about students in their class only, not broad access to all information about all students in the school. This Role Based Access Control mitigates a potential risk of broader disclosure or use outside of purpose (IPP10). However, per IPP5 there is always a risk that an authorised user performs unauthorised actions **P-06, P-08, P-14.**	**Compliant**	**P-01** **P-06** **P-08** **P-13** **P-14** **P-15** **P-17**

Proactively released

IPP	Assessment against Privacy Principles	Compliance	Risk
IPP11 cont	The Te Rito privacy statement and user training emphasize the requirement to only share or disclose information held in Te Rito for the purposes it was collected. In addition to this, the Kāhui Ako Privacy Protocol makes it clear that the anonymous information provided for the operation of Communities of Learning can only be used for the purpose for which it was collected and can only be used for another purpose with the permission of the school(s) that provided the information. The (Kāhui Ako) Communities of Learning Privacy Protocol can be found in Appendix One of the Community of Learning Guide for Schools and Kura. In the context of Health or Medical information, ensuring that accurate information is available to new schools is critically important for schools to ensure that they are able to keep a child safe. A new school could rely on disclosure or sharing as being in scope of HIPC Rule 10 subrule (1)(b) or HIPC Rule 11 subrule (1)(c) – both related to the purpose of collection, or HIPC Rule 10 subrule (1)(d)(ii) or HIPC Rule 11 subrule (2)(d)(ii) – both relating to lessening a threat to the health of the individual. When considering the different sources of funding information, this is already made available to schools. Although accessibility of the information is a problem. As funding for additional teaching assistance is associated with a student, being able to continue funding that is for the student's benefit is important to avoid detrimental impacts for students. For other Ministry data stores, such as ENROL or NSI, this information is already provided by schools to the Ministry. Re-presenting that information back to schools does not represent a disclosure. Where schools may be collecting excess information in their SMS, Te Rito by default filters out excess information from being retained in, and thus disclosed via, Te Rito in the first place. There is a risk that a common field is used incorrectly, thus unnecessary information is retained from some schools in Te Rito. Privacy risk **P-01.** Per IPP10, the potential for scope creep in the use and disclosure of information is risk **P-13.** A Service Agreement for schools (as an organisation) to accept in addition to individual user acceptance of Terms of Use will be provided to ensure schools are clear on their roles and responsibilities. OPC's view on the Ministry's Service Provider status may also effect risks **P-13** & **P-06**. The Te Rito Data Kaitiakitanga Group would be responsible for advising on any requests for access to aggregate Te Rito data, in lieu of direct Privacy Act or Official Information Act requests to individual schools. The group would consider whether acceding to any requests presents a risk of scope creep **P-13** or potential detrimental use of information. The ETA and NSN Gazette notice prohibit use of the NSN except by authorised users. Thus the Te Rito Data Kaitiakitanga Group is likely to require any potential research disclosures to be only of anonymous data with StatsNZ rules about minimum cohorts for any possible filtering applied.		
IPP12	Personal information may only be disclosed to a person or organisation outside of New Zealand if the person/ organisation is subject to comparable privacy safeguards to New Zealand		
	Under the Privacy Act 2020 s11, as confirmed by the OPC[8], where organisations are storing information offshore with a third-party IT supplier, the supplier is acting as the organisation's agent, so the storage of information is not considered an 'offshore disclosure'. The Master Services Agreement with Edsby stipulates that Edsby must comply with the Privacy Act in the performance of providing the Te Rito service. Both in relation to storage of information in Australia, and any support services provided by staff in Canada.	**Compliant**	**N/A**

[8] https://privacy.org.nz/tools/knowledge-base/view/219?t=338829_455184

Proactively released

IPP	Assessment against Privacy Principles	Compliance	Risk
	Australia and Canada are considered privacy friendly countries with privacy safeguards that are equivalent to NZ safeguards. Edsby are a signatory to the (US) Student Privacy Pledge, and beyond this their work on Te Rito and with the Ministry has provided confidence that student privacy is a core value for them. No material Privacy risk was identified in relation to the storage of information in Te Rito with Microsoft whether that is in Australia or elsewhere, or under the management of Edsby.		

Table 14: Privacy principles related to identifiers

IPP	Assessment against Privacy Principles	Compliance	Risk
IPP13	Don't assign a unique identifier unless this is necessary to carry out your functions, make sure they're right and that they're protected, and don't use another agency's unique identifier instead of creating your own		
	Te Rito is using an existing assigned unique identifier, in this instance the National Student Number (NSN), which is necessary to ensure that student records received from multiple different sources are correctly associated with the right student. This is privacy preserving by ensuring that records are accurate and up to date. However, this does introduce the risk that this consistent and unique identifier could be used to re-identify a student from otherwise pseudonymous information **P-09**. Existing provisions in the ETA section 621, Schedule 24 and associated Gazette notices, clearly identify specified users and specified purposes related to the NSN, with an offenses provision defined. This places strict restrictions on the use of the NSN, as well as a process for the Secretary for Education to authorise specified users to use NSNs via a Gazette notice. Education providers and the Ministry are specified users. In addition to this IPP13 of the Privacy Act performs a similar controlling function. Unique identifiers for staff and parents are not assigned, outside of the technical need for Te Rito to generate a Globally Unique Identifier (GUID) for database storage. The GUID is unique to Te Rito.	**Compliant**	**P-09**

Proactively released

6.1.2 Age Appropriate Design Code analysis

In addition to the Privacy Act, Te Rito has been reviewed against the fifteen (15) standards that form the UK ICO's Age Appropriate Design Code (AADC). The AADC represents a generally agreed standard of best practice when dealing with services consumed by children, that is increasingly being used as the foundation for new legislation. The ICO's *children's code self-assessment risk tool* has also been used in detail to consider applicable risks. Although Te Rito would not, if in the UK, be in scope of the AADC as it is delivered by the Ministry to schools, the analysis provides insight to potential areas for improvement. This shows full alignment with eleven (11) of the fifteen (15) AADC Standards, partial alignment with three (3) Standards, with one (1) final Standard being not applicable, as elaborated in Table 15 below.

Table 15: Te Rito AADC analysis

Standard	Description	Te Rito summary context	Alignment
1. Best interests of the child	The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child.	"*Uphold the mana of the child and their family*". The design and implementation of Te Rito has been student focussed. The benefits derived from using the Te Rito service by schools are objectively in the best interests of the child. Benefits are achieved from providing a consistent view of their educational needs and progression, in a timely manner, irrespective of school they attend or frequency of school changes. Te Rito is not a commercial service to NZ schools, though the Edsby offering to the Ministry is on a commercial basis. Te Rito is co-developed & co-governed with representatives from the education sector including peak bodies. A Te Rito Data Kaitiakitanga Group has been established, which may include youth representation.	Fully Aligned
2. Data protection impact assessments	Undertake a DPIA to assess and mitigate risks to the rights and freedoms of children who are likely to access your service, which arise from your data processing. Take into account differing ages, capacities and development needs and ensure that your DPIA builds in compliance with this code.	This PIA identifies potential risks and provides traceability to previous PIAs for Te Rito. As the intended use of Te Rito relates to student records for all school years, access to and engagement with Te Rito by students in years 1-4 may be limited. Acceptable use guidance for students in different age cohorts has been developed.	Fully Aligned
3. Age-appropriate application	Take a risk-based approach to recognising the age of individual users and ensure you effectively apply the standards in this code to child users. Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing or apply the standards in this code to all your users instead.	Te Rito is for school aged students from age 5 – 19, alongside adults where they are school staff, teachers, or parents. There are no specific features of Te Rito that are age restricted for students. The Capture app provides a limited user experience that may be more suitable for 5-8 y/o students. The age of all student users can be accurately determined based on DoB data from the SMS. Risk **P-16** is identified to consider the potential that not all content shared by all users in a school is necessarily age appropriate for the audience.	Fully Aligned
4. Transparency	The privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent and in clear language suited to the age of the child. Provide additional specific 'bite-sized' explanations about how you use personal data the point that use is activated.	A Plain language Privacy statement has been developed; Terms of Use are also in plain language. Both have been translated to Te Reo. A plain language summary of this PIA will be published. An age-appropriate summary of the privacy statement, along with an age-appropriate acceptable use guidelines for students have been developed. These will also be translated to Te Reo. More age-appropriate information in non-text form is being developed. Presenting privacy infobites at suitable privacy moments is being considered. Translations to additional languages are being considered.	Fully Aligned
5. Detrimental use of data	Do not use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or Government advice.	A precautionary principle is applied. Te Rito and the underlying Edsby service are privacy respecting, as articulated in the Edsby privacy policy and Te Rito applicable versions. There is no advertising within Te Rito. No biometric information is collected or processed. There is no automated decision making functionality. Nor automated predictive/forecasting functionality of 'future performance' based on 'past performance'. Profiles are not built of users, and geo-location information is never collected or stored for any users (neither adults or children). There is no function within Te Rito that rewards excessive use or promotes a reward for extended use. There is no payment processing function. All messages have a 'report inappropriate' function, allowing students, kaimahi or parents, to raise to the Principals attention any potential instances of bullying, offensive language etc.	Fully Aligned
6. Policies and community standards	Uphold your own published terms, policies and community standards (including but not limited to privacy policies, age restriction, behaviour rules and content policies).	Acceptable use guidelines applicable to students has been developed. This is unusual from comparative research, where there is a tendency to rely on a school having a generic 'digital citizenship agreement' to cover student use of school IT equipment and services. Ultimately it is for a school to address any Te Rito specific issues with students. They have that relationship and can consider appropriate consequences without adversely impacting the students learning at school or through Te Rito.	Fully Aligned
7. Default settings	Settings must be 'high privacy' by default (unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child).	Privacy by design in the underlying service has a default of high privacy. Experience with customer testing and feedback informs appropriate changes from this default. The various Te Rito governance groups and user groups are risk averse and keep privacy protection in mind. For student generated content, 'Student Portfolio' publication options are, 'just student', 'student & teacher', 'Student, teacher & parents'. While the default is the latter of these, this is still privacy preserving as there is no 'publish to everyone' option. One purpose for Te Rito is to encourage Parents to participate more in their child's education.	Fully Aligned

