Te Tāhuhu o te Mātauranga
Ministry of Education

Please note: The PIA was prepared at an earlier stage in the programme's development. Many of the recommendations have either been addressed or are currently being worked through. The PIA should therefore be read as reflecting the point in time at which it was developed and not the current state of the project.

Privacy Impact Assessment

Student, Measurement, Achievement and Reporting Tool (SMART)

Assessment ID: PP-295

Released under the Official Information Act 1982

Te Kāwanatanga o Aotearoa
New Zealand Government

Contents

1. Document Information 2
1.1. Revision History 2
1.2. Internal Consultation 2
2. Approvals 3
3. Related Documents 4
4. Executive Summary 5
4.1. Summary 5
4.2. Scope of Assessment 6
4.2.1. Out of Scope 7
4.3. Dependencies 7
5. Summary of Findings 10
5.1. Summary of Privacy Risks 10
5.2. Agreed Privacy Enhancing Actions 10
5.3. Summary of Recommended Actions 13
6. Initiative/Solution Information 15
6.1. Key Stakeholders 15
6.2. Initiative/Solution Overview 15
6.3. Legal Authority and Context 24
6.4. Collection 26
6.5 Storage and Security 32
6.5.1. Information Classification 36
6.6. Access and Correction 36
6.7. Accuracy and Data Quality 37
6.8. Retention and Disposal 37
6.9. Use 39
6.10. External Sharing 40
6.11 Unique Identifiers 40
7. Compliance Assessment 43
8. Risk Assessment 65
Definitions 65
Appendix 1: Ministry Risk Assessment Methodology 71
Appendix – Data Elements 77

Released under the Official Information Act 1982

1. Document Information

1.1. Revision History

Version	Date	Author	Description of Changes
0.1	14/7/2022	9(2)(a)	Initial Draft
0.2	09/09/25	9(2)(a) Simply Privacy Ltd	Amending and completing initial draft; conducting analysis and completing compliance and risk assessments
0.3	22/9/2025	9(2)(a) .	Feedback Changes
0.4	29/9/2025	9(2)(a) Simply Privacy Ltd	Updates from feedback
0.5	6/10/2025	9(2)(a)	Updates form Records Team
0.6	4/11/2025	9(2)(a)	Updates from Privacy Team
0.7	13/11/2025	9(2)(a)	Updated from Records Team
0.8	17/11/2025	9(2)(a) Simply Privacy	Review and signature

1.2. Internal Consultation

The following internal stakeholders have been consulted or have otherwise contributed to the preparation of this assessment.

Name	Role	Date
9(2)(a)	Technology Programme Manager	6/10/2025
9(2)(a)	Senior Privacy Advisor	29/10/2025

Released under the Official Information Act 1982

2. Approvals

The following **Privacy Subject Matter Expert** (SME) endorses and acknowledges that the appropriate privacy risks and privacy enhancing actions have been identified. The findings and recommended privacy enhancing actions in this report are not a legal opinion.

Privacy Comment		
<This section will be completed as needed by the Privacy team to provide the Business Owner with information on any qualifications or caveats relevant to Privacy sign-off>		
Name and Position	**Signature**	**Date**
9(2)(a) 9(2)(a) Simply Privacy	9(2)(a)	17 Nov 2025

The following **project/initiative PIA lead** endorses and acknowledges the identified risks and recommended privacy enhancing actions.

Name and Position	Signature	Date
9(2)(a) Programme Director Curriculum and Assessment Change Programmme	9(2)(a)	

The **Business Owner** approves and accepts the risks identified in this Privacy Impact Assessment and is responsible for ensuring that the agreed privacy enhancing actions are implemented.

Name and Position	Signature	Date
Kiritina Johnstone General Manager, Te Uepū Reo Māori Te Poutāhū		24 Nov 2025

Released Under the Official Information Act 1982

3. Related Documents

Document reference	Document title and link	Author	Version/Date/Date Accessed
D01	Original Brief Privacy Assessment (10/24) (**BPA)**	9(2)(a)	24/10/2024
D02	Updated Brief Privacy Assessment (**Updated BPA**)	9(2)(a)	8/7/2025
D03	Assessment and Aromatawai Tool – Data Security Classification (**Security classification**)	9(2)(a)	29/7/2025
D06	Single Stage Business Case (**SSBC**)	9(2)(a) with the following contributors: 9(2)(a) Technical advisory 9(2)(a) – Procurement specialist responsible for Commercial Case 9(2)(a) – Financial cost model 9(2)(a) – Benefits profile assistance	17/1/2025

Released under the Official Information Act 1982

4. Executive Summary

4.1. Summary

This PIA considers the privacy impacts of the deployment by Te Tāhuhu o te Mātauranga | The Ministry of Education (the **Ministry**; **MoE**) of the Student, Measurement, Achievement and Reporting Tool **(SMART**; the **solution**). SMART is a digital platform designed to support teaching and learning by providing a consistent way to deliver, manage, and report on student | ākonga assessments across the New Zealand education system.

SMART will be delivered as a software-as-a-service platform by Janison Solutions Pty Ltd (**Janison**), an ASX-listed company that provides online assessment and learning solutions around the world. Personal information in SMART will be hosted by Janison in Microsoft Azure NZ, with disaster recovery in Sydney. Security measures that include role-based access controls, encryption, access logging and audit trails.

SMART will replace the legacy "e-asTTle" tool and will deliver twice-yearly assessments across key learning domains for students | ākonga in Years 3–8, with potential extension to Years 9–10. It is designed to improve fairness, reduce teacher | kaiako workload and provide consistent national data to support teaching practice and system-level decision-making.

A large volume of personal information, particularly of students | ākonga, will be handled by the solution. The personal information of children is considered sensitive given children's inherent vulnerability and more limited agency than adults. It is expected that the personal information of approximately 432,000 children | tamariki, 22,400 teachers | kaiako and 6,160 school | kura administrators will be processed to assess and report on student achievement and progress across the New Zealand education system.

The Ministry remains accountable under the Privacy Act 2020 (**Privacy Act**) for all personal information in SMART, with Janison handling that information as the Ministry's "agent" under section 11 of the Privacy Act.

Key findings

- **Overall view:** SMART aims to deliver educational benefits for students | ākonga, teachers | kaiako, schools | kura and the Ministry. While the privacy risks are not negligible, particularly around transparency, accuracy, use limitation and retention, they are manageable with appropriate targeted controls.
- **Compliance:** SMART is broadly compliant with the Information Privacy Principles (**IPPs**) in the Privacy Act. The information provided indicates that the collection of personal information is lawful and proportionate to education purposes (IPP 1), with the predominantly indirect collection of personal information by the Ministry through schools being generally justifiable under exceptions in IPP 2 and IPP 3A. However, current transparency arrangements for direct collection activities are incomplete and a dedicated privacy statement for SMART is required (IPP 3). Accuracy obligations (IPP 8) and retention/disposal requirements (IPP 9) depend on Ministry and school processes being designed and implemented.
- **Risk assessment:** Most of the identified risks are rated medium under current controls, moving to low or medium residual risk ratings where the recommended actions are implemented.

Released under the Official Information Act 1982

- **Transparency:** The Ministry has not developed a clear privacy statement for SMART and may be perceived as not sufficiently transparent about the way personal information is indirectly collected and processed in SMART (noting we consider available exceptions will mean the Ministry is likely to be compliant under the incoming IPP 3A) (R01, R02).
- **Accuracy:** Inaccurate personal information from school Student Management Systems (**SMS**) may be imported into and relied on in SMART, leading to potential errors, unfair outcomes and unreliable decision-making (R04).
- **Data retention:** Potential excessive retention of personal information given the criteria and processes for the retention and disposal of personal information in SMART are yet to be defined or implemented (R05).
- **Scope creep:** There is potential for scope creep if SMART data is later re-purposed without adequate governance processes in place (R06).
- **Security:** The overall security posture of the platform at the time of drafting appears to be sound, noting this is not a formal security assessment (which will be conducted via the Ministry's formal Certification and Assurance process (**C&A**), to be completed separately). We note that but the potential severity of any security breaches means that even the limited security-related risks we found still present a Medium residual risk (R03).

Key recommendations

1. Publish a clear, age-appropriate SMART Privacy Statement for students | ākonga, their families | whānau and educators before full deployment (IPP 3). The Ministry also has an important education sector-wide role to play in raising awareness of privacy issues and supporting school transparency efforts, for example by providing schools with templated privacy notice wording.
2. Finalise the agreement with Janison, ensuring appropriate and enforceable contractual obligations are placed on Janison in respect of its role as a data processor and handling of the personal information in SMART.
3. Carefully assess and address potential data quality and accuracy issues in SMART, including conducing an AI Impact Assessment where generative AI is used in the Platform.
4. Establish, document and operationalise rules and processes for personal information retention and disposal and the monitoring of secondary uses of SMART data to prevent scope creep (i.e. use of personal information beyond the purpose for which it was originally collected).

By implementing these recommendations, the Ministry can ensure SMART achieves the intended educational outcomes while remaining consistent with the Privacy Act and minimising related risks. Ongoing oversight and proactive communication will be critical to maintaining trust and managing residual risks as SMART is embedded and scaled.

4.2. Scope of Assessment

This PIA considers the collection and processing in SMART of the personal information of New Zealand students | ākonga, teachers | kaiako and school | kura administration staff.

It assesses compliance with the Privacy Act, incorporating consideration of other legislation as relevant, including the Education and Training Act 2020, the Public Records Act 2005, the Education (School Boards)

Released under the Official Information Act 1982

Regulations 2020 and the Education (National Student Numbers) Notice 2023. It identifies key privacy and broader privacy-related risks.

In preparing this assessment, Simply Privacy has relied upon information, statements and representations provided by the Ministry. Simply Privacy provides no warranty of completeness, accuracy or reliability in relation to any such information, statements or representations. This assessment is not legal advice and its contents should not be treated as a legal opinion.

4.2.1. Out of Scope

This PIA does not consider the handling within SMART of the personal information of Ministry staff, school compliance with the Privacy Act, the use of generative AI in the platform or the use of SMART by a small number of "realm" schools from the Pacific Island. We understand that, in the case of realm schools, information will transit from New Zealand to the relevant country.

This PIA does not consider compliance with any laws other than those stated above. While it considers and may identify high-level security risks, it does not consider technical security risks associated with SMART and is not a security assessment. Those issues will be considered in the separate C&A process to be undertaken by the Ministry.

4.3. Dependencies

This section identifies relevant privacy assessments and any known issues with implementation of privacy enhancing controls that could impact the compliance of SMART.

Any issues identified in this section are not owned by the SMART Business Owner. However, any variations to handling of information within a solution that are specified by SMART and/or differ from an established pattern, for example access settings and policies, are considered the responsibility of the Business Owner.

The Privacy team has not yet established a monitoring and renewal process for privacy assessments. It currently relies on the business to initiate renewal of privacy assessments, which is typically triggered by Certification and Accreditation renewal. Therefore, older privacy assessments may not reflect an initiative or solution's current privacy risk profile.

Released under the Official Information Act 1982

Solution Name	Privacy Assessment Status	Comments
ESL: Teachers and school administrators will log into SMART using a single sign-on service provided by the Education Sector Logon (ESL), the Ministry's main identity and access management service across the education sector. ESL holds personal information like the names, email addresses, roles and schools of staff and school administrators, which is used to verify an individuals' identity and role.	Current – September 2025	• Risk identified relating to devolved access management relevant to the use of ESL to authenticate users to the Attendance Service CMS • The risk relates specifically to the use of the delegated authoriser model • The Privacy team recommended that the ESL Business Owner considered implementing additional actions to reduce the risk likelihood
Learner Identity Broker (formerly DI4OL – Digital Identity for Online Learning)	Current – updated in June 2025	Medium rated risks identified relating to: - transparency with learners, or their parents/guardians, about the purpose of collection and disclosure to the Ministry. - unauthorised disclosure of student information cause by ineffective or insufficient safeguards implemented by schools.

Released under the Official Information Act 1982

Solution Name	Privacy Assessment Status	Comments
Education Data Warehouse (EDW)	Completed in 2021 (Reference: PP-115)	Access to EDW is guided by the EDW Access Control Policy, which was developed in 2021 and appears to be final but lacks all signatures. This policy sets out protocols for monitoring and auditing access to the EDW. • Role Based Access Controls (RBAC) are achieved using Active Directory lists which are regularly audited by the Manager Data Warehousing. Responsibility for this post restructure will likely be the Data Delivery Platform Manager or delegate.

Released under the Official Information Act 1982

5. Summary of Findings

5.1. Summary of Privacy Risks

A total of six privacy risks have been identified through the assessment. The full risk assessment is located in Section 8 of this document and the risk assessment methodology is located in Appendix 1.

Current Risk Rating	Risk ID	Risk Description	Residual Risk Rating
High	R04	Inaccurate personal information leads to errors, unfair outcomes and unreliable decision-making	**Medium**
Medium	R01	Lack of transparency for direct collection	**Low**
	R02	Perceived lack of transparency for indirect collection	**Low**
	R03	Security breach	**Medium**
	R05	Personal information is retained excessively	**Medium**
	R06	Scope creep breaches purpose and use limitation obligations	**Low**

5.2. Agreed Privacy Enhancing Actions

After consultation with the Business Owner the following privacy enhancing actions will be implemented.

Action Reference	Action Description	Associated Risk IDs	Associated IPPs	Action Owner and Target Resolution Date
R01-1 R02-1	Develop a compliant, age appropriate Privacy Statement.	R01 R02	IPP3	19/12/2025 SMART - Project
R01-2 R02-2	Publish a SMART privacy statement	R01 R02	IPP3	19/12/2025 SMART – Project
R01-3 R02-3	Provide age appropriate point in time privacy notices at relevant points within SMART.	R01 R02	IPP3	19/12/2025 SMART - Project
R03-2 R06-3	Finalise the contract with Janison so it is clearly identified as a processor	R03 R06	IPP11 IPP12	5 / 12 / 2025 SMART Project

Released under the Official Information Act 1982

Action Reference	Action Description	Associated Risk IDs	Associated IPPs	Action Owner and Target Resolution Date
R04-1	Implement automatic alerting of data mismatches or anomalies (e.g. same NSN linked to two schools; mismatched age/year)	R04	IPP8	19/12/2025 SMART Project
R04-2	Build error detection into SMART automated scoring to identify misconfigured items before they impact students.	R04	IPP8	19/12/2025 SMART Project
R04-3	Apply data quality checks before SMART pushes results to the EDW	R04	IPP8	19/12/2025 SMART Project
R04-4	Regularly remind schools to strengthen validation rules in the SMS, including checking the accuracy of key fields.	R04	IPP8	19/12/2025 Te Poutāhū Change Management and Training

Released under the Official Information Act 1982

Action Reference	Action Description	Associated Risk IDs	Associated IPPs	Action Owner and Target Resolution Date
R05-1	Once the Temporary Care Records Protection is lifted, it is anticipated that retention and disposal will be governed by the School Retention and Disposal Schedule, Class Student Records 1.7 Records relating to individual students kept by the school and not transferred to the student's next school. Recommended action: Keep until all operational/administrative actions and reporting actions have been completed by the school. Should any revisions occur Record Services will provide guidance to the business.	R05	IPP9	Once Temporary Care Record is revised. Ministry Records Services Team to advice business SMART – Project (Implementation)
R05-2	Ensure Janison is contractually required to provide the Ministry with the capability to remove information from SMART to support its compliance with IPP 9	R05	IPP9	5 / 12 / 2025 SMART - Project
R06-1	Document the Ministry's purposes for collecting personal information in SMART, including in SMART privacy notices	R06	IPP1	19/12/2025 SMART Project.
R06-2	Maintain strict governance processes for approving requests for new uses of SMART personal information, including updated PIAs and privacy notice updates.	R06	IPP1	From go-live Ministry Digital Product Management and Te Poutāhū Business Owner

Released under the Official Information Act 1982

Action Reference	Action Description	Associated Risk IDs	Associated IPPs	Action Owner and Target Resolution Date
R06-4	Conduct regular sampling of access log data. Consider adopting anomaly detection to highlight unusual access patterns.	R06	IPP5	From go-live SMART Project
R06-5	Conduct an AI Impact Assessment to identify key risks and mitigants, including in relation to accuracy issues (e.g. "hallucinations") and bias risks.	R06	IPP8	19/12/2025 SMART Project

5.3. Summary of Recommended Actions

The Risk Assessment in Section 8 includes several recommended actions to support best privacy practice that have not been agreed by the Business Owner. Therefore, they are not included in Section 5.2. The recommended actions and the Business Owner rationale for not agreeing to them is described in the following table.

Released under the Official Information Act 1982

Action Reference	Action Description	Associated Risk IDs	Impact on Risk Rating	Business Owner Rationale
R02-1	Support school compliance with IPP 3 by providing template privacy notice wording to schools that references the indirect collection of personal information by the Ministry.	R02	Low	A sector wide initiative is needed to improve the current privacy and information use statements provided by schools | kura. This initiative falls outside the scope of the SMART project. Privacy team comment: For efficiency, the Privacy team's preference is that Te Poutāhū develops and disseminates an overarching privacy statement targeted at parents/guardians disclosing all its assessment and achievement collection activity. However, as at time of writing there is no guarantee that joined-up communication will progress, a specific action is recommended for the initiative to own. Business owner response. This remains out of scope.
R03-1	Automate RBAC updates	R03	Low	A fully automated RBAC implementation originating from on-boarding through to application role assignment is an enterprise-wide consideration and falls outside the scope of the SMART implementation.

Released under the Official Information Act 1982

6. Initiative/Solution Information

6.1. Key Stakeholders

Stakeholder Type	Name and Role
Business Owner (Risk)	Kiritina Johnstone General Manager, Te Uepū Reo Māori Te Poutāhū
Project Sponsor (Initiative/Solution)	Pauline Cleaver Hautū | Deputy Secretary Te Poutāhū
Product Manager	9(2)(a) Product Manager Te Pou Rangatōpū
9(2)(a)	Solution Architect
9(2)(a)	Senior Advisor | Records Services
9(2)(a)	9(2)(a) | Enterprise Data Architect, Digital

This PIA considers the privacy impacts of using SMART to assess and report on student | ākonga achievement and progress across the New Zealand education system. While the personal information of student | ākonga, teachers | kaiako and school | kura administrators will be handled by the solution, this PIA focuses on the personal information of students, teachers and school administrators only.