Proactively released

Standard	Description	Te Rito summary context	Alignment
8. Data minimisation	Collect and retain only the minimum amount of personal data you need to provide the elements of your service in which a child is actively and knowingly engaged. Give children separate choices over which elements they wish to activate.	Te Rito collects and aggregates disparate information about the student so that it is all available in one location. Excess information provided by SMSs is discarded. Schools' opt-in to Te Rito and there are few options for students to consent to the use of specific categories of data or not.	Partially Aligned
9. Data sharing	Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child.	Data is only made accessible to a school that a child attends, access is granted. Access is removed when a child moves school. Pre-enrolment scenarios exist and the level of visibility to information in pre-enrolment is being considered given the necessity of the use case. Data is not shared, or sold, by the Ministry or Edsby to any third parties. Except where sharing is required or permitted by law. Should a request for access to data for research purposes be made, this would be considered by the Te Rito Data Kaitiakitanga Group, and even if granted would be provided in anonymous form that could not be re-identified.	Fully Aligned
10. Geolocation	Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child). Provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others must default back to 'off' at the end of each session.	Geolocation information is not collected or stored in Te Rito. That a child attends an identified school, would by implication, identify their likely location during normal school hours on school days. However, that would be implied outside of the Te Rito service anyhow.	Fully Aligned
11. Parental controls	If you provide parental controls, give the child age-appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored.	Te Rito does not provide parental controls. Parents are instead provided with a portal, which allows parents to see school content and group messaging from school staff to their children. This is not monitoring of the child's activity, simply visibility of content about, and group communications to, their children. The parent portal provides visibility of: School news articles, student portfolio, comments on their child's portfolio by the other parent, any group/class messages from a teacher to students that are in an 'open to parents' group/class, updates by a teacher to their child's assessments, report card or grades, student calendar. Parents do not have visibility of direct student-teacher messages. Age-appropriate privacy information for students will include information about what their parents can see in Te Rito. There is no mechanism in Te Rito to show a clear and obvious 'your parent has access' or 'your parent is accessing Te Rito' real time status message, nor to reflect to the child when a parent has viewed a message.	Partially Aligned
12. Profiling	Switch options which use profiling 'off' by default (unless you can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing).	There is no profiling of any users, adult or child, in Te Rito. Students can manually select interests in their settings-My Interests page, e.g., science, sports, art. This is then used to recommend other extant school groups that the student may be interested in based upon the tags a school assigns to those groups. However, this interest is manually identified and selected by the student, there is no automated recommendations based on usage or membership of other groups. While all pages include a footer hyperlink to the Privacy policy, the My Interests page includes a more prominent assertion of privacy respect and link to the same privacy policy.	Fully Aligned
13. Nudge techniques	Do not use nudge techniques to lead or encourage children to provide unnecessary personal data or weaken or turn off their privacy protections.	Notifications are provided to users, focussed on appropriate teacher to student communications. Notifications can be turned on or off for each class a student is enrolled with. 'Notifications off' is a useful red colour, implying stop. Buttons are all represented as the same size, with no nudge techniques that could be detrimental being applied.	Fully Aligned
14.Connected toys & devices	If you provide a connected toy or device, ensure you include effective tools to enable conformance to this code.	Te Rito does not provide any connected toys or devices. There is a Google & iOS app, which provides the same interface to Te Rito as available for browsers on other computers, just optimised for mobile presentation. A Capture app also exists as a low touch content upload app with a streamlined UX.	Not Applicable
15. Online tools	Provide prominent and accessible tools to help children exercise their data protection rights and report concerns.	Group and personal messages have a 'report inappropriate' option available. This flags the content to the school office, with principals and deputy principals having access to the 'flagged items' view. Students have visibility of most of the information in Te Rito about them, noting prior commentary about high safety and high privacy by design meaning that medical and health information is not visible to students. Parents and students retain a right of access, which would have to be facilitated by their school. In addition students can only update some information themselves, as it would be inappropriate to allow them to update things like their name or profile photo for obvious reasons.	Partially Aligned

Proactively released

7 Assessment part 3 – Risk assessment

The Ministry has an established Risk Assessment Methodology that must be used to assess privacy risks. The outcome of the risk assessment process is documented in Table 16 below. Some risks identified through the PIA are more information security risks than purely privacy risks, these have been documented in the associated information security risk assessment part of the C&A memo. A number of control recommendations apply to all risks, to avoid repetition these are identified in Table 18 on page 79. More detailed information about the Risk Assessment Methodology can be found in Appendix B. The 'control reference' numbers are from the Ministry's Information Security Controls Catalogue.

Table 16: Privacy risk assessment

Risk ID	Risk Description	Likelihood	Impact	Inherent Risk	Control Recommendations and Privacy Response	Likelihood	Impact	Current Risk	Rationale
P-01	Excessive items of personal information (PI) are collected for no clear purpose. It results in a complaint to the Office of the Privacy Commissioner, potential breach of Privacy Act Principle 1 (IPP1), media attention, and reputational impact for the Ministry and schools.	Likely	Moderate	Medium	**HRS-03** A full engagement and communications plan has been developed to ensure that all stakeholders are informed about the Te Rito deployment and use. **PRI-03** Guidance will be developed for schools to review enrolment forms and privacy statements for specific requirements **PRI-04** Existing school business processes address collection of information about young children from parents with parental consent. **PRI-06** Personal information - students & school staff have access to review some information stored about them in Te Rito. **PRI-10** Guidelines issued to ensure the quality, utility, objectivity, integrity, and de-identification of Personal Information. **SEA-09** Input Validation. Process to validate information output from SMS sync to ensure that the information is consistent with the expected content. ***Not yet implemented:*** **PRI-05** Retention requirements – agree an approach to retaining PI in a 'lifelong learning' context. Implement differing retention periods.	Possible	Minor	Low	Mostly with schools on collection and in communications of purpose at the point of collection. Ministry can filter out excess data sent, which prevents Te Rito storing excess data. Ministry can work on communications in public, in lieu of any school specific Te Rito comms. Also related to P-11 possibly increasing retention risk.
P-02	Schools are insufficiently transparent with students or parents about their use of Te Rito to collect and share personal information, whether at point of enrolment or at point of opting into Te Rito. It results in a complaint to the Office of the Privacy Commissioner, a potential breach of IPP3, media attention, and reputational impact for the Ministry and schools.	Likely	Moderate	Medium	**HRS-03** Advice and guidance is provided to School Board, teachers, staff, as to their responsibilities for Privacy and Security of school information and systems. **HRS-03** A full engagement and communications plan has been developed to ensure that all stakeholders are informed about the Te Rito deployment and use. **PRI-01.2** & **PRI-01.3** Te Rito specific communications is made publicly available through multiple channels for students and Parents. Clarifying Te Rito information use, purpose and storage. **PRI-03** Guidance will be developed for schools to review enrolment forms and privacy statements for specific requirements **PRI-03.1** Te Rito will record 'consent to share' with the next school. This may prompt schools to provide more information when seeking consent. **PRI-04** Existing school business processes address collection of information about young children from parents with parental consent. Or collection of PI from older children with their consent for identified purposes ***Not yet implemented:*** **PRI-09** Schools to perform privacy brief analysis focused on the use of Te Rito.	Possible	Minor	Low	Could arise due to lack of communications from schools, or lack of understanding by students or parents. Schools today do not tend to stipulate all systems they use or store info in. Whether at enrolment, or when using a new system. Ministry can work on communications in public, in lieu of any school specific Te Rito comms.
P-03	Personal Information is exposed to an unauthorised third party. This is due to the Te Rito solution not implementing effective or sufficient safeguards to ensure the security of PI stored. PI is disclosed, the Privacy of multiple individuals is breached with potential to cause serious harm. Potential breach of IPP5, media attention, and reputational impact for the Ministry.	Unlikely	Severe	Medium	**CHG-02** Configuration management – integral with change control are technical configurations implemented to prevent sharing of PI except where appropriate managed by RBAC. **CPL-01** Due Diligence – Assurance reporting requirements defined, and a framework established to enable reporting. Inc RACI matrix to clarify shared responsibility obligations. **CPL-01** Service Agreement between schools, Ministry and Edsby **CRY-03** Transport Layer Security – all data is encrypted in transit from external connections to Te Rito. **CRY-05** Storage data security – all information and data is encrypted at rest and in storage. **GOV-01** Compliance requirements – Ministry information security and Privacy requirements and recommendations to be articulated to other parties, to be embedded in contracts (**TPM-08** SLAs and Contracts). **Controls for P-03 continue in Table 17 below.** ***Note not yet implemented:*** **IAC-06** Multi Factor Authentication (MFA) – All ESL users should be required to use MFA. Implementation is in progress thus not considered in risk analysis.	Rare	Severe	Medium	OPC guidance is that privacy breach involving info about children has serious harm impact.

Proactively released

Table 17: Controls for P-03 continued from previous page

GOV-03 Te Rito Data Kaitiakitanga Group provide assurance over access to and use of Te Rito data. **GOV-05.2** Operational and business reporting of key risk indicators will be defined. This reporting will include reports on idle accounts. **HRS-09.4** Te Rito automated deprovisioning of kaimahi access based on SMS update **IAC-02** Central Authentication, Authorisation of Te Rito users and processes acting on behalf of organizational users. **IAC-03** Central Authentication, Authorisation of third party users and processes accessing Te Rito. **IAC-07** Formal user registration and de-registration process that governs the assignment of access rights. **IAC-08** Role Based Access Control – All access to Te Rito (Kaimahi, students) is managed by RBAC. **IAC-10.1&4** Password complexity requirements. **IAC-11** Error messages during authentication provide minimally useful feedback. **IAC-15** User Account Management – the Cyber Security and Digital Support for Kura and Schools programme (CSDS) is undertaking work to document guidelines for schools.	**IAC-15 & 15.8** Terms & Conditions of use for Te Rito are enforced for ESL users. **IAC-15.8** Student Usage Guidelines for Te Rito have been defined for students. They are made available for schools to use as appropriate. **IAC-17** Periodic review of the privileges assigned to users to validate the need for such privileges and reassign or remove privileges, if necessary, to correctly reflect school business needs. **IAC-18** ESL requires users to follow accepted practices in the use of authentication mechanisms. **IAC-20** Principle of 'least privilege' is enforced by RBAC and linking of student records to their current school and teachers **IAC-22** ESL enforces a limit for consecutive invalid login attempts by a user and automatically locks the account when the maximum number of unsuccessful attempts is exceeded. **IAC-24** Session lock initiated after a period of inactivity, or on receiving a request from a user and retain the session lock until the user re-establishes access using established identification and authentication methods. **IAC-25** Automated mechanisms exist to log out users at the end of the session or after a defined period of inactivity. **IAC-28** Staff (ESL) users are required to provide Evidence of Identity (EoI) before an ESL account is created. Staff are also required to undergoing Identity Verification as part of the workforce safety checks under the Childrens' Act.	**IRO-04** Sector facing cyber and privacy Incident Response Plan (IRP) **IRO-10** Process exists to report incidents to applicable: Internal stakeholders, Affected schools, Governance bodies, and Regulatory authorities. **MON-01.12** Automated mechanisms exist to alert incident response personnel of inappropriate or unusual activities that have security incident implications. **MON-02** Logging and Auditing – Te Rito has full logging of all system and user events. Logs automatically feed in to monitoring and alerting tools. **MON-02.3** System monitoring and alerting – Te Rito is monitored, and alerts generated using existing tools. **MON-02.3** Security Incident and Event Management (SIEM) – in addition to creation of anomaly reporting criteria in monitoring tools, Ministry SIEM solution will receive alerts. **NET-04** & **NET-08** Firewalls & Intrusion detection **OPS-03** Service Management RACI & SoPs to be established. **PRI-05.2** Need to consider whether a two stage access model (request, confirm) can be implemented. **PRI-08** RBAC testing is conducted **PRI-10** Guidelines issued to ensure the quality, utility, objectivity, integrity, and de-identification of Personal Information. **SEA-09** Input Validation from SMS sync ensures that the information is consistent with the expected content.

Table 16: Privacy risk assessment (continued)

Risk ID	Risk Description	Likelihood	Impact	Inherent Risk	Control Recommendations and Privacy Response	Likelihood	Impact	Current Risk	Rationale
P-04	Schools have ineffective or insufficient safeguards to protect kaimahi credentials or ensure the integrity of data stored in SMSs. Data in Te Rito is compromised as a result. Significant quantities of PI, or sensitive PI, could be disclosed from Te Rito, the Privacy of multiple individuals is breached with potential to cause serious harm to some. Potential breach of IPP5	Likely	Moderate	Medium	**CPL-01** Service Agreement between schools, Ministry and Edsby **DCH-22** Data Quality and Validation checking is performed **IAC-07** Formal user registration and de-registration process that governs the assignment of access rights. **IAC-20** Principle of 'least privilege' is enforced by RBAC and linking of student records to their current school and teachers **IAC-22** ESL enforces a limit for consecutive invalid login attempts by a user and automatically locks the account when the maximum number of unsuccessful attempts is exceeded. **IRO-04** Sector facing cyber and privacy Incident Response Plan (IRP) **IRO-10** Process exists to report incidents to applicable: Internal stakeholders; Affected schools; Governance bodies; and Regulatory authorities. **MON-02** Logging and Auditing – Te Rito has full logging of all system and user events. Logs automatically feed in to monitoring and alerting tools. **SAT-02** Security awareness training – Ministry's Cyber Security and Digital Support for Kura and Schools programme has a specific workstream for awareness raising in the education sector. **SAT-02** There is extensive engagement in the education sector from NZ organisations such as Netsafe, NZ Police, OPC, CERT NZ on basic cyber security and privacy awareness applicable to children. **SEA-09** Input Validation. Process to validate information output from SMS sync to ensure that the information is consistent with the expected content. ***Not yet implemented:*** **IAC-06** Multi Factor Authentication (MFA) – All ESL users with access to student information should be required to use MFA.	Likely	Moderate	Medium	Impact is driven by potential extent of unintended disclosure and need for reporting of potential privacy breach with serious harm to OPC. Despite controls, impact of the event is still Moderate, likelihood remains as Likely given there are 2,550+ schools. The Ministry's Cyber Security and Digital Support for Kura and Schools programme (CSDS) is providing broad privacy and security guidance to education providers as a core objective. It is outside of Te Rito scope to broadly address school cyber security. IAC-06 implementation is in progress, thus not considered when assessing the residual risk.