6.2. Initiative/Solution Overview

6.2.1 Overview

The Student, Measurement, Achievement and Reporting Tool (**SMART**; the **solution**) is a new Te Tāhuhu o te Mātauranga | The Ministry of Education (the **Ministry**; **MoE**) digital platform designed to support teaching and learning by providing a consistent way to deliver, manage, and report on student | ākonga assessments.

- **Purpose**: SMART will give teachers | kaiako and schools | kura a system to conduct assessments and record results that can inform teaching practice and support equity in education. Those results will also help the Ministry identify where educational resources are most needed across the country.
- **Data**: Most personal information used in SMART comes indirectly from schools | kura. That data comes either from each school's Student Management System (**SMS**), where it is already collected for enrolment and teaching, or to set up single sign-on (**SSO**) access to SMART and other Ministry systems for students | ākonga, teachers | kaiako and school | kura administration staff. The only

Released under the Official Information Act 1982

personal information the Ministry collects directly into SMART relates to student assessment results and accessibility settings.

- **Benefits**: SMART is intended to improve the consistency and fairness of assessment delivery, reduce administrative burden on schools and give teachers better information to support student progress. At the system level, it enables the Ministry to monitor achievement patterns and support equity, without creating public "league tables" or disclosing personal information inappropriately.

SMART will eventually replace the Electronic Assessment Tools for Teaching and Learning (**e-asTTle**), an online curriculum assessment tool developed to assess students' achievement and progress. SMART aims to address the various limitations of e-asTTle, which is constrained by an ageing, bespoke design that limits enhancements and integration and includes assessment content that is outdated, misaligned with the updated curricula and culturally/linguistically inappropriate in places. It also relies on a mix of manual and automated marking, which can create heavy workload for teachers. In addition, a PIA conducted on e-asTTle identified various privacy risks including potential unfair collection methods (IPP 4), over-permissive teacher access (IPP 5) and the lack of disposal functionality leading to over-retention (IPP 9).

In its place, SMART will enable twice-yearly assessments for all students | ākonga in Years 3–8 across six learning domains, with the option to extend to Years 9–10. SMART is expected to generate consistent data about student learning to:

- provide the teacher | kaiako and school | kura with a view of the student's progression aligned to the New Zealand Curriculum (**NZC**) | Te Marautanga o Aotearoa (**TMoA**);
- inform the student | ākonga and their parents and whānau about their learning progress and next learning steps, noting this will be generated in SMART but provided to parents and whānau by schools from SMS data; and
- support decisions at all levels of the education system, including meeting government targets for student achievement.

6.2.2 Background and context

This project is part of the assessment and aromatawai workstream of the wider Curriculum and Assessment Change Programme (**CACP**). The CACP is a multi-year work programme (spanning 2021-2027) being delivered by the Ministry that will make significant changes to the national curriculum ecosystem, including associated curricula, teaching and learning resources. That includes introducing a strategically driven, whole-of-pathway approach to assessment, aromatawai, reporting and monitoring that will make good quality data about students' learning available to inform teaching and learning, provide timely information to parents, whānau and caregivers, and inform decisions at every level of the education system.

The practice of aromatawai is a holistic, indigenous approach to learning and teaching that uses assessment as a deliberate and considered way of understanding mokopuna Māori and their learning journey. It is not derived from Western education models of measurement or used to judge or rank. An aromatawai approach provides indigenous ways of confirming ākonga progress, achievement, success and next learning steps.

It is envisaged that SMART will be an up-to-date assessment and aromatawai tool aligned to the updated New Zealand Curriculum (**NZC**) and Te Marautanga o Aotearoa (**TMoA**) to assist teachers and kaiako to support students and ākonga on their learning journey.

Released under the Official Information Act 1982

6.2.3 About the solution

Following completion of Request for Information and Request for Proposal processes, the Ministry selected Janison Solutions Pty Ltd (**Janison**) to deliver the SMART solution. The solution has been re-named as SMART from its original name of "Assessment and Aromatawai" (**AAT**).

Janison is an Australian-owned, ASX-listed company that provides online assessment and learning solutions. It develops digital platforms used by schools, governments and professional bodies to deliver large-scale digital assessments. Its online assessment platform, Janison Insights, is used in more than 117 countries, including the Australian National Assessment Program – Literacy and Numeracy.

Janison Insights, which underpins SMART, was developed in collaboration with multiple education authorities, including the OECD (for PISA for Schools), state and national government bodies and professional institutions like the British Council and Chartered Accountants ANZ. It is designed to accommodate high-volume testing scenarios and supports features such as offline test delivery, multi-factor authentication, role-based access controls, and integration with external systems.

Janison was selected as the provider of SMART based on an assessment of the Janison Insights platform. Janison's solution was assessed positively for its reliability, scalability and strong support for educators | kaiako, including helping schools use assessment data to improve learning outcomes.

Janison will deliver SMART as a Software as a Service solution in an environment dedicated to the Ministry. Janison hosts and runs SMART, including the platform, servers and cloud environment. It is responsible for the technical operation of the SMART platform, including availability, performance, security monitoring, backups and patching.

6.2.4 Data classification

Data has been classified as "IN-CONFIDENCE" under the New Zealand Government Information Security Manual (**NZISM**), which details the processes and controls that are essential for the protection of New Zealand Government information and systems.

The IN-CONFIDENCE classification reflects that a compromise of information will have impacts that include adverse impacts on the privacy of New Zealand citizens. It is used when unauthorised disclosure could cause harm to the organisation, government or individuals and is intended for official information that is not suitable for public release but does not warrant the higher protection of SENSITIVE. Handling expectations of IN-CONFIDENCE classified data include that it should only be accessed on a need-to-know basis, can usually be stored and transmitted within standard government ICT systems accredited for IN-CONFIDENCE and, if sent externally, agencies are expected to apply reasonable safeguards (e.g. encryption). Disposal of information should be by secure means.

6.2.5 Role of the Ministry

The Ministry will provide access to SMART to students | ākonga, teachers | kaiako and schools | kura for the purposes of assessing and reporting on student learning. The Ministry will also use the information collected

Released Under the Official Information Act 1982

into and generated by SMART to inform decision-making across the education system, including in relation to resourcing and support in meeting government targets for student achievement. To do this, the Ministry will analyse SMART data in its Education Data Warehouse (**EDW**). Assessment results from SMART will be stored in the EDW for research and longitudinal and education-system level summarised reporting.

As such, the Ministry is responsible for the governance and use of SMART, including deciding what personal information goes into SMART, compliance with the Privacy Act 2020 and Ministry data policies, providing secure access to SMART for students | ākonga, teachers | kaiako and administrators and managing system-level reporting and transfer of results into the EDW.

6.2.6 Relationship between the Ministry and Janison

Section 11 of the Privacy Act 2020 (**Privacy Act**) states that an **"**agency**"** (i.e. the Ministry) remains responsible for personal information even when it is held by another party on its behalf, referred to in section 11 as an "agent". This means the Ministry is accountable for ensuring compliance with the Information Privacy Principles (**IPPs**) in the Privacy Act even where Janison is doing the day-to-day processing of that information.

As an agent or "**data processor**", Janison hosts the SMART platform, provides technical and security services and processes personal information on instruction from the Ministry for the purposes of delivering SMART.

As an agent/data processor under section 11, Janison cannot use or disclose any personal information made available to it via SMART for its own purposes. The Ministry's contract with Janison (which is still under negotiation at the time of drafting this PIA report) will therefore need to be clear that Janison has no independent rights to use the personal information, including using personal information from SMART for its own analytics purposes or to share such information with other customers.

6.2.7 How SMART is used by educators

The Ministry will structure and develop the twice-yearly assessments as follows.

- The Ministry will set an "**assessment"**, which is a structured test designed to evaluate a learner's knowledge, skills or competencies.
- Each assessment will be composed of individual "**items",** namely questions or tasks designed to measure specific skills or knowledge.
- Items will be stored in an "**item bank**", which is a centralised repository that enables educators and psychometricians to manage, organise and reuse content.
- The effectiveness of each item will be evaluated through "**item performance"** metrics, which help determine how well the item measures learning and whether it aligns with curriculum goals. This is a key concept in assessment design and evaluation that helps assess whether each item is effective, fair and aligned with learning objectives.
- The Ministry engages external **psychometricians** to measure the quality and fairness of assessments by testing items to see how they are performing, particularly for different demographic groups. In the context of SMART, psychometricians will get a data extract showing each item, how students answered it and some general demographic information for each student (e.g., year level, possibly age group, ethnicity). These extracts will **not** contain any personal information like names or National Student Numbers and the psychometricians will not be able to identify individual students | ākonga from the information provided.

Released under the Official Information Act 1982

- Items can be **"open-ended**", encouraging students | ākonga to express their understanding in their own words. Or they can be **"closed-ended"**, offering predefined options for quick and automated scoring (e.g. multiple choice).
- Students engage with assessments as part of a scheduled **"event"** (i.e. a structured and scheduled occurrence where one or more assessments are delivered to students), which is assigned by teachers.
- As students | ākonga complete assessments, their responses are mapped against "**essential progress markers**", which act as milestones to track how far a student | ākonga has advanced in their understanding or skill development within a specific learning area over time.

6.2.8 Personal information flows in SMART

The following personal information is handled in SMART:

- **Student | Ākonga**:
  - NSN (National Student Number)
  - School Student ID
  - First and last name
  - School | Kura
  - Gender
  - Ethnicity
  - Age; year or level
  - Email address (to support Single Sign On)
  - Student language and accessibility settings (e.g. high contrast, read aloud)
  - School enrolment information
  - Assessment participation details (e.g. answers to questions) and results
  - Information on progression through the curriculum

- **Teachers | Kaiako and School administrators**
  - First and last name
  - Email address (for Single Sign On)
  - School | Kura

Released under the Official Information Act 1982

The following flow diagrams illustrates how the personal information of students | ākonga, teachers | kaiako, school administrators and Ministry staff is collected and used within SMART.

SMART Key information elements

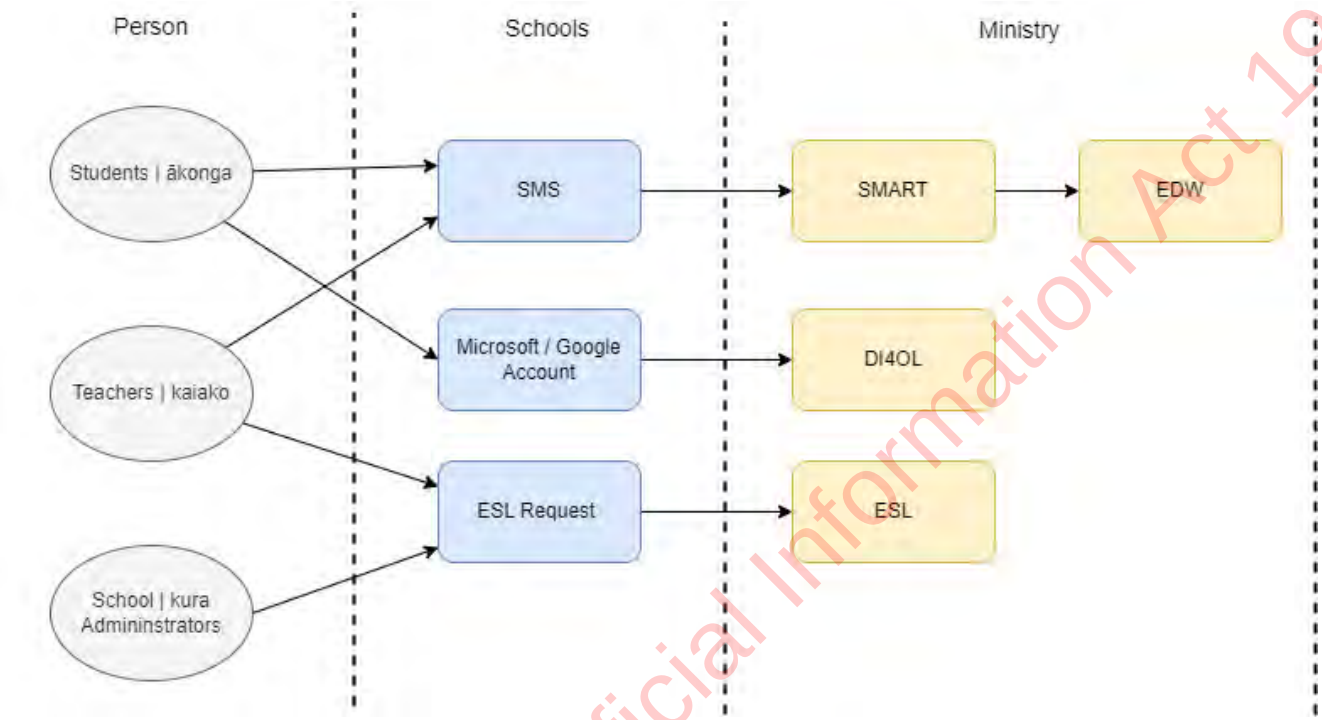


Figure 1 - Key Information elements

Released under the Official Information Act 1982

SMART Detailed information flow

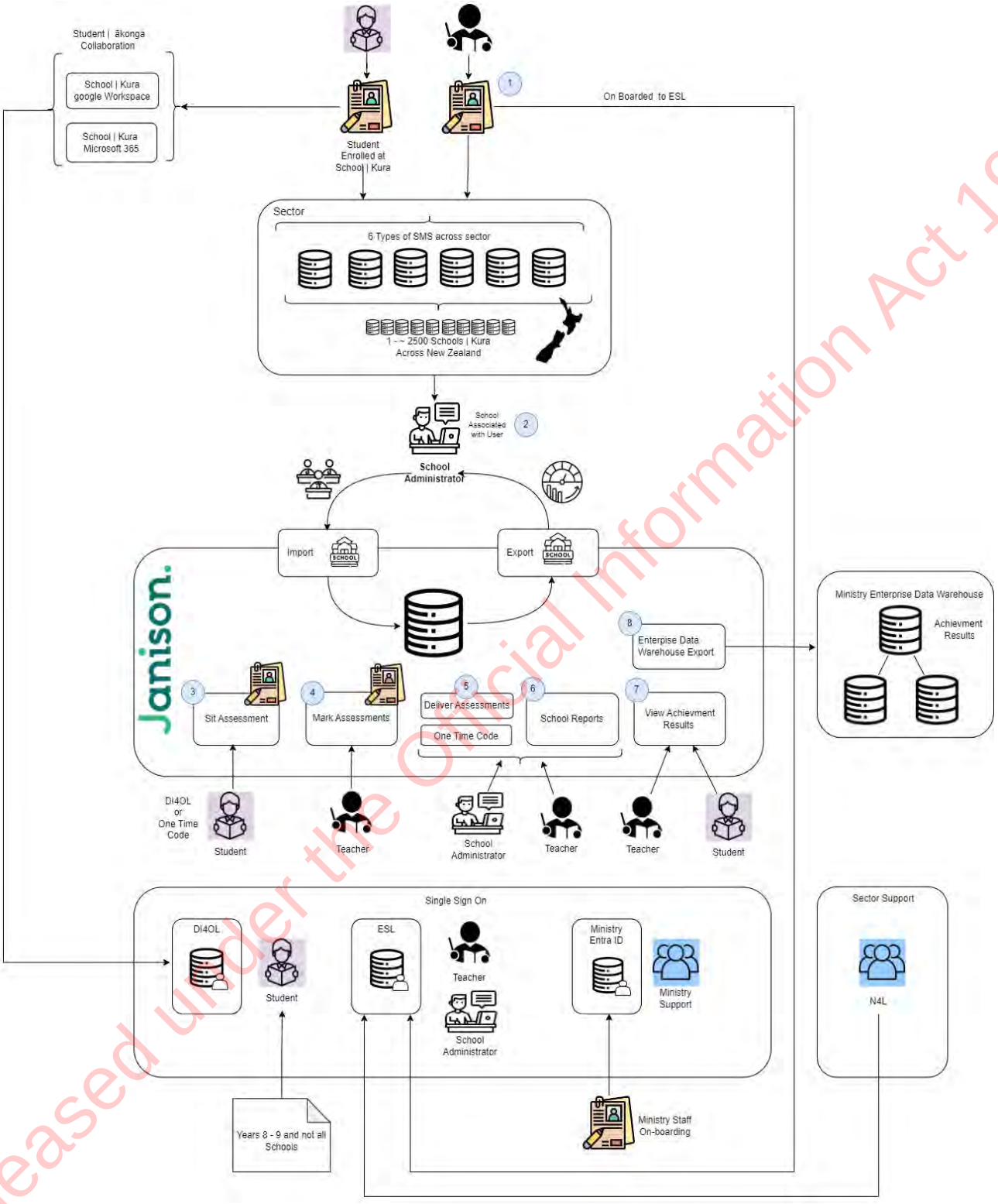


Figure 2 - SMART Detailed Information flow

Released under the Official Information Act 1982

SMART environments and personal information

SMART is hosted on Microsoft Azure in New Zealand with a backup "Disaster Recovery" site in Microsoft Azure Sydney. Janison will provide dedicated environments exclusively for the Ministry for testing, training, production and disaster recovery as set out in the table below.

SMART data will be segregated into different environments to reduce help privacy risks. That includes test, training and practice spaces using synthetic data, with only the live Production system and its disaster recovery backup in Sydney containing real personal information of students | ākonga and teachers | kaiako.