Proactively released

Risk ID	Risk Description	Likelihood	Impact	Inherent Risk	Control Recommendations and Privacy Response	Likelihood	Impact	Current Risk	Rationale
P-05	Requests for access or correction are not adequately processed by schools, or Statements of Correction made visible in Te Rito. This may result in detrimental impacts for a student, a loss of reputation and trust for schools and the Ministry with parents or whānau. Potential breach of IPP6, 7, 8	Possible	Minor	Low	**HRS-03** A full engagement and communications plan has been developed to ensure that guidance and recommendations for all stakeholders about the Te Rito. **PRI-06** Access to Information – process to be defined for Right of Access to data in Te Rito post-school. **PRI-06** Personal information permission – students & school staff have access to review some information stored about them in Te Rito. **PRI-08** Te Rito specific Privacy training is available.	Unlikely	Minor	Low	Te Rito will provide self-service visibility to students and then parents to review info, without schools needing to facilitate access. Improves correction and info being up to date. Depending on how a school documents a Statement of Correction, this may not be visible in Te Rito with the associated data. Docs can be uploaded.
P-06	Personal information is used or disclosed outside of the specified purpose for which it was collected and stored in Te Rito. Specifically, Ministry staff access Te Rito to obtain information not otherwise accessible to the Ministry. Limited or non-identifying PI of many individuals is disclosed, the Privacy of many individuals is breached though without serious harm. Potential breach of IPP1, 4, 10, 11.	Rare	Major	Low	**GOV-03** Te Rito Data Kaitiakitanga Group provide assurance over access to and use of Te Rito data. An ethics review process for research requests will be established. **GOV-05.2** Operational and business reporting of key risk indicators. **HRS-03** A full engagement and communications plan has been developed to ensure that all stakeholders are informed about the Te Rito deployment and use. **IAC-08** Role Based Access Control – All access to Te Rito (Kaimahi, students) is managed by RBAC. **IAC-15 & 15.8** Terms & Conditions of use for Te Rito are enforced for staff (ESL) users. Including Professional Code of Conduct obligations. **IAC-17** Business reporting of ESL & Te Rito roles assigned to staff will be developed to help identify excess Roles or Permissions. **MON-02** Logging and Auditing – Te Rito has full logging of all system and user events. **MON-02.3** System monitoring and alerting – Te Rito is monitored, and alerts generated using existing tools. **PRI-08** Te Rito specific Privacy training is available. **SAT-02** Security awareness training – the Ministry's Cyber Security and Digital Support for Kura and Schools programme (CSDS) has a specific workstream for awareness raising in the education sector.	Rare	Moderate	Low	Likely that many parents would expect a school to share information about their child with the Ministry. Particularly when that relates to educational delivery such as teaching support. Beyond this, some info sharing to Ministry is mandated under ETA. OPC's view that MoE is more than a Service Provider for Te Rito may influence this risk in the future.
P-07	A technical fault in Te Rito leads to an authorised user being able to see PI that they have no purpose to see. Potential breach of IPP5, 11	Possible	Moderate	Medium	**IAC-17** Business reporting of ESL & Te Rito roles assigned to staff will be developed to help identify excess Roles or Permissions. **PRI-08** RBAC testing is conducted. **Additional controls as for P-08 below.**	Unlikely	Moderate	Low	Despite all good testing practices, a tech fault may still happen. The fault in itself may not be a privacy issue. Impact driven by likely scale. Becomes an issue under P-08 where a user does something.
P-08	An authorised user of Te Rito accesses, uses or discloses Personal information that is inappropriate or outside identified purposes. E.g. school staff disclose student information to other staff or students who have no need to know. PI of one or multiple individuals is disclosed, Privacy is breached though without serious harm.	Likely	Moderate	Medium	**CHG-02** Technical configurations implemented to prevent sharing, export or download of PI except where appropriate and managed by RBAC. **CPL-01** Service Agreement between schools, Ministry and Edsby **GOV-05.2** Operational and business reporting of key risk indicators. **IAC-08** Role Based Access Control – All access to Te Rito (Kaimahi, students) is managed by RBAC. **IAC-13** Alternative methods of authentication under specific circumstance exist for young children. **IAC-15 & 15.8** Terms & Conditions of use for Te Rito are enforced for staff (ESL) users. Including Professional Code of Conduct obligations. **IAC-15.8** Student Usage Guidelines for Te Rito have been defined for students. They are made available for schools to use as appropriate. **IAC-20** Principle of 'least privilege' is enforced by RBAC and linking of student records to their current school and teachers **IRO-04** Sector facing cyber and privacy Incident Response Plan (IRP)	Possible	Minor	Low	Considering authorised users have access to the information in both school systems and Te Rito, risk is more a school's risk. Availability of info in Te Rito when a student changes schools means there may be more historical info available to a new school. An easier flow (in Te Rito) means easier Kaimahi access to info that is currently inaccessible from prior school. Likely that parents would expect a school to share information about their child with a new school. Especially when that relates to learning or teaching support.

Proactively released

Risk ID	Risk Description	Likelihood	Impact	Inherent Risk	Control Recommendations and Privacy Response	Likelihood	Impact	Current Risk	Rationale
	Potential breach of IPP10, 11.				**IRO-10** Process exists to report incidents to applicable: Internal stakeholders; Affected schools; Governance bodies; and Regulatory authorities. **MON-02** Logging and Auditing – Te Rito has full logging of all system and user events. **PRI-03.1** Te Rito will record 'consent to share' with next school. **PRI-08** Te Rito specific Privacy training is available. **SAT-02** Security awareness training – Ministry Cyber Security and Digital Support programme includes training & awareness for sector **SEA-09** Input Validation. Process to validate information output from SMS sync to ensure that the information is consistent with the expected content. ***Not yet implemented:*** **PRI-05.2** Need to consider whether a two stage access model (request, confirm) can be implemented. **PRI-09** Schools to perform privacy brief analysis focused on the use of Te Rito.				Inappropriate disclosure could be serious if it is to people outside the school, perhaps not as serious if to other teachers. Risk is primarily about human action and intent, can't be addressed by technical controls.
P-09	An individual is able to be identified from a number of aggregated or anonymised data sets, or through unique identifier such as NSN. Potential breach of IPP10, 11, 13. Also related to P-11 retention risk.	Possible	Moderate	Medium	**CHG-02** Configuration management – anonymised dashboards are configured to suppress PI, and not display cohorts of 5 or less. **IAC-15 & 15.8** Terms & Conditions of use for Te Rito are enforced for staff (ESL) users. Including Professional Code of Conduct obligations. **IRO-10** Process exists to report incidents to applicable: Internal stakeholders; Affected schools; Governance bodies; and Regulatory authorities. **PRI-01.5** The ETA identifies specified users and specified purposes for use of the NSN, with an offenses provision defined. **PRI-10** Guidelines issued to ensure the quality, utility, objectivity, integrity, and de-identification of Personal Information. ***Not yet implemented:*** **PRI-05.7** Define and implement data handling and protection requirements for specific categories of sensitive Personal Information.	Unlikely	Moderate	Low	In a Te Rito context the dashboards provide anonymised reporting at a Cluster level. Only principals & deputy principals have dashboard access. Dashboard configuration removes any identifiable PI from being displayed. Filters are applied in the dashboard align with StatsNZ guidance on minimum cohort size. With an NSN any sector staff can identify the student's name & DoB, though not which school they are at. Thus comes down to professional trust & code of conduct issue.
P-10	A school pre-enrols a student in their SMS, resulting in the principal or administrator for that school being able to see additional information in Te Rito about a student who is not currently attending the school. Potential breach of IPP11	Likely	Moderate	Medium	**CPL-01** Service Agreement between schools, Ministry and Edsby **DCH-22** Data Quality and Validation checking is performed. **GOV-05.2** Operational and business reporting of key risk indicators. **HRS-09.4** Te Rito automated deprovisioning of kaimahi access based on SMS update. **IAC-08** Role Based Access Control – All access to Te Rito (Kaimahi, students) is managed by RBAC. **IAC-15 & 15.8** Terms & Conditions of use for Te Rito are enforced for staff (ESL) users. Including Professional Code of Conduct obligations. **IAC-20** Principle of 'least privilege' is enforced by RBAC and linking of student records to their current school and teachers **MON-02** Logging and Auditing – Te Rito has full logging of all system and user events. **PRI-03** Guidance will be developed for schools to review enrolment forms and privacy statements for specific requirements **PRI-03.1** Te Rito will record 'consent to share' with next school. **SEA-09** Input Validation. Process to validate information output from SMS sync to ensure that the information is consistent with the expected content. ***Not yet implemented:*** **PRI-05.2** Need to consider whether a two-stage access model (request, confirm) can be implemented. **PRI-09** Schools to perform privacy brief analysis focused on the use of Te Rito.	Possible	Minor	Low	Te Rito currently discards pre-enrolled records sent from SMS. Only showing up once an enrolment date is current. Typo or human error could lead to invalid claim of enrolment. Valid pre-enrolment are dependent on Parents supplying correct biographical info to the school. Business process of pre-enrolment. Thus is authorised.

Proactively released

Risk ID	Risk Description	Likelihood	Impact	Inherent Risk	Control Recommendations and Privacy Response	Likelihood	Impact	Current Risk	Rationale
P-11	Te Rito may retain personal information for longer than operationally necessary. This is due to insufficient retention and disposal measures, inadequate system functionality and/or legal authority to dispose of records Increased exposure and impact from a breach. Potential breach of IPP9	Likely	Major	High	**GOV-05.2** Operational and business reporting of key risk indicators. **HRS-09.4** Te Rito automated deprovisioning of kaimahi access based on SMS update. **IAC-08** Role Based Access Control – All access to Te Rito (Kaimahi, students) is managed by RBAC. **IRO-04** Sector facing cyber and privacy Incident Response Plan (IRP) **MON-02** Logging and Auditing – Te Rito has full logging of all system and user events. Logs automatically feed in to monitoring and alerting tools. **PRI-10** Guidelines issued to ensure the quality, utility, objectivity, integrity, and de-identification of Personal Information. **SEA-09** Input Validation. Process to validate information output from SMS sync to ensure that the information is consistent with the expected content. ***Not yet implemented:*** **PRI-05** Retention requirements – agree an approach to retaining PI in a 'lifelong learning' context. Implement differing retention periods. **PRI-05.7** Define and implement data handling and protection requirements for specific categories of sensitive Personal Information.	Possible	Major	Medium	'Operationally necessary' is typically left to schools to decide. In Te Rito retention is aligned with SRRDS. Active sLSR data retained for a shorter period, then part of seven year backup. No current provision for more flexible retention or archive options. Disposal Authority needs to consider which agency is holding the data post school. Or whether Discharge to students is a valid approach. Including possible retention for 'lifelong learning'. Currently there is no 'lifelong retention'. Also related to P-03, security management.
P-12	Students or parents may not understand the use and purpose for collection and storage of information in Te Rito, this results in a privacy complaint. Potential breach of IPP3, 4, 10	Possible	Minor	Low	**HRS-03** A full engagement and communications plan has been developed to ensure that all stakeholders are informed about the Te Rito deployment and use. **PRI-01.2** & **PRI-01.3** Te Rito specific communications is made publicly available through multiple channels for students and Parents. Clarifying Te Rito information use, purpose and storage. **PRI-02** The Privacy statement applicable to Te Rito is publicly published in plain language, in Te Reo, is summarised for students, and an age appropriate format for students aged under 12 will be developed. Te Rito Ts&Cs for adults are in plain language, publicly published and an age appropriate acceptable use guidelines have been written for students. **PRI-03** Guidance will be developed for schools to review enrolment forms and privacy statements for specific requirements **PRI-06** Personal information permission – students & school staff have access to review some information stored about them in Te Rito. ***Not yet implemented:*** **PRI-05.7** Define and implement data handling and protection requirements for specific categories of sensitive Personal Information. **PRI-09** Schools to perform privacy brief analysis focused on the use of Te Rito.	Unlikely	Minor	Low	Proactive comms plan with publicly available information. Parental concerns likely raised in the first instance with their school for clarification.
P-13	Scope, function, or purpose creep in Te Rito may lead to new Privacy risks not being identified and mitigated. Including schools or other Governance stakeholders not being aware of changes in progress. Potential breach of IPP4, 11	Possible	Moderate	Medium	**GOV-01** Compliance requirements – Ministry information security and Privacy requirements and recommendations to be articulated to other parties, to be embedded in contracts (**TPM-08** SLAs and Contracts). **GOV-03** Te Rito Data Kaitiakitanga Group provide assurance over access to and use of Te Rito data. An ethics review process for research requests will be established. **GOV-05.2** Operational and business reporting of key risk indicators. **PRI-01.2** & **PRI-01.3** Te Rito specific communications is made publicly available through multiple channels for students and Parents. Clarifying Te Rito information use, purpose and storage. **PRI-10** Guidelines issued to ensure the quality, utility, objectivity, integrity, and de-identification of PI **PRI-14** Privacy-related audit records. Privacy related reporting to internal senior management, , as well as external oversight bodies as appropriate, demonstrating accountability with privacy requirements. **SEA-09** Input Validation. Process to validate information output from SMS sync to ensure that the information is consistent with the expected content.	Unlikely	Moderate	Low	Collective responsibility and agreement with Ngā Rau Whakatupu and Te Rito Data Kaitiakitanga groups applies. This does not mean everyone will necessarily agree with planned changes. Assurance reporting via PRI-14 will remain the key control, in concert with governance arrangements including GOV-01, GOV-03. An ethics review process for potential research requests to access Te Rito data will be defined. OPC's view that MoE is more than a Service Provider for Te Rito may influence this risk in the future.

Proactively released

Risk ID	Risk Description	Likelihood	Impact	Inherent Risk	Control Recommendations and Privacy Response	Likelihood	Impact	Current Risk	Rationale
P-14	Kaimahi authorised to access Te Rito, uses or discloses (inadvertently or deliberately) sensitive personal information that is inappropriate with the potential for serious harm. E.g. disclosure of student health, medical or behavioural information to others who have no need to know. PI of one or multiple individuals is disclosed, Potential breach of IPP10, 11, media attention, and reputational impact for the Ministry and schools.	Possible	Moderate	Medium	**CHG-02** Technical configurations implemented to prevent sharing, export or download of PI except where appropriate and managed by RBAC. **CPL-01** Service Agreement between schools, Ministry and Edsby **HRS-09.4** Te Rito automated deprovisioning of kaimahi access based on SMS update **IAC-08** Role Based Access Control – All access to Te Rito (Kaimahi, students) is managed by RBAC. **IAC-15 & 15.8** Terms & Conditions of use for Te Rito are enforced for staff (ESL) users. Including Professional Code of Conduct obligations. **IAC-17** Business reporting of ESL & Te Rito roles assigned to staff will be developed to help identify excess Roles or Permissions. **IAC-20** Principle of 'least privilege' is enforced by RBAC and linking of student records to their current school and teachers **IAC-24** Session lock initiated after a period of inactivity **IAC-25** Automated mechanisms exist to log out users at the end of the session or after a defined period of inactivity. **IRO-04** Sector facing cyber and privacy Incident Response Plan (IRP) **IRO-10** Process exists to report incidents to applicable: Internal stakeholders; Affected schools; Governance bodies; and Regulatory authorities. **MON-02** Logging and Auditing – Te Rito has full logging of all system and user events. **SEA-09** Input Validation. Process to validate information output from SMS sync to ensure that the information is consistent with the expected content. ***Not yet implemented:*** **PRI-05.2** Need to consider whether a two-stage access model (request, confirm) can be implemented. **PRI-05.7** Define and implement data handling and protection requirements for specific categories of sensitive Personal Information. **PRI-09** Schools to perform privacy brief analysis focused on the use of Te Rito.	Unlikely	Moderate	Low	Considering authorised users have access to the information in both school systems and Te Rito, risk is more a school's risk. Inappropriate disclosure could be serious if it is to people outside the school, perhaps not as serious if to other teachers. Risk is primarily about human action and intent, can't be addressed by technical controls. Beyond minimising kaimahi who have access to sensitive information.
P-15	Schools may be sharing personal information to other schools which is outside of the specified purpose for which it was collected. Te Rito facilitates this. Schools may not identify on enrolment forms or in a privacy statement that information is shared with a student's next school, or consent to do so is not sought. Potential breach of Privacy IPP3, 10, 11.	Likely	Moderate	Medium	**CPL-01** Service Agreement between schools, Ministry and Edsby **HRS-03** A full engagement and communications plan has been developed to ensure that all stakeholders are informed about the Te Rito deployment and use. **IAC-15 & 15.8** Terms & Conditions of use for Te Rito are enforced for staff (ESL) users. Including Professional Code of Conduct obligations. **PRI-01.2** & **PRI-01.3** Te Rito specific communications is made publicly available for students and Parents. Clarifying Te Rito information use, purpose and storage. **PRI-03** Guidance will be developed for schools to review enrolment forms and privacy statements for specific requirements **PRI-03.1** Te Rito will record 'consent to share' with next school. **PRI-04** Existing school business processes address collection of information **SAT-02** Security awareness training – the Ministry's Cyber Security and Digital Support for Kura and Schools programme (CSDS) includes training & awareness for sector ***Not yet implemented:*** **PRI-05.2** Need to consider whether a two-stage access model (request, confirm) can be implemented. **PRI-05.7** Define and implement data handling and protection requirements for specific categories of sensitive PI. **PRI-09** Schools to perform privacy brief analysis focused on the use of Te Rito.	Unlikely	Moderate	Low	See prior discussion of enrolment & privacy statement review activity. Expect 92% of schools will be good. Schools may consider identifying a Purpose for collection in a Privacy statement is sufficient consent from a parent or student. Schools may alternatively consider exception under IPP11 or Principal's duties under ETA, provide sufficient legal permission in lieu of consent on forms. Ultimately whether a school updates their enrolment form(s) or privacy statements is a decision for the schools to make, consistent with the level of detail they provide to students and Parents. Te Rito has checkbox to record consent in lieu of SMS's having checkbox.
P-16	A student uses Te Rito to publish to a school wide group (or cross school group) personal	Possible	Minor	Low	**HRS-03** A full engagement and communications plan has been developed to ensure that all stakeholders are informed about the Te Rito deployment and use.	Possible	Minor	Low	Schools upload photos or good news stories to public websites & social media on a regular basis. Objective breach of

Proactively released

Risk ID	Risk Description	Likelihood	Impact	Inherent Risk	Control Recommendations and Privacy Response	Likelihood	Impact	Current Risk	Rationale
	information about another student without permission, or publishes content that is not age appropriate. Limited PI of one or a few individuals is disclosed, within a community they are a part of. Potential breach of Privacy and potential harm. IPP1, 10, 11.				**IAC-08** Role Based Access Control – All access to Te Rito (Kaimahi, students) is managed by RBAC. **IAC-15.8** Student Usage Guidelines for Te Rito have been defined for students. They are made available for schools to use as appropriate. **IAC-20** Principle of 'least privilege' is enforced by RBAC and linking of student records to their current school and teachers **PRI-01.2** & **PRI-01.3** Te Rito specific communications is made publicly available for students and Parents. Clarifying Te Rito information use, purpose and storage. **PRI-08** Te Rito specific Privacy training is available. **SAT-02** Security awareness training – the Ministry's Cyber Security and Digital Support for Kura and Schools programme (CSDS) has a specific workstream for awareness raising in the education sector.				privacy would need to be demonstrably more than common or accepted practice in the school community. Numerous other mechanisms exist for wide publication/distribution by a student e.g. social media groups. Te Rito has a content review function. Publishing to a school group remains within the school community. Student 'about me' and portfolio is safe by default.
P-17	A student is unable to exercise their Privacy rights given the mandatory nature of school enrolment and attendance, and the school being a custodian of student information in Te Rito. A Privacy complaint may arise over issues such as purpose, meaningful consent, opt-in, scope of data held. IPP3, 6, 9, 10, 11	Possible	Minor	Low	**GOV-03** Te Rito Data Kaitiakitanga Group provide assurance over access to and use of Te Rito data. **HRS-03** A full engagement and communications plan has been developed to ensure that all stakeholders are informed about the Te Rito deployment and use. **IAC-20** Principle of 'least privilege' is enforced by RBAC and linking of student records to their current school and teachers **PRI-01.2** & **PRI-01.3** Te Rito specific communications is made publicly available through multiple channels for students and Parents. Clarifying Te Rito information use, purpose and storage. **PRI-03** Guidance will be developed for schools to review enrolment forms and privacy statements for specific requirements **PRI-03.1** Te Rito will record 'consent to share' with next school. **PRI-04** Existing school business processes address collection of information about young children from parents with parental consent. ***Not yet implemented:*** **PRI-05.2** Need to consider whether a two stage access model (request, confirm) can be implemented. **PRI-05.7** Define and implement data handling and protection requirements for specific categories of sensitive PI. **PRI-09** Schools to perform privacy brief analysis focused on the use of Te Rito.	Unlikely	Minor	Low	ETA and extant school policies authorise & address school business processes. Te Rito holding student owned information with the schools and Ministry as custodians or stewards, may need a perspective shift in Ministry or school business processes. Communications and transparency, alongside education and awareness will be critical to informed and meaningful understanding by parents and students to the purposes of Te Rito.
P-18	The Capture app is used to upload photos, audio, and/or video of young children to Te Rito. Young children lack the capacity to genuinely consent to this or comprehend the implications of their likeness being captured and stored in Te Rito. This is caused by inadequate consideration by teachers of ethical and age-appropriate considerations. It results in a complaint to the Office of the Privacy Commissioner, a breach of IPP4, media attention, and reputational impact for the Ministry and schools.	Possible	Moderate	Medium	**HRS-03** A full engagement and communications plan has been developed to ensure that all stakeholders are informed about the Te Rito deployment and use. **IAC-15.8** Student Usage Guidelines for Te Rito have been defined for students. They are made available for schools to use as appropriate. **PRI-01.2** & **PRI-01.3** Te Rito specific communications is made publicly available through multiple channels for students and Parents. Clarifying Te Rito information use, purpose and storage. **PRI-03** Guidance will be developed for schools to review enrolment forms and privacy statements for specific requirements **PRI-04** Existing school business processes address collection of information about young children. **PRI-05** Retention requirements – default active retention period for student classwork is one (1) year. ***Not yet implemented:*** **PRI-09** Schools to perform privacy brief analysis focused on the use of Te Rito.	Unlikely	Minor	Low	Parents and young children will be familiar with tools such as Storypark used in ECE. Uploading of photo or video content will be familiar situation. Ability of young children to understand concept of Privacy, outside of 'personal bubble' is limited, ability to comprehend potential consequences is also minimal. This is simply too much to expect from young children. Reliance upon Teacher ethics & integrity. All children will have a mandatory school profile photo. And likely be included in general class photos. Schools' complaint process would be followed before escalation to OPC.