Table 1 - SMART Environments

Location	Environment Name	Tenant Name	Function	Personal Information
Azure New Zealand	E1 (System Integration Testing)	Test	Used by the Ministry to test functionality and integration (e.g. new features and system links) before wider testing in the UAT environment. All tenants on E1 will have the same version of software but will have separate configuration, integration, and data.	**None:** uses synthetic test data about students | ākonga and teachers | kaiako for testing purposes only. Logins are test only and are not linked to real SSO accounts for test users.
Azure New Zealand	E2 (User Acceptance Testing)	UAT	Used by the Ministry for end-to-end testing before release into the production environment. All tenants on E2 will have the same version of software but will have separate configuration, integration and data.	**None:** uses synthetic test data of students | ākonga and teachers | kaiako for testing purposes only. Logins are test only and are not linked to real SSO accounts for test users.
Azure New Zealand	E3 (Production)	Training	Used by the Ministry or its agents to deliver training material to schools | kura.	**Ministry staff personal information:** first name, last name, account name and role of Ministry staff within SMART used.

Released under the Official Information Act 1982

			Schools | Kura will not access this environment directly. All tenants on E3 will have the same version of software but will have separate configuration, integration and data.	Also uses synthetic data of students | ākonga and teachers | kaiako for training purposes only.
Azure New Zealand	E3 (Production)	Production	This is the "live" system used by the Ministry and schools. To provide a production environment for the MOE and schools. All tenants on E3 will have the same version of software but will have separate configuration, integration and data.	**Student personal information** as detailed above in section 6.2.8. **Teachers & school administrator personal information** as detailed above in section 6.2.8. Before new assessments go live, they may be tested in this production environment using synthetic or obfuscated information to make sure the questions work properly.
Azure New Zealand	E3 (Production)	Familiarisation	This is a "sandbox" environment where students can practice using the platform and familiarise themselves with digital assessments. All tenants on E3 will have the same version of software but will have separate configuration, integration and data.	**None:** No personal information
Azure Sydney	(Disaster Recovery)	Disaster Recover	In the event of a failure of SMART in New Zealand, the solution will use the Disaster Recovery environment in Australia until NZ services are restored.	**Student, teacher and school administrator personal information:** will hold the same personal information as held in the New Zealand production environment (but is normally inactive).

Released under the Official Information Act 1982

			Provides a near real-time copy of the New Zealand production environment and the information stored in SMART. The disaster recover environment is NOT used by users unless a disaster has occurred.	

6.3. Legal Authority and Context

Students | Ākonga personal information is collected in SMART for the following **purposes.**

- To enable access to SMART and set individual accessibility preferences, including for assistive technologies that help students complete computer-based assessments.
- To monitor student achievement and assess learning and measure progress against the New Zealand Curriculum and Te Marautanga o Aotearoa.
- To provide feedback to students on achievements and next steps.
- To ensure assessments in SMART are valid, fair and unbiased across diverse student populations via psychometric analysis of item/question performance in assessments.
- To enable system-level reporting by the Ministry, inform curriculum development and education system planning, support schools with teaching and learning resources, monitor and report on student achievement nationally and ensure the education system is equitable and responsive to learners' needs.
- To support the wider Curriculum and Assessment Change Programme (**CACP**), which is aimed at delivering a coherent, whole-of-pathway approach to assessment and reporting.

Teacher | Kaiako personal information is collected for the following **purposes.**

- To enable single-sign on authentication for secure access to SMART.
- To allow teachers to administer and review assessments, assist with marking and use reports to support student learning.
- To supports the Ministry's accountability for quality of teaching resources and enables linking of assessment data to teaching outcomes.

School Administrator personal information is collected for the following **purposes**:

Released under the Official Information Act 1982

- To manage user access and school-wide configuration of SMART.
- To facilitate integration with school SMSs for consistency and reporting.
- **Privacy Act 2020**

  The Ministry must comply with the Privacy Act 2020 (the **Privacy Act**) when collecting, using, storing and disclosing personal information. 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 personal information.

- **Education and Training Act 2020**

  The Education and Training Act 2020 (**Education Act**) sets out New Zealand's education and training system (section 3), including the roles and responsibilities of the Ministry and school boards.

  Relevant sections include the following.

  - Section 5: Following consultation, the Minister of Education may issue a statement of national education and learning priorities for primary and secondary education.
  - Section 90: The Minister of Education may make foundation curriculum policy statements, national curriculum statements and national performance measures.
  - Section 127(2): To meet a board's primary objectives in governing a school, the board must have particular regard to the statement of national education and learning priorities issued under section 5 and give effect to its obligations in relation to any foundation or national curriculum statements and national performance measures, teaching and learning programmes and the monitoring and reporting of students' progress.
  - Sections 125 and 131: A board is the governing body of it school and is responsible for the governance of the school, including setting the policies by which the school is to be controlled and managed. It has complete discretion to perform its functions and exercise its powers as it thinks fit, subject to the Education Act, any other enactment and the general law of New Zealand.
  - Section 165: School boards must ensure their principal and staff monitor and evaluate the performance of students and provide information about student performance to parents. The board must also report to the Secretary (i.e. the Chief Executive of the Ministry), the school community and parents on the performance of the school's students. Monitoring and evaluation must include any foundation curriculum policy statements and national curriculum statements made under section 90 of the Act.

One of the Ministry's key roles is to provide support and resources for teachers[1]. That includes resources for learning and assessment using platforms like SMART.

[1] See www.education.govt.nz/our-work/about-us/our-purpose-and-role/role-ministry-education

Released under the Official Information Act 1982

- **Education (School Boards) Regulations 2020**

  Regulation 21 of the Education (School Boards) Regulations 2020 (**Education Regs**) requires school boards to use good quality assessment or aromatawai information to report on student progress and achievement and provides some specifications for reports.

- **Public Records Act 2005**

  The Public Records Act (**PRA**) governs the creation, maintenance and disposal of "public records" by "public offices", which include government departments like the Ministry of Education and schools. Public records are broadly defined as any information created or received by a public office in the course of conducting its affairs.

The Education (National Student Numbers) Notice 2023 (**NSN Notice**) is a legal instrument issued under the Education and Training Act 2020. It sets out how National Student Numbers may be used in the education system to maintain accurate educational records.

The Ministry and registered schools are authorised by the NSN Notice to use NSNs for various purposes, including ensuring students' educational records are accurately maintained. The collection and use of the NSN by schools and the Ministry in relation to SMART is consistent with this purpose.

The Ministry is also authorised to establish and maintain student identities to support online learning, which includes submission, assessment and moderation. The collection and use of the NSN by schools and the Ministry in relation to SMART is consistent with this purpose. Schools are similarly authorised, though they must only use the NSN for this purpose through a service for establishing and maintaining student identities that has been approved by the Ministry.

The use of other unique identifiers in SMART and the extent to which they comply with IPP 13 is discussed in the section 7 Compliance Assessment.

6.4. Collection

Refer to section 6.2.8 above and Appendix – Data Elements for full details. In summary, SMART will collect and hold the personal information of students (the bulk of the data), teachers, school administrators. The personal information of certain Ministry staff is also collected in SMART but is outside the scope of this PIA.

The following types of sensitive information will be collected and held in SMART.

Information type	Who	Purpose of collection
Children's personal information	Student | ākonga	The personal information of children is sensitive given children's inherent vulnerability and more limited agency than adults. This information is collected to assess and report on student achievement and progress across the New Zealand education system.

Released under the Official Information Act 1982

Gender Ethnicity	Student | ākonga	Collected and used to support the analysis of item performance in SMART assessments. This enables reporting at a demographic level across students | ākonga and schools | kura and helps identify whether questions perform differently for different groups. For example, whether a maths item consistently produces lower scores for one demographic group despite equal overall ability. This information enables the Ministry to monitor and address potential bias, ensuring SMART assessments are valid, fair and unbiased across diverse student populations

Note that student | ākonga accessibility settings in SMART (e.g. "text-to-speech enabled") do **not** store any underlying condition or diagnosis (e.g. dyslexia), which is likely to be considered sensitive personal information.

Accessibility settings are designed to enable fair, accessible assessments tailored to each student's needs, including support for Special Assessment Conditions. They are set by the student | ākonga, then automatically applied in SMART to ensure a consistent experience and can be changed by a student | ākonga and/or teacher | kaiako within SMART at any time.

SMART will process a large volume of personal information of children across New Zealand. The volume of attributes referenced in the table below is based on all 540,000 students | ākonga and 28,000 teachers | kaiako using SMART based on an assumed uptake of 80%.

Table 2 - Volumes of Personal Information

	Volume*
Student | ākonga	**432,000 students | ākonga**; ~5 Attributes / Fields; 2,160,000 Attributes
Teachers | kaiako	**22,400 teachers | kaiako**
School Administrators	**6,160 School Administrators**; ~ 5 Fields; 30,800 Attributes

Direct collection:

Who & What	Method and source of collection	Purpose
Students | ākonga	**Direct collection by MoE**	To help teachers understand and support student learning, to allow schools to meet their reporting duties and to give the

Released under the Official Information Act 1982

Who & What	Method and source of collection	Purpose
Assessment participation and results	The Ministry directly collects students' personal information in the form of assessment results within SMART.	Ministry consistent, system-wide data for monitoring and improving education outcomes across New Zealand.
Students | ākonga Accessibility settings	**Direct collection by MoE** Students | ākonga can select their own accessibility options within SMART (e.g. larger text, higher contrast, text-to-speech) and save those preferences inside the solution. Settings are saved in SMART, not the school's SMS record, and automatically applied each time the student uses it.	Accessibility settings enable fair, accessible assessments tailored to each student's needs, including support for Special Assessment Conditions (**SAC**). Automatically applying them each time the student uses the solution avoids repeated setup and ensures a consistent experience. This approach also minimises the collection of personal (including sensitive) information by storing in SMART only the accessibility feature required (e.g., "text-to-speech enabled") and **not** the underlying condition or diagnosis (e.g. dyslexia), which is likely to be sensitive personal information.