Proactively released

Controls applicable to every Privacy risk are shown in Table 18 below.

Table 18: Controls applicable to every Privacy risk

GOV-01 Compliance requirements – inc. Certification and Accreditation (C&A) of the Te Rito solution and end to end service.	**GOV-03** Information security & privacy reviews – Perform a risk assessment, in concert with major changes of scope, solution capability.	**GOV-03** Information security reviews – The Ministry reviews Edsby assurance documentation and will assess the reliance of assurance that can be placed on the Edsby evidence.
GOV-03 Periodic reviews – The Te Rito project will engage an independent auditor to perform project IQA.	**GOV-03** Privacy control and risk review – Evaluation and discovery work with schools will provide feedback to confirm which controls are effective or ineffective, updating the risk level. Identification of new effective controls.	**HRS-03** Advice and guidance is provided to School Board, teachers, staff, as to their responsibilities for Privacy and Security of school information and systems. Guidance identified to date includes; Roles & Responsibilities elaboration, How to assign roles in Te Rito, Privacy Act request process (considering Te Rito nuances), filing a Statement of Correction in Te Rito, Student Acceptable Use Guide, How to handle reports of inappropriate messages, Incident Management guidance, Directory search op-out (for teachers), Privacy Brief analysis template (**PRI-09**).
PRI-01 Policies for information security and **PRI-02** Privacy Policy – Existing Ministry and Edsby information security and privacy policies, practices, processes, education, and awareness training, applicable for all staff involved in the design, operation, and management of the end-to-end service.	**PRI-01 & PRI-02** Schools have existing Privacy policies, these may need updating in line with the purpose for storing info in Te Rito. A sample of school Privacy policies are being reviewed to assess whether further guidance from the Ministry to schools may be needed.	**PRI-02** The Privacy statement applicable to Te Rito is publicly published in plain language, in Te Reo, is summarised for students, and an age-appropriate format for students aged under 12 will be developed. Te Rito Ts&Cs for adults are in plain language, publicly published, in Te Reo, and an age appropriate acceptable use guidelines have been developed for students.
IRO-04 Incident response plan – Ministry incident response plans cater for information security and privacy incidents, including escalation, communications, notification to effected parties.	**IAO-05 & PRI-14** Operational Assurance Plan. In concert with the assurance requirements identified of supporting or integrated services, the Ministry will agree a formal assurance plan covering the end-to-end Te Rito service.	**PRM-01** In the Ministry's overall digital strategy are several initiatives to help schools with their cyber security including Te Mana Tūhono, Cyber Security and Digital Support for Kura & Schools programme (CSDS), Network for Learning (N4L), Safer Technology for Schools (ST4S).
PRI-08 OPC's PrivacyABCs for Schools is available as privacy training for all school Kaimahi. Privacy touch points are included in overall Te Rito user training guides.	**PRI-01.6** Privacy by design inc. data minimisation, transparency, user-centric.	**VPM-07** Security testing – Perform security testing, remediate findings to an acceptable risk level.

Proactively released

8 Assessment part 4 – Data Protection and Use Policy (DPUP)

8.1 Overview of the DPUP

The DPUP describes values and behaviours that will build trust and help ensure that data practices are focused on the wellbeing of people and communities. These values and behaviours are represented as five principles. The focus is on relationships, rather than rules — a way of working that respects people, their information, and their stories.

The DPUP provides good practice Guidelines on how to uphold these Principles in four key areas to help organisations understand and apply the Privacy Act. The DPUP also goes beyond privacy matters to include ethical considerations when making decisions. Good practice requires that if, and when, agencies consider how and when to use people's information, it's done with the involvement, understanding, and support of the people impacted by those proposals.

A summary of Te Rito's compliance against the four key areas is given in Table 19 in the following section.

8.2 Assessment against guidelines

The Ministry is ensuring strong relationships between Te Rito and the sector by collaborating with the sector groups Ngā Rau Whakatupu and Te Rito Data Kaitiakitanga group. This formalises strong engagement with peak bodies, individual schools, and principals. A Te Rito specific version of the human trust framework was developed during 2021 identifying eleven (11) themes across four key groups. They are described in detail in the *Te Rito Building Trust Summary* and *Details* documents, and are summarised here:

- **Whanaungatanga:** An enduring focus on building connections between ourselves and our work, with Te Rito at the centre of our efforts.
  - 1 Relationships
  - 2 Behavioural Expectations
  - 3 Engagement Approach
  - 4 Communications
- **Tikanga for data:** Te Rito data is taonga, and its care and correct use is supported by guidance about what it may be used for, and how.
  - 5 Purpose of Use of Data
  - 6 Method of Use of Data
  - 7 Capability and Support
- **Kaitiakitanga:** Stewardship of Te Rito's data is based on partnership, inclusion, transparency, and understanding people's rights.
  - 8 Positions, Roles, Functions
  - 9 Governance / Decision Rights

Proactively released

- **Pou Whenua:** We stand on what we value, and the value we deliver for tamaiti as a "system that learns". Our mahi strengthens trust and signals intentions for the future.
  - 10 Delivering Value
  - 11 Delivery Confidence

Table 19: DPUP guidelines and Te Rito's compliance

DPUP Guidelines	Manner of compliance
Purpose Matters • The vital importance of purpose to collecting and using people's personal information • Be clear about the purposes of collecting personal information, only collect what's needed, and consider how collection and use could affect people's wellbeing.	The Key Principle for Te Rito is "*Me tiaki te mana o te tamaiti me tōna whānau* – To protect and uphold the mana of the child and their whānau". Recognising that our tamariki are our taonga, it stands to reason that the information about them is also taonga. It is therefore important to protect the privacy and security of our learners' information whilst ensuring that the right people have access to it, for the right purpose, at the right time. Te Rito is focused on enabling data that is currently held within school Student Management Systems (SMSs) and Ministry systems, to be exchanged with the national learner repository so that the information is available to support that student, their whānau, and educators. Te Rito has the potential to bring considerable benefits to children, young people and teachers by: • improving the transfer of student information between schools so that schools have access to key information from day one • reducing the need for teachers to reassess new students • providing more timely information to support students with additional learning needs • storing information securely and making it more accessible to those who have the appropriate permissions • improving the flow of information within and between Communities of Learning | Kāhui Ako • reduced administration overhead which provides more time to focus on supporting student achievement and wellbeing • enables a better understanding of a student joining the school which provides the ability to build rapport and support the student in the ways they need.

Proactively released

DPUP Guidelines	Manner of compliance
Transparency and Choice • Enable people to understand what's happening with their information and what choices they have • When collecting information from people, help them understand why it's being collected, how that might help them or people in similar circumstances, and what rights they have to access and request changes. Provide them with choices whenever possible.	Use of Te Rito is opt-in for schools, though not for individual students. Students will have a choice about what additional information they proactively stored in Te Rito, while the school will remain responsible for providing the majority of information within their purview. Once a school has opted in additional information about a student will also be sourced from systems that are managed by the Ministry. A major focus of the *Te Rito Engagement and Communications Strategy and Plan* is ensuring that information about Te Rito is in plain language, translated to Te Reo, along with age-appropriate summaries for different age cohorts of students. Comms are being delivered via schools, through the sector working groups to peak bodies and peer groups for kaimahi, and from the Ministry directly. Schools remain responsible for collecting information in the first place, with comms from the Ministry to support discussions with students and parents at enrolment time about the purpose of Te Rito. Risks have been identified in relation to student agency (P-17, P-18), school communications (P-02) and parent understanding (P-12).
Access to Information • Make it easy for people to see and request correction of their information • Help people to understand what personal information is held about them, to access it, to request correction of it and, where possible, to correct it themselves.	Te Rito will improve student and parent access to and visibility of information that schools and the wider education ecosystem hold about their child. Correction of any errors remains primarily with the school, who are able to assist with any updates required to Ministry sources of information. This PIA will be made available with a plain language summary, and age-appropriate outputs will also be developed. This PIA is supported by the plain language privacy statement published on the Te Rito website. Both sources provide detail of the information held in Te Rito.
Sharing Value • Work together for better insights and outcomes • Work together and be inclusive to ensure that information used to create insights is relevant and usefully describes real experiences. Share insights that deliver value and improved wellbeing.	Te Rito's focus is on improving the day-to-day student experience at school and achieving better outcomes for students during changes of school or teacher. Aggregate insights or analytics are not a specific objective for Te Rito.

Proactively released

9 Assessment part 5 – GCSB Information Classification

9.1 Part B: GCSB Information rating – SENSITIVE

Information security requirements	Manner of compliance
Principles and clearance levels • Information classified as RESTRICTED or SENSITIVE should be held, processed, transmitted and destroyed with discretion to make compromise highly unlikely. • Only Staff authorised by the department to access RESTRICTED or SENSITIVE levels are authorised to handle the information. This includes all staff involved with transmission, storage, and disposal.	As much of the information in Te Rito is sourced from schools there is no formal classification of the information at source. The Ministry has defined Te Rito as a system to be SENSITIVE. Ensuring that appropriate management practices and controls are implemented considering the risk associated with the significant aggregation of information in Te Rito. Aka the 'one up' principle for classifications. This is consistent with other Ministry systems that Te Rito sources data from, such as PaCT. Some information in Te Rito is sensitive (small s), e.g., assessment data, and in the future medical data, without having been formally classified as SENSITIVE. Staff at a school have access to information in Te Rito for students in their class. Some sensitive (small s) information is only available to certain school staff such as a principal.
Electronic transmission All RESTRICTED or SENSITIVE information transmitted across public networks must be encrypted.	Te Rito transmission of information is secured using TLS v1.3.
Electronic storage Electronic files (including databases) should be protected against illicit internal use or intrusion by external parties through two or more of the following mechanisms: • user challenge and authentication (username/password or digital ID/Certificate) • logging use at level of individual • firewalls and intrusion-detection systems and procedures • server authentication • OS-specific/application-specific security measures.	Te Rito uses the Education Sector Logon (ESL) to authenticate all staff access; and will federate authentication from each school's identity provider (Microsoft 365 for Education or Google Workspace for Education) for student access. All service accounts are required to use authentication. Te Rito has full audit logging, with audit trail visibility available to principals for student record updates. Edsby implement firewalls and other network security protections in addition to the inherent network security protections from Microsoft's Azure hosting capabilities. OS and application specific security controls are the responsibility of Edsby, who have achieved ISO27001 Certification.
Electronic disposal Electronic files should be disposed of in a way that makes reconstruction highly unlikely.	Disposal of Te Rito information is aligned with the seven (7) year schools data retention schedule. Formal disposal at the seven year mark is secure.
Manual transmission, Storage, Disposal	Not Applicable, Te Rito does not involve manual transmission, storage or disposal of information

Proactively released

Appendix A - Information Privacy Principles

The Privacy Act 2020 sets out 13 Information Privacy Principles (IPPs).

The IPPs are based on international principles of fair information practice. Similar Principles form the backbone of privacy and data protection legislation in an increasing number of jurisdictions throughout the world. The IPPs apply to the collection, accuracy, use and security of personal information. They also provide for access to, and correction of, personal information and place controls on unique identifiers.

The IPPs impose duties on agencies, and confer rights on individuals, in relation to personal information. Their coverage can be discerned from their general headings:

- Principle 1 – purpose of collection of personal information
- Principle 2 – source of Principle of information
- Principle 3 – collection of information from subject
- Principle 4 – manner of collection of personal information
- Principle 5 – storage and security of personal information
- Principle 6 – access to personal information
- Principle 7 – correction of personal information
- Principle 8 – accuracy of personal information to be checked before use
- Principle 9 – agency not to keep personal information for longer than necessary
- Principle 10 – limits on use of personal information
- Principle 11 – limits on disclosure of personal information
- Principle 12 – disclosure of personal information outside of New Zealand
- Principle 13 – unique identifiers.

Read more about each privacy principle on the Office of the Privacy Commissioner's website: Office of the Privacy Commissioner|The privacy principles - overview.

Proactively released

Appendix B - Ministry risk assessment methodology

Note that as of September 2023 the Ministry's enterprise risk framework has been updated, one substantive change being the introduction of a 5x5 risk matrix. This PIA has been completed against the new risk matrix and definitions elaborated in the tables below.

Risk assessment guidelines

Risks to privacy can arise in many circumstances. Collecting excessive information, using intrusive means of collection, or obtaining sensitive details in unexpected circumstances all represent risks to the individual. Unexpected or unwelcome uses or disclosure of that information, or its retention for an unduly long period, put individual privacy at risk. The privacy impact report should identify the avoidable risks and suggest cost-effective measures to reduce them to an appropriate level. This will provide the inherent risk rating and enable the effectiveness of the proposed controls to be assessed.

Impact (consequences) assessment

The qualitative scale used to assign an impact rating is presented in Table A below. All impacts need to be seen in a business context and be informed by the business. Rating the impact of a risk should include a consideration of any possible knock-on effects of the consequences of the identified risks, including cascade and cumulative effects.

The effect of a risk event materialising must be assessed using the agency's approved risk rating scales. If a risk has multiple potential consequences, then the impact with the largest effect must be used to rate the risk. However, where multiple consequences for a single risk are assessed at the same level, the impact may be Evaluated as being higher than the individual impact statements (e.g., a risk that has two moderate impacts might be judged to have a significant impact when they are combined). Rating the impact of a risk should include a consideration of any possible knock-on effects of the consequences of the identified risks, including cascade and cumulative effects.

Likelihood (probability) assessment

The qualitative scale used to assign a likelihood rating is presented in Table B below. Where information is available about the frequency of an incident in the past it should be used to determine the likelihood of the risk eventuating. However, where such information does not exist it does not necessarily mean that the likelihood of the risk eventuating is low. It may merely indicate that there are no controls in place to detect it or that the agency has not previously been exposed to the particular risk.

Risk matrix

Table B presents a 5x5 matrix for assigning a risk rating to a risk. It is used by mapping the likelihood and impact ratings. The rating being the point where the likelihood and impact ratings intersect.

Proactively released

Table A – Impact assessment – Threats

	Harm & Safety	Service Delivery	Financial	Legislative	Trust & Confidence
Extreme	• Fatality or fatalities to an employee, contractor or visitor attributable to Ministry actions or inaction.	• Significant impact for delivery of multiple services nationally or regionally • Significant long-term implications or disruption for critical services, outputs or outcomes.	• Cost over runs and expenditure exceed budget and contingency funding across multiple appropriations. • Significant loss, mismanagement or misappropriation attributable to Ministry actions or inaction.	• Significant long-standing breach of primary legislation with associated penalties and legal costs as a result of Ministry legal decision or advice.	• Requires Ministerial involvement with Secretary for Education/Executive leadership fully focussed on response. • Sustained and high-profile national media coverage. •
Severe	• Injury or illness with permanent or long-term severe disabling effects and irreversible health damage. Immediate emergency medical assistance and hospitalisation required. • Psychological trauma resulting in immediate inability to continue work in any capacity prior to the trauma incident occurring and requiring medical or professional intervention.	• Substantial disruption for a key service area or region or for a particular part of the system or sector. • Significant implications or disruption for some services, outputs or outcomes and Ministry financial provisions.	• Cost over runs and expenditure exceed budgets for significant nationwide or multiple programmes and projects putting delivery and benefits at risk. Funding redistribution is limited or not available.	• Breach of significant legislation or clauses with associated penalties and legal costs as a result of Ministry legal decision or advice.	• Significant Ministerial attention with Secretary for Education/Executive leadership attention required. • Significant widespread public and/or stakeholder concern. • Focussed national or regional media coverage.
Major	• Injury or illness with temporary significant or severe disabling effects. Advanced first aid or attention by medical services or hospital required. • Psychological trauma resulting in a reduced ability to continue work on the same terms prior to the trauma incident occurring and requiring medical or professional intervention.	• Impacts capability to deliver one or more key processes required for one or more key services. • Quality, time and cost impacts exceed services recovery objectives, standards, contingencies or risk thresholds.	• Cost over runs and expenditure exceed budgets for an operational area of regional programme(s) and project(s) putting delivery and benefits at risk. Funding redistribution is available but will have service delivery impacts.	• Breach or misinterpretation of legislation clauses with associated legal costs as a result of Ministry legal decision or advice. •	• Secretary for Education requires briefings and oversight and significant Executive leadership attention required. • Key stakeholders require additional and regular updates. • Focussed national or regional media coverage.

Proactively released

	Harm & Safety	Service Delivery	Financial	Legislative	Trust & Confidence
Moderate	• Injury or illness with non-severe or temporary disabling effects requiring first aid and/or referral to a medical professional. • Psychological trauma resulting in minor reduction of ability to continue work on the same terms prior to the trauma incident occurring and may require some medical or professional intervention.	• Impacts to quality, timeliness or efficiency of a key process or part of a service. • Limited or capped exposure to disruption, quality, time or cost impacts.	• Cost over runs and expenditure exceed budgets for an operational area or operational project(s). Funding reprioritisation is required.	• Misinterpretation of legislation clauses with associated legal costs and retrospective confirmation as a result of Ministry legal decision or advice.	• Additional Executive or Senior leadership attention required. • Some stakeholders may require additional communications. • Limited national or local media interest or coverage.
Minor	• Minor injury or illness that does not require medical attention and no recovery time is needed. • Psychological trauma resulting in no reduction of ability to continue work on the same terms prior to the trauma incident occurring and may require some medical or professional intervention.	• Minimal or limited impact on key processes or service quality or outputs. • Current business capability can respond and manage.	• Cost over runs and expenditure exceed budgets for an operational activity. Funding and budget contingencies or reprioritisation are available.	• Minor interpretation issues and clarification of processes as a result of Ministry legal decisions or advice.	• Senior leadership or team management oversight to respond and manage. • Minimal or no media interest or coverage.

Proactively released

Table B: Risk Matrix

		Consequence				
Likelihood	**Description**	**Minor**	**Moderate**	**Major**	**Severe**	**Extreme**
Almost Certain	The event or condition is expected to occur in the future (>95% chance of occurring)	**High** 19	**High** 20	**High** 21	**Very High** 23	**Very High** 25
Likely	Events or conditions like this have occurred several times before and are likely to occur again (51 – 95% chance of occurring)	**Medium** 14	**Medium** 15	**High** 16	**Very High** 22	**Very High** 24
Possible	Events or conditions like this could occur and may have occurred once before (21 – 50% chance of occurring)	**Low** 6	**Medium** 10	**Medium** 13	**High** 17	**High** 18
Unlikely	Events or conditions like this could occur but may not have occurred before (5 – 20% chance of occurring)	**Low** 4	**Low** 5	**Medium** 9	**Medium** 11	**Medium** 12
Rare	Events or conditions like this have not occurred and are not expected to occur (<5% chance of occurring)	**Low** 1	**Low** 2	**Low** 3	**Medium** 7	**Medium** 8

Proactively released

Appendix C - Previous PIA risks, privacy responses, and recommended controls

A supplementary document to this appendix provides the detail of the risks, recommendations and controls identified in the previous PIA's for Te Rito:

1. *SISI SMS ESR PIA* (2018)
2. *Learning Support Register PIA* (2019)
3. *Te Rito Data Analysis ESR PIA* (2019)
4. *Te Rito high level discovery PIA* (2021).

This is to enable traceability from the prior work to the current PIA and information security risk assessment.

In the past five years, the scope and design of Te Rito has changed, and change will continue in the future. Therefore, not all the previously identified risks or recommended controls are still relevant.

Where still applicable, all the recommendations for the medium rated risks mentioned below have been implemented or other compensating controls are in place. The full details of the recommendations and control implementations' status is given in the Supplementary document to this appendix.

The documents listed above evaluated many potential risks and associated recommendations. Assuming all recommendations were implemented, the *Data Analysis ESR PIA forecasted* there would be four (4) medium level risks, of which:

- risks DA21 and DA27 are assessed as Medium in this PIA's risk **P-03**
- risks DA1 and DA7 are mitigated and reassessed as low.

The *SISI SMS ESR PIA* forecast three (3) risks to be medium level:

- risk SE-R-08 is assessed as Medium as it is aligned with this PIA's risk **P-03**
- risk SE-R-10 relating to potential security vulnerabilities with SMSs is outside the scope of Te Rito. It is noted as risk **P-04** in terms of schools having suitable controls for IT systems or services they use, which remains assessed as medium. A separate program of work looking at security of SMS solutions remains active, alongside the Cyber Security and Digital Support Programme.
- risk SE-R-07 is mitigated and assessed as low and is related to this PIA's risk **P-15** which is low.

The *Te Rito high level discovery phase PIA* identified two (2) further risks considered to be medium after implementing all recommended controls. Both of these are now mitigated and assessed as low:

- risk PR01, relating to individual student consent, is mitigated via other approaches, particularly parental consent on behalf of their children, reliance upon school Privacy statements for the Purpose of collection or sharing, communications and transparency with parents per this PIA's risk **P-02**. While these other mitigations are implemented PR01 would be aligned with P-15, which is low.
- risk PR02, relating to dual enrolment, has been a focus of work under Te Rito and is now assessed as low per this PIA's risks **P-06** & **P-10**.