Indirect collection:

Who & What	Method and source of collection	Purpose
SMS: Students | ākonga National Student Number, name, gender, ethnicity, year/ level, class information and assessment records.	**Indirect collection by MoE via SMS** Schools collect this information directly from students via input into their School Management Systems (**SMS**). The Ministry then collects this information into SMART through schools.	Schools collect student personal information in their SMS so they can (1) know who their learners are, (2) track their learning progress, (3) provide the right support and communication and (4) manage enrolment and reporting obligations. Each school's SMS is the source of truth for student and class information for each school. Collecting this information indirectly through schools means the Ministry avoids repeatedly asking families for the same information, ensures data is consistent and

Released under the Official Information Act 1982

Who & What	Method and source of collection	Purpose
		enables the Ministry to meet its system-level responsibilities for monitoring and improving education outcomes.
DI4OL: Students | ākonga DI4OL SSO details - name, email address Please note, in alignment with section 4.3, DI4OL is now referred to as *Learner Identity Broker (formerly DI4OL - Digital Identity for Online Learning)*	**Indirect collection by MoE via school MSFT/Google environment** When students enroll at a school, the school sets up a Microsoft or Google account for the student using their name and email address. The Ministry then collects this information into SMART through schools to set up SSO access via the Ministry's Digital Identity for Online Learning (**DI4OL**) service.	DI4OL is used to authenticate students | ākonga and confirm the right student is signing in. This ensures tests are delivered to the right learner and results are reported correctly. DI4OL is not yet widely in use. It is not available for primary school students and is yet to be fully adopted in secondary schools. However, it remains a service that the Ministry wants to develop over time. In the interim, teachers will be able to use SMART to generate a one-time code for each student to access SMART based on information drawn from their SMS. The code is printed off and given to students who then enter it in SMART to be matched with their school record. This avoids the need to collect identity details directly from students.
ESL: Teacher | Kaiako; school staff and administrators SSO details - name, email address	**Indirect collection by MoE through schools** The Ministry's Educator Sector Logon (**ESL**) service is the main identity and access management service for education sector personnel, facilitating SSO access to Ministry systems, including SMART. Each school has an ESL "Online Delegated Authoriser", typically the principal or a designated teacher or administrator (**ODA**), who grants the appropriate level of access to teachers. The ODA provides teachers | kaiako and school administrators	ESL verifies a person's identity and their role (e.g. teacher, principal, administrator) and enables teachers and school administration staff to log in securely to SMART, preventing access by anyone who is not authenticated. Once authenticated, teachers can assign tests, create/view tests and produce reports. Principals can manage access and data-sharing settings and school administrators can create and maintain student/group details.

Released under the Official Information Act 1982

Who & What	Method and source of collection	Purpose
	with an invitation to sign up to ESL, which each individual then completes with their name and email address details so they can be set up with SSO access to Ministry systems. Schools | kura do not use the personal information collected for ESL for their own purposes. The Ministry collects it indirectly through schools.	
Teacher | Kaiako; school administrators; students | ākonga **Support and helpdesk interactions**	**Indirect collection by MoE through** Teachers have access to helpdesk and support services in relation to the use of SMART, including on behalf of students. Helpdesk services will be provided by Network 4 Learning (**N4L**), a Crown-owned technology company.	N4L will collect teacher, school staff and, where relevant, student, personal information to respond to requests for assistance in relation to SMART. For example, a teacher's name, contact details and school for inclusion in their support tracking system. If a query cannot be resolved by N4L, they will pass the issue to the Ministry support services along with the relevant personal information (e.g. teacher | kaiako details).

How collection is communicated to individuals.

Who	How collection is communicated
Students | ākonga	• **SMS details:** Schools communicate their collection and handling of student personal information via their own privacy notices/statements. • **Assessment results and accessibility settings in SMART:** An equivalent statement to the e-asTTle Privacy Statement[2] will be developed in relation to SMART and made available on the Ministry website. • **DI4OL SSO details / one-time pass:** Nothing currently available.

[2] https://newzealandcurriculum.tahurangi.education.govt.nz/e-asttle-overview-and-access/5637219681.p?activeTab=tab:2

Released under the Official Information Act 1982

Teacher | Kaiako; school administrators	• **SSO details for ESL:** The Ministry has an ESL privacy statement available on its website at https://applications.education.govt.nz/education-sector-logon-esl/esl-application-privacy • **Support and helpdesk interactions:** N4L has a privacy statement that refers to its interactions with the Ministry at https://www.n4l.co.nz/privacy-statement/

Released under the Official Information Act 1982

6.5 Storage and Security

Storage

All personal information in SMART is stored in Microsoft Azure data centres in New Zealand. Janison manages the platform remotely from Australia.

- Structured student information from school SMSs (e.g. name, class, demographic information) is stored in a secure Microsoft Azure SQL (Structured Language Query) database, which provides a secure, structured way of storing and managing personal information. Only users with permission can see or change data.
- Unstructured data such as images (e.g. scanned assessments) and images relating to assessment questions / items are stored within Azure Blob storage. “Blob” (Binary Large Object) storage is a way of storing unstructured data at scale that ensures large unstructured files are stored securely and retrievable when needed.

Data centre security

SMART features multiple layers of security to protect this information.

- The SMART assessment platform is hosted by Janison in a dedicated environment within Microsoft Azure New Zealand, provisioned exclusively for the Ministry of Education. This means no other Janison customers share this environment, ensuring data isolation and security.
- Azure Network Security Groups (**NSGs**) act like firewalls, with a “deny everything unless explicitly allowed” rule. This means only the services that really need access can see the data.
- All information is encrypted both when stored and when sent across the network, using ciphers (formulae that scramble information to keep it private) approved by the New Zealand Information Security Manual (**NZISM**).

Infrastructure Access

If Janison requires additional lower-level access as providers of the solution, this is handled as follows.

- Janison staff log in through Janison’s Microsoft Entra ID to reach the SMART Azure environment.
- All user access at the infrastructure level requires Multi-Factor Authentication (**MFA**).
- Granular role-based access controls (**RBAC**) is placed on Azure Resources using least privilege permissions.
- Privileged Access Management (**PAM**) is used for roles that have access to personal information requiring “just-in-time” access, explicit approvals and time-limited access.

Access controls

Released under the Official Information Act 1982

Janison controls access to SMART functions and information via RBAC integrated with the Ministry identity providers for Single Sign On (i.e. DI4OL, ESL and Microsoft Entra ID). This means SMART users log in once and their access is based on their role.

The full detail of roles with access to **personal information** in SMART is set out in the table below.

Role	Personal information	Access reasons
Student | ākonga	Their own personal information	• Set accessibility settings • Sit assessments, review achievements and understand their progression pathway.
Teacher | Kaiako (Includes principals where relevant)	Personal information of all students in their **school | kura**	Within SMART, teachers | kaiako can: • Assign assessments to students | ākonga • Score student | ākonga assessments and add them to their records • Review assessment results, plan next steps (including progression pathways) and report to families | whānau and the school | kura board. It would not be practical to implement access controls limiting teacher access to only their classes because this would require the collection of personal information about teacher and class relationships, which is not currently collected. This would also present issues for relief teachers working across multiple schools and those in shared Modern Learning Environments.
Administrators - schools | kura (Includes principals where relevant)	Personal information of all students in their **school | kura**	School administrators need access to all student personal information to create and maintain student and group details in SMART. They use this to: • Import student | ākonga progression results from SMART to their school SMS • Manage student information between the school's SMS and SMART and help assign students to sessions (where required).
N4L help desk staff	Personal information of teachers | kaiako and students | ākonga where delegated	Help desk staff may have limited access to student information to support troubleshooting but only where a teacher | kaiako delegates such access so help desk staff can provide appropriate support and assistance. For the avoidance of doubt, help desk staff will never have access rights to set assessments or the ability to see all student information.

Released under the Official Information Act 1982

Role	Personal information	Access reasons
Ministry staff: Operational and system support staff	All personal information in SMART	SMART system administrators and support staff (approx. 20 people) have access to all data in SMART to maintain SMART, resolve issues (e.g. troubleshooting) and ensure integration with school SMS and EDW.
Ministry staff: Data Warehouse and Data and Insights team	All data in the EDW, including personal information drawn from SMART	A small group of Ministry data analysts have access to the personal information from SMART in the EDW, which they use to: • provide aggregated and system-level summarised reporting (e.g. by school, region, ethnicity or nationally) to inform policy and monitoring of education outcomes and generate insights for Ministers, Treasury, and the public on student progress • conduct research (e.g. studying patterns of learning and assessment outcomes) • integrate SMART assessment results into the EDW for longitudinal analysis and reporting It is not expected that this reporting will expose personal information to recipients. The Brief Privacy Assessment notes that personal information in EDW can be obfuscated if required. See the further discussion about EDW access controls for this group below.
Ministry staff: Statisticians, reporting specialists Curriculum & Assessment (Te Poutāhū), policy and leadership staff	Aggregated personal information (e.g. in the form of dashboard reporting)	Ministry staff outside the data analytics team have limited role-based access to aggregated personal information prepared by the data analytics team.