Proactively released

Appendix D - Te Rito summary of student data categories

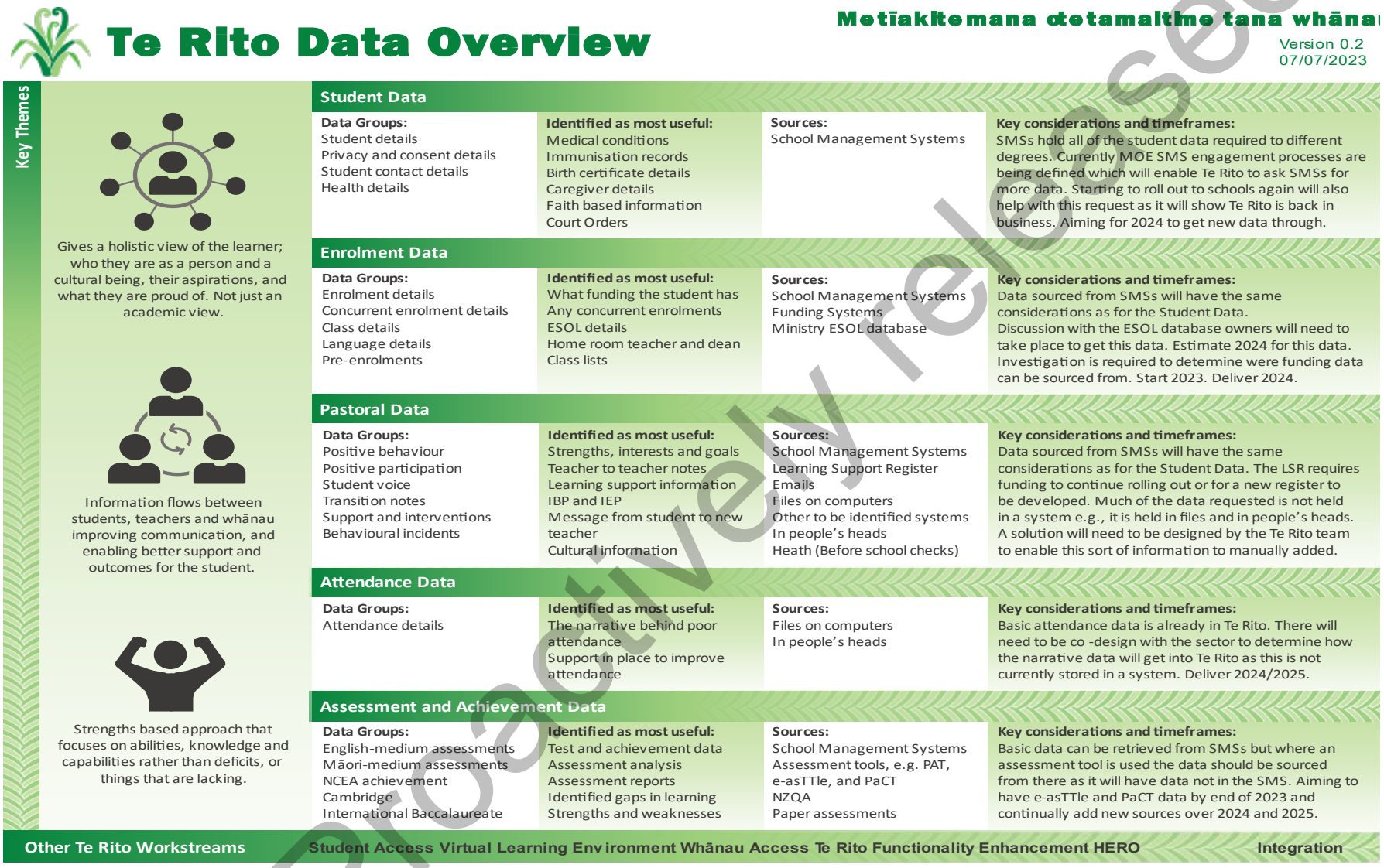


Figure 12: Te Rito - Student Data Overview

Proactively released

Figure 12 above was discussed with the Ngā Rau Whakatupu sector working groups to elaborate the detail of their identified priorities (2nd column) and how Te Rito may, or may not, be able to deliver the requested outcomes. The data categories stored in Te Rito, with a headline of the data contained is below. Te Rito may not store all of the identified information, some may only be stored in an SMS, or remain with schools unstructured storage of email, file shares etc.

- **Student details**: NSN; names; date of birth and age; gender; ethnicity (plus hapu and iwi where applicable); addresses and phone numbers; citizenship, residency and country of origin, with visa details if applicable; birth certificate number; previous schools and/or early childhood attended.
- **Privacy and consent details**: Tick box view of whether consent has been obtained for common scenarios such as consent to share (a) details with Dental Authorities, (b) record with next school; (c) student and caregiver details with Board of Trustees; (d) student details for routine health checks (hearing, sight, vaccination)
- **Caregiver details**: name, relationship, languages, contact details, main caregiver, existence of any custodial or restricted access order, though the detail will not be in Te Rito
- **Temporary caregiver details**: name, relationship, contact details, dates student is with temporary caregiver, reason for temporary care
- **Emergency contact details**: name, relationship, contact details
- **Health details**: high health needs; ORS; health condition; action required; doctor's and dentist's name and contact; (unlikely to be in Te Rito, being considered as part of B4SC) immunisation status and certificate
- **Administrative details**: Information about the school (such as ID, boarding or zoning status); student type; whether full or part time; subjects studied, at what level, for how many hours, and under what qualifications framework; ORS and section 9; first and last attendance dates; funding levels; privacy notes such as withholding contact details.
- **Concurrent enrolment details**: including provider, type of enrolment, start date, and which school is the 'base school'.
- **Language details**: English as a Second Language, other languages spoken, on ESOL programme, Māori medium education (with time in programme and immersion level), Pacific medium education (with language, time and immersion level)
- **Pastoral data**: positive behaviour and participation (specific events, awards, roles and responsibilities, gifts and talents); conditions affecting learner (e.g. death in family, refugee); diagnosed learning or behaviour condition. Excluding behavioural incidents (minor and major).
- **Student voice**: interests
- **Transition notes**: e.g. teacher recommendations for class placement and effective strategies
- **Support and interventions**: details of applicable services being delivered, tending to be related to funding
- **Attendance data**: number of half-day absences; attendance rate
- **Assessment data**: by type, in both English medium and Māori medium assessment
- **Achievement data**: by type in both English medium and Māori medium.
- **Unstructured information:** such as a learner's work

Proactively released

Appendix E - Te Rito All data attributes

The proposed full set of data attributes stored about students, parents, and school staff as of 30/11/2024 is included in the attached document. Some information is not currently stored in Te Rito and is subject to further integration following approval of this PIA. The core information held in Te Rito is marked as **Bold**. Explicitly biometric and geolocation data is not collected or stored by Te Rito.



Te Rito Data 30112024 updated.c

Proactively released

Appendix F - Logical architecture view

The simplified data flow diagram in Figure 4 on page 30 is represented from a logical architecture perspective in Figure 13 and Table 20 below from the solution architecture document.

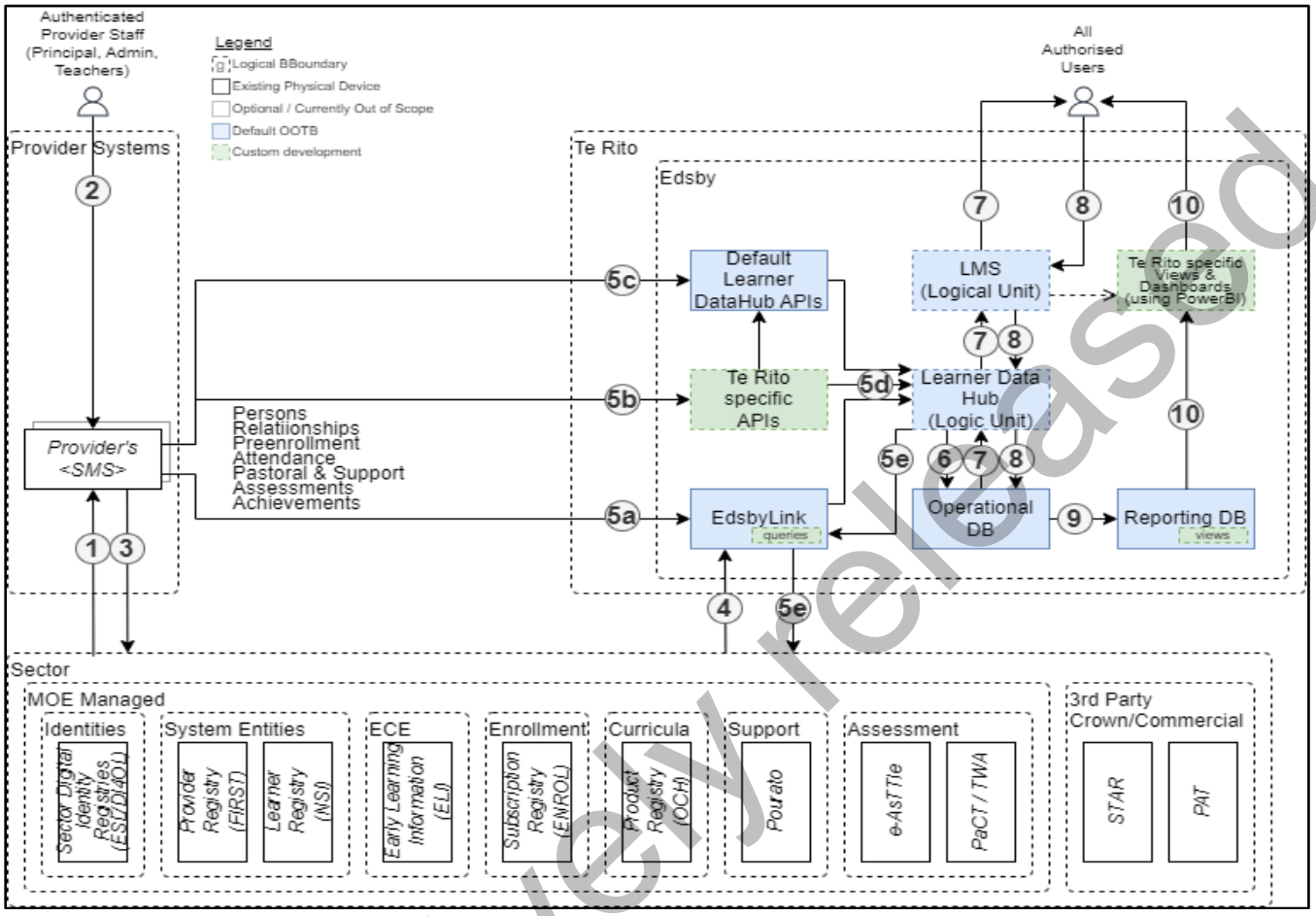


Figure 13: Te Rito data flows – logical view

Table 20: Data flows elaboration

1	A Subset of Data is extracted from Ministry provided Services by individual Provider SMSs.
2	Data is Manually entered by principals, administrators, or teachers into their school's SMS
3	SMS queries Ministry systems for data validation, or sends required information e.g. to ENROL
4	A Subset of Data is extracted from Ministry provided Services by Te Rito. Uses include as Reference data for subsequently validating data incoming from SMSs.
5a	PULL Approach: A Subset of Data is extracted from the SMS via an Edsby Link Service Agent on a scheduled or other trigger basis, and serialised as is & packaged.
5b	PUSH Approach: Alternatively, a subset of Data is sent by the SMS itself invoking Te Rito specific API endpoints. HERO SMS will be the first example.
5c	Data is transformed & validated before acceptance by the Service
5d &e	The subset of Data is compared against Operational Data, validated, homogenised, and transformed before importing into the Service. Flow e is a query for validation, data is not sent out of Te Rito.
6	The data is persisted in the Operational Database.

Proactively released

7	Data is recalled from the database on demand for transformation by the Service into web-based UI Views to support authorised, authenticated, and audited end User operations.
8	Including new Data input from end users, validated by the service, persisted in the Te Rito Operational Database.
9	Data for reporting is regularly exported from the Operational Database to the Te Rito Reporting Database.
10	Reporting Data is rendered via Te Rito customised Power BI enabled web Views (Dashboards).