Released under the Official Information Act 1982

Ministry access controls

The following Ministry procedures and rules are in place for granting, reviewing and revoking access to SMART when staff leave or change roles.

- **New staff:** When a new staff member joins the Ministry, they are entered into the Human Resources Information System (HRIS). Once approved, a Microsoft Entra ID is automatically created, which enables the staff member with the relevant privileges to log in to the Ministry environment, but not specific systems or applications. Access to SMART will require a manual process and/or Standard Operating Procedure (**SOP**) to be established to set up RBAC to SMART specifically. A manual process and SOP for this purpose is yet to be developed, but we understand will be in place before SMART goes live.

- **Departing staff:** When a staff member leaves the Ministry, their profile is updated in HRIS, which automatically updates their Entra ID by disabling the staff member's account and access to Ministry resources.

- **Role changes:** A formal business process governing changes to SMART access permissions is yet to be developed. This is not an automated process and will require an SOP to be created for the IT help desk to action that will provide appropriate access permissions based on an individual's role.

Access monitoring and logging

- Janison continuously monitors SMART for suspicious activity. It aims to detect and respond to any unauthorised or suspicious attempts to access Ministry data, including personal information. All access attempts are recorded, including successful and failed login attempts, as well as any modifications to or deletions of Ministry data.

- The SMART platform will generate and retain detailed audit logs recording who accesses personal information, when, their role and the function they were performing. This will enable the Ministry to detect and investigate any unauthorised or inappropriate access or use of personal information, provides an accountability trail for all users (including Ministry staff, schools | kura, Janison and psychometricians) and will support periodic reviews and audits to confirm data is only used for authorised educational purposes.

Education Data Warehouse access

The Ministry's EDW will receive and store personal information from the SMART. The EDW acts as a central data repository for the Ministry, integrating data across Ministry systems that is used for purposes such as reporting student progression at scale.

The EDW is classified as suitable to hold SENSITIVE information under the Government Security Classification System and the Ministry's adoption of it through the NZISM. A SENSITIVE rating has stronger security and privacy requirements than the IN-CONFIDENCE rating applied to SMART, including restricted access using RBAC, identity management (Entra ID), restricted views and de-identification for wider reporting. The EDW is designated to handle a higher tier of sensitivity because it aggregates and links large datasets from across the education system, raising both privacy risk and systemic impact if breached.

Released under the Official Information Act 1982

The EDW has its own Privacy Impact Assessment describing how the EDW handles personal information. When new information is added to the EDW – as it will be when SMART is fully deployed – we understand the PIA for the EDW will be revised.

As noted above, access to personal information in the EDW is controlled via RBAC, with personal information held in separate views linked to user roles. Permissions are managed via the Ministry Entra ID system. Data analysts with access to personal information create additional views that provide aggregated or de-identified information for wider reporting.

Certification and Accreditation, including a full security assessment, is currently underway.

The agreement with Janison is currently in negotiation at the time of conducting this PIA. We understand it will include appropriate clauses clearly defining the roles and responsibilities of the parties, including obligations for Janison not to use or disclose any personal information for its own purposes.

It is expected that a similar approach will be adopted with other relevant third parties, including external item developers (e.g. for Te Reo Māori items) and external psychometricians used to measure the quality and fairness of items and assessments (noting they do not require or receive access to any personal information).

6.5.1. Information Classification

The Ministry has evaluated SMART and the information in it based on the *New Zealand Government Information Security Management Requirements – New Zealand Government Security Classification System* and recommended a security classification of "IN-CONFIDENCE". That classification was endorsed by the Ministry's Deputy CISO after consultation with the Information team.

That security classification was selected because the system holds or processes information about learners and/or education provider staff, unauthorised disclosure of which would adversely affect their privacy

6.6. Access and Correction

Access to, and correction of, personal information will be available as follows.

- **SMS-held data:** Most of the personal information in SMART is collected and stored by schools in their respective SMSs. Students and teachers can therefore follow existing school IPP 6 and IPP 7 processes to access and correct their information.
- **SMART results:** Student personal information in the form of assessment results, accessibility settings and progression information is collected and held in SMART.
    - If assessment details are incorrect (e.g. entered incorrectly by a teacher), these can be corrected directly by a teacher | kaiako.
    - Teachers | kaiako can correct student | ākonga progression details within SMART, which synchronises with and updates the relevant SMS where any changes are made in SMART.
    - Student | ākonga accessibility settings can be changed directly by a student | ākonga or teacher | kaiako in SMART.

Released under the Official Information Act 1982

- **SSO tools:** Students | ākonga, teachers | kaiako and administrators will follow the existing IPP 6 and IPP 7 processes of DI4OL, ESL and N4L to access and correct their information.

6.7. Accuracy and Data Quality

Describe any known issues with data quality and how they are addressed before personal information is used or disclosed.

We were not made aware of any known issues with data quality at this stage, noting that schools are responsible for checking the quality of SMS data before they use it for monitoring or reporting on student performance, including for uploading to SMART.

Given the Ministry is also collecting this information indirectly through schools, it too has IPP 8 obligations to ensure personal information used in SMART is accurate, up to date, complete, relevant and not misleading. This is discussed in the Compliance Assessment section.

6.8. Retention and Disposal

All state and state-integrated schools | kura are required to comply with the Public Records Act 2005, which provides a framework for the creation and maintenance of public records. A "public record" is a record created or received by a public office in the conduct of its affairs (s 4 PRA). All records created or received by schools in the course of business are "public records" under the PRA, including enrolment forms, individual student records and assessment records.

The PRA prevails over the provisions of the Privacy Act.

The *School Records – Retention and Disposal Schedule* (the **School Retention Schedule**) published by the Ministry and the Archives New Zealand[3] was developed to help schools comply with the requirements of the PRA. It requires all state and state-integrated schools to create and maintain processes to develop and manage their school records. It sets out what schools | kura need to do to uphold the PRA, including information about how long to keep school records. School boards are responsible for maintaining and monitoring school records and cannot legally destroy any school records without the authority of Archives New Zealand, as reflected in the School Retention Schedule.

The Ministry's Records Services team has advised that the School Retention Schedule applies to the information in SMART, as it did to e-asTTle.

In the context of SMART, student achievement records are public records about a student that are covered by the Schools Retention Schedule. These records are held and maintained by the school as an official record of each student's | ākonga educational achievement. The Ministry contributes to those records by recording assessment results in SMART and sending those results back to schools.

Class 1.7 and 1.8 of the School Retention Schedule are the likely applicable classes to the records in SMART.

- Class 1.7 covers "Records relating to individual students kept by the school and not transferred on to the student's next school (except for those relating to students in class 1.9, and students' own work – not public records). Listed examples include school reports, test results, Unit Standard passes, internal assessment grades, external exam results, progress and achievement data and care plans for vulnerable students".

[3] https://web-assets.education.govt.nz/s3fs-public/2024-08/School-Records-Retention-and-Disposal-Schedule-All.pdf?VersionId=jIDsjW8vQJbskiFsKnW05s.ldZv8H_is

Released under the Official Information Act 1982

- These records need to be kept "until all operational / administrative actions and reporting actions have been completed by the school. Then they can be destroyed with permission from the board".

- Class 1.8 covers "Records relating to individual students transferred to the student's next school (except for those relating to students in class 1.9, and students' own work – not public records). Any versions or copies retained fall into class 1.7)". Examples provided include academic progress records, pastoral records and Resource Teacher Learning and Behaviour (RTLB) records.
    - These records need to be kept "until all operational / administrative and reporting actions have been completed by the last attended school. Following this the period the records may be destroyed with permission from the board".

The "Data Retention and Disposal for the Education Data Warehouse (EDW)" schedule (**EDW Schedule**) applies to Personal information from SMART that goes into the EDW. The Ministry's Records Services team has advised that this information is considered to be "longitudinal data held in EDW (extracted from operational source systems)" that must be retained "indefinitely".

Temporary Care Records Protection Instruction: The Chief Archivist has issued a temporary care records protection instruction[4] (**Temporary Care Instruction**). It requires all care records in a school's system to be retained indefinitely and not disposed of, altered or destroyed. It is in place to protect public office care records while work is undertaken to review the retention and disposal of State care records in relation to the Royal Commission of Inquiry into Historical Abuse in State Care and in the Care of Faith-based Institutions.

"Care records" include records about students and staff that document the provision of care services to individuals (a child or vulnerable adult in or who has been in State or non-State care) by State care and non-State care organisations in certain care settings.

The Records Services team has advised that the Temporary Care Instruction will supersede the requirements of the Retention Schedule because the records in SMART will include children's "care records". That is because if a child in State care sits an assessment in SMART, this will constitute part of the student's | ākonga care record.