Proactively released

Appendix G - Document Information

Revision History

Version	Date	Author	Description of Changes
0.1	March 2023 – September 2024	Alan Heward	Drafting. Ministry review. Consultations & review with GCPO & OPC. Split out Appendix C for historical traceability to prior PIAs.
1.0	October 2024	AH	Distribution for approval

Distribution List

Name	Role
Myles Ferris	Chair Te Rau Whakatupu Māori
Graeme Barber	Chair Te Rau Whakatupu Auraki|English
Stuart Wakefield	Chief Digital Officer, Te Rito SRO
Mark Brumby	Te Rito Program Manager
Craig Haywood	Manager Sector Products & Service Delivery – Business Owner
Martin Rothbaum	Enterprise Architect & (former acting) Te Rito Business Owner
Margaret-Anne Barnett	Strategic ICT Business Advisor
Russell Campbell	Te Rito Technical Manager
Sandy Britain	Enterprise Architect
Amy Orr	Senior Technical Architect
Sky Sigal	Solution Architect
Michelle Greenwood	Senior Business Analyst & Technical Writer
Michael Middlemiss	Edsby - Managing Director Asia Pacific
Mike O'Connor	Enterprise Architect – Security
Louise Hull	Digital Policy Advisor
Maya Jones	Manager Privacy
Vanessa Cuthbert-King	Senior Privacy Advisor
Catherine Gavigan-Binnie	Legal
Katrina Young	Chief Data Steward
Dayton Hight	Manager Digital Assurance and Cyber Security
Eve Kennedy Stephanie Gregor	Office of the Privacy Commissioner
Katrine Evans & Clare Ruru	Office of the Government Chief Privacy Officer

Proactively released

References

Table G1: References specific to Te Rito

Title	Date	Source and Link	Comment
Te Rito website	n.d.	Home Page|Te Rito	
Te Rito Privacy Statement and Terms of Use	2023	Privacy statement|Te Rito Terms of use|Te Rito	Updated from 2019 original
Te Rito Student Usage Guidelines	2024	To be published on Te Rito website	
NZBA website - The Te Rito project and Privacy	2024	Sharing Student Information - Te Rito	
Te Rito High Level Discovery PIA	2022	MoE-Te Rito-Privacy Impact Assessment (Discovery Phase).pdf	
Te Rito Core C&A	2023	Memo CA Application - Te Rito Core May 2023	Includes information security risk assessment, security test findings and resolution. Also *Business Impact Levels of Protective Security for Te Rito*.
Te Rito Incident Response Plan	2024	Edsby IRP for Te Rito from 2022 and Ministry IRP updated 2024.	Incident Categorisation | National Cyber Security Centre
Te Rito Solution Architecture Document	2023	Ministry internal	
Te Rito Data	2023	Attached per Appendix E	
Te Rito Roles & Permissions	2023	Ministry internal	Also, Edsby Roles & Permissions
Te Rito Guidance for updating privacy notices	2021	Shared to Principals June 2021 onwards.	Advice to schools about potential updates to school privacy statements considering Te Rito.
Te Rito Information Classification memo	2021	See C&A memo	
SISI Threat Model - draft	2017	Ministry internal	Draft only.
Te Rito Glossary	n.d.		Sector and Technical glossaries
Te Rito Data Kaitiakitanga Group ToR	2023	ToR	
Ngā Rau Whakatupu ToR	2023	Ministry internal	
Te Rito Steering Committee |Te Uru Puia ToR	2023	Ministry internal	Previously known as Executive Oversight Group
Te Rito Engagement and Communications Strategy, and Plan, Change Management Strategy and Plan	2024	Ministry internal	Four discrete and interlinked documents. Specific Change Plans for different deployments will be created.
Building Trust in Te Rito Summary and Detail	2021	Ministry internal documents	Development of human trust framework specific to Te Rito
Te Rito Programme Assurance Strategy, Quality & Assurance plan	2024	Ministry Internal	
Data Analysis ESR PIA & SISI SMS ESR PIA	2018	Both Ministry internal	
Learning Support Register PIA	2019	Ministry internal	
Business Context workshop Te Rito PIA	2021	Ministry internal	Notes & Minutes from workshop
Privacy protocol template	2021	Ministry internal	For Te Rito & non-Te Rito, User School & User Cluster templates.
Te Rito Roadmap	2023	Ministry internal	Strategic initiative, five year plan, 6-12 month roadmap
Integrated Education Data (iED) detailed business case	2018	Ministry internal	Quotations are from various pages.
Identification Risk Assessment	2023	Ministry internal	Te Rito sector staff
Edsby assurance documentation and collateral	Var	ISO27001 Statement of Applicability & Certification report. Security testing report. DR Plan & DR test report.	Public assurances About Edsby, User Data and Privacy Also Edsby (vimeo.com) Plus, HubSpot SOC3 report.
Edsby Privacy Policy	var	www.edsby.com/privacy-policy	Updated August 2024 Privacy policies updated
Commonsense Privacy assessment of Edsby	2023	Edsby - Privacy Evaluation (commonsense.org)	
ST4S assessment of Edsby	2024	Safer Technologies for Schools (ST4S) - NZ	

Table G2: Other Ministry documents

Title	Date	Source and Link	Comment
Education Counts	n.d.	Education Counts	Data source for various statistics
SMS Vendor PIA's	2022	Ministry internal	PIA reviews of multiple SMS vendors
SMS Data Exchange (SDEX) Service PIA	2006	Ministry internal	Now known as Student Record Transfer Service (SRTS).
FIRST PTA & C&A memo	2021	Ministry internal	
PaCT PIA	2023	Ministry internal	PaCT website

Proactively released

Title	Date	Source and Link	Comment
e-asTTle	var	Ministry internal	e-asTTle website & documentation
ELI PIA ELI PTA update	2024 2019	Ministry Internal	
ESL CA & Information Classification memo	2022	Ministry internal	Education Sector Logon C&A memo from January 2022
DI4OL C&A memo	2022	Ministry internal	Includes Security Risk Assessment of DI4OL
DI4OL PIA	2022 2024	DI4OL PIA for proactive release PIA v1.1 Ministry internal	Plus a Plain language summary v1.1 v1.1 of PIA approved April 2024. Now renamed Learner Identity Broker
Identification Risk Assessment – DI4OL	2023	Ministry internal	Te Rito students
MoE Information Security Controls catalogue	2021	Ministry internal	Derived from Secure Controls Framework (SCF) catalogue
Enterprise Risk Management Framework	2023	Ministry internal	Updated August 2023
Schools Records Retention / Disposal Information Pack	2022	Archiving and disposing of school records – Education in New Zealand	assets.education.govt.nz/public/Records/School-Records-Retention-and-Disposal-Schedule-All.pdf (SRRDS)
Sharing Information in schools	2022	[Sharing ref 1] Enrolling and starting your child at school – Parents.education.govt.nz – Practical information about education for parents and carers [sharing ref 2] Sharing information – Education in New Zealand Sharing personal information	Ministry guidance to schools on sharing student information
Education Counts – Transient Students	2022	Transient students | Education Counts	Plus ibid 2022 Indicators Report
About Safer Technology for Schools (ST4S)	2023	Safer Technologies for Schools (ST4S) – NZ Safer Technologies 4 Schools – st4s.edu.au	Ministry introduction to ST4S. Official ST4S website and guide.
Connected Ako: Digital and Data for Learning Strategy	2023	Connected Ako: Digital and Data for Learning	
Assessing the privacy implications of new tech	June 2024	Education Gazette Issue 103.7	

Table G3: Other references

Title	Date	Source and Link	Comment
Microsoft assurance documentation	var	docs.microsoft.com/en-us/compliance/regulatory/offering & Privacy and Security for Schools - Microsoft Education	ISO Certifications, SOC2 reports, CSA questionnaires. Microsoft for Education privacy overview links to Microsoft Trust Center
Azure IRAP	2021	Microsoft Azure IRAP Cyber.gov.au - IRAP	Aus IRAP issued August 2019, replaced with Aus CSP in 2021.
Azure GCDO	2021	Microsoft on NZ Security and Privacy Considerations	
TMR Māori Data Sovereignty Principles	2018 2022	Te Mana Raraunga & Compendium of Māori Data Sovereignty v2	
DPUP	var	Data Protection and Use Policy	Reference links from Part 4 DPUP
Public Service Commission – Code of Conduct	2022	Integrity and conduct	
Teaching Council code of conduct	2019	Our Code, Our Standards	
Code of Conduct for School Board members - MoE	2023	Code of Conduct for School Board members	
NSN Gazette Notice	2023	Education (National Student Numbers) Notice 2023 - 2023-go4534 - New Zealand Gazette	
Education (2024 School Staffing) Order 2023	2023	Education (2024 School Staffing) Order 2023 (SLSRTS 2023/209) 25 Employment of principals – New Zealand Legislation	Definition of roles such as Dean, Deputy Principal s25 onwards.
Privacy in Schools	2009	OPC Guidance - Privacy-in-Schools-September-2009	OPC publication of guidance
Health Information Privacy Code (HIPC) – OPC	2022	Health Information Privacy Code 2020	
NZ Privacy Concerns and Sharing Data survey - OPC	2018 2020	Privacy-concerns-and-sharing-data-survey-Mar-Apr-2018.pptx Privacy-concerns-and-sharing-data-OPC-reportApr-20.pdf	NZ specific survey data on public attitudes and perceptions relating to privacy.
Australian Community Attitudes to Privacy Survey	2023	Australian Community Attitudes to Privacy Survey | OAIC	Office of the Australian Information Commissioner
Australian eSafety Commissioner Safety by Design	2019	Safety by Design | eSafety Commissioner	
Protecting privacy while supporting students who change schools	2019	protecting-privacy-while-supporting-students-who-change-schools/	US Centre for Democracy & Technology
NZ Govt Treasury Student Mobility across schools	2015	Treasury Student Mobility	Using StatsIDI data

Proactively released

Title	Date	Source and Link	Comment
NZCER Student movement and schools	2007	Student movement and schools - what are the issues? | New Zealand Council for Educational Research	
Student privacy pledge	2020	Signatories 2.0 - Pledge to Parents and Students	Independent USA org campaigning to protect student privacy.
IEEE 2089 Standard for an Age Appropriate Digital Services Framework	2021	IEEE SA - IEEE 2089-2021	Based on UK ICO AADC & 5Rights work
Age appropriate design and self-assessment risk tool UK Information Commissioners Office (ICO)	2021	Age appropriate design: a code of practice for online services|ICO Children's Code Self-Assessment Risk Tool|ICO	Additional ICO references What is special category data?|ICO & designing-data-transparency-for-children.pdf (ico.org.uk)
UK GDPR guidance - UK ICO	n.d.	Special category data | ICO	
Defend Digital Me about UK ICO audit of UK DfE	2022	The ICO audit of UK Department for Education two years on|Defend Digital Me	Also UK Department for Education warned about learning records database|UK ICO
5Rights Foundation	2023 2017	Digital Childhood Development Milestones digital-childhood---final-report	Other resources relating to Children's privacy in a digital context DFC publications list Jul 2023
United Nations Convention on the Rights of the Child (UNCRC) General Comment 25	1989 2021	Convention on the Rights of the Child | OHCHR General comment No. 25 on children's rights in relation to the digital environment	Also The Convention on the Rights of the Child: The children's version | UNICEF Also from 5Rights UNCRC GC25 Explanatory Notes & In_Our_Own_Words_Young_Peoples_Version & Our Rights in a Digital World
Te Reo translation of UNCRC	2005	CRC Māori translation	UN Convention on the Rights of the Child | New Zealand Ministry of Justice
International Association of Privacy Professionals (IAPP)	var	Childrens_Privacy_Whitepaper	Various resources relating to Children's privacy
Privacy for the Homo Digitalis	2016	Privacy for the Homo Digitalis by Lokke Moerel, Corien Prins	Discussion of using best interests instead of relying upon consent as the sole authority to process data.
Children's Privacy across cultures.	2022	Livingstone et al Childrens privacy across cultures	London School of Economics (LSE)
Children's data and privacy online	2019	Childrens-data-and-privacy-online-report	Plus, LSE website at www.myprivacy.uk
State of CyberSecurity	2022	State of CyberSecurity in Education	LSE
Common Sense State of Kids Privacy	2021	common-sense-2021-state-of-kids-privacy	
StatsNZ family and household composition data Publications | Stats NZ	Var & 2021	New data shows 1 in 9 children under the age of five lives in a multi-family household | Stats NZ Family and household projections: 2018(base)–2043 | Stats NZ	

Proactively released

Proactively released