The Temporary Care Instruction provides that child care records must be held **indefinitely** until Archives NZ can give specific instructions.

Janison has advised that they will provide the Ministry with the capability to remove information from SMART in support of the Ministry's obligations under IPP 9 of the Privacy Act to only retain personal information for as long as it is required for the purpose for which it may lawfully be used.

The Ministry is responsible for defining the criteria and process for such removal / deletion, including authorisation for the removal of information as part of the SMART implementation. Janison has advised they will implement the removal of personal information using a combination of built-in platform functions and processes run at the Ministry's request based on the Ministry's requirements.

[4] https://www.education.govt.nz/education-professionals/schools-year-0-13/administration-and-management/managing-school-records

Released under the Official Information Act 1982

The Ministry is in the process of configuring SMART, which means retention and deletion requirements and settings are not yet operational.

6.9. Use

The Ministry will collect and use personal information in SMART as set out in section 6.4 above.

- For Ministry use, see the table in section 6.5 above setting out access controls for different Ministry teams and their reasons for access.
- Schools | kura will use the personal information in SMART as described in this report. School SMSs are the source of most of the personal information that goes into SMART, which they collect for their own purposes and therefore may use and disclose accordingly.
- As a data processor, Janison is not expected to use or disclose SMART personal information for its own purposes.

Note that:

- The Ministry will **not** use any personal or other information in SMART to develop league tables at the school | kura and/or teacher | kaiako level that rank schools according to academic results.
- Psychometricians, who determine the quality of "items" used in assessments, will **not** have access to student | ākonga personal information, such as NSNs or names.

The key third party involved in SMART is Janison, the provider of the SMART platform. Janison is expected to be a service provider / data processor / agent under section 11 of the Privacy Act only, with no right to use or disclose personal information in SMART for its own purposes. Appropriate provisions in support of this role are expected to be included in the agreement between the Ministry and Janison, which is currently being drafted at the time of this PIA.

Psychometrician services are provided by external service providers. We understand the relevant contracts clearly specify that psychometricians may not use or disclose personal information that they access on behalf of the Ministry for their own purposes. We note, however, that we have not sighted those agreements.

Schools:

- As part of the Ministry's Professional Learning and Development (PLD) programme, teachers | kaiako will receive targeted training on privacy responsibilities associated with the use of SMART.
- A privacy statement equivalent to the e-asTTle statement will be developed and published for SMART.

Janison: Janison provide mandatory training to staff, including in respect of data breaches and understanding privacy. This training is provided in their LMS and staff completion is tracked.

The Ministry will ensure personal information in SMART is only used for the purposes for which it was collected in the following ways.

- **Contractual obligations**: on Janison and psychometricians not to use or disclose the personal information in SMART for their own purposes.

Released under the Official Information Act 1982

- **Privacy training:** All Ministry staff are given mandatory privacy training as part of the staff onboarding process. This is required via the Ministry's Learning Management System (LMS) and is supported by compliance reporting to People Managers.

- **Audit logs and monitoring:** The SMART platform will generate and retain detailed audit logs recording who accesses personal information, when and what their role is. This will enable the Ministry to detect and investigate any unauthorised or inappropriate access or use of personal information, provide an accountability trail for all users, including Ministry staff, schools | kura, Janison and psychometricians and support periodic reviews and audits to confirm data is only used for authorised educational purposes.

- **Agreed procedures**: Ministry staff use of SMART will be subject to the formal governance and operational processes that the Ministry requires for all systems handling "IN-CONFIDENCE" personal information. That includes access control management (e.g. RBAC aligned with the "need to know" principle under the In-Confidence classification), use of secure SSO mechanisms to access SMART and procedures for granting, reviewing and revoking access when staff leave the Ministry or change roles.

- **Regular review of access controls:** The Ministry's product management team within Te Pou Hanganga, Matihiko – Digital (PM team) will meet regularly with Janison to discuss SMART service levels, issues and performance. As part of those reviews, the DPM team will produce reports on user access to SMART data. Where there are reports of unusual access to SMART, the PM team will work with the business to validate, access or remove access as necessary.

- **SOPs for access**: Other Ministry requests for access to SMART data will be managed by a SOP / process that is yet to be developed.

6.10. External Sharing

The Ministry will not disclose any personal information from SMART with external agencies or individuals except as set out below.

- Janison will have access to personal information in SMART but only as a processor (i.e. the Ministry's "agent" under section 11 of the Privacy Act). This is not a "disclosure" under the Privacy Act.
- Personal information is never shared with or accessed by external psychometricians.

The personal information in SMART will be stored in the Microsoft Azure New Zealand environment, with back-up to Azure Sydney for disaster recovery.

6.11 Unique Identifiers

Three different types of unique identifiers are used in the context of SMART.

1. NSNs

National Student Numbers are assigned centrally by the Ministry of Education as the unique identifier for all school students in New Zealand. SMART does not assign new NSNs but it will collect and use existing NSNs imported from each school's | kura SMS or from Ministry data sources.

Released under the Official Information Act 1982

The NSN will be used as the key identifier to link a student's assessment data within SMART and across related Ministry systems like the EDW. Functions supported by the NSN include:

- associating students with their assessments, results and progression through the curriculum;
- ensuring accuracy in reporting for teachers, schools and the Ministry; and
- linking results back into SMS and into the wider Ministry data ecosystem.

NSNs in SMART will be protected via access controls & SSO access for teachers | kaiako via ESL and, eventually, for students | ākonga via DI40L. This means that only authenticated users with an educational role and purpose can see or use NSNs, reducing the risk of unauthorised access or unauthorised use of identifiers.

Security measures include encryption, secure hosting in New Zealand, regular penetration testing and reporting, incident response aligned with ISO 27001 and monitoring of system access and audit logging.

2. Student IDs

Student IDs are identifiers generated and maintained within each school's SMS. They are different from the NSN, which is generated by the Ministry. Student IDs are personal information under the Privacy Act 2020 because they can identify a student when combined with school data.

Schools provide files to SMART that include student groupings (e.g. classes, reading groups, intervention groups). Each group record includes the school's Student IDs, which SMART uses to construct and manage these groups. When assessments have been completed, SMART then matches the results back to the Student IDs, ensuring they are correctly mapped to the school's local student records in the SMS. Accordingly, the Ministry only uses Students ID in SMART to recognise which student belongs to which school-defined group and send results back to the correct school record.

Student IDs have no meaning outside the school context and the Ministry does not use them for other purposes, like national reporting, long-term storage, or analysis They function solely as a temporary "handle" for exchanging data between SMART and school systems.

3. SMART IDs

A third type of identifier is generated inside SMART to separate student | ākonga results from one another so psychometricians can analyse test results and conduct item calibration without needing to see students' official identifiers. This helps ensure test questions are fair and reliable.

The SMART ID is a unique number distinguishing a student within the dataset and is not usable outside of SMART. That is, it has no meaning if exported or matched against external systems.

SMART IDs are linked with:

- Student | ākonga demographic information already in SMART (e.g. year level, gender, ethnicity, language/learning needs),
- student | ākonga answers,
- event-level data (timestamps, item attempts)
- item metadata (subject domain, skill, language).

This allows psychometricians to analyse how students interact with test items, calibrate item difficulty, and maintain the validity and reliability of assessments.

Released under the Official Information Act 1982

Importantly, psychometricians do not need access to NSNs or school-assigned Student IDs to do this work.

Released under the Official Information Act 1982

7. Compliance Assessment

This assessment of SMART against the 13 Information Privacy Principles (**IPPs**) in the Privacy Act 2020 has been completed by Simply Privacy Ltd.

Released under the Official Information Act 1982

IPP	Assessment	Compliance Rating	Risk ID
IPP 1	**IPP 1 requires agencies to collect personal information only for lawful purposes connected with their functions or activities, where the information is necessary for that purpose. This principle is about data minimisation.** **Lawful purposes:** • SMART's core purposes are to provide a technology platform to deliver twice yearly assessments for all New Zealand school children in Years 3 - 8 (optionally Years 9 - 10) to inform teaching and learning, provide timely information to parents/whānau and support decisions across the education system. These are legitimate education purposes and the personal information of students, teachers and administrators is reasonably required for those purposes and in connection with the Ministry's core functions and activities. • Aggregated personal information will be used by the Ministry for system-level monitoring, reporting and decision-making on education policy, curriculum development and resource allocation. This is a legitimate and justifiable purpose in the context of the Ministry. • The collection of teacher and school administration staff personal information to operate SMART is also in line with those lawful purposes. **Data minimisation:** The Ministry's approach supports data minimisation by re-using SMS data as the primary source of most student personal information for the solution. This information is already collected by schools for their own purposes (e.g. enrolment, teaching and administration) and schools remain responsible for the handling of such information. Ministry use of SMS data avoids having to repeatedly asking families for the same information, helps ensure the data is consistent and limits the new collection of student personal information to what SMART strictly needs to operate, namely student assessment results and accessibility settings. It also enables the Ministry to meet its system-level responsibilities for monitoring and improving education outcomes.	**Compliant**	N/A

Released under the Official Information Act 1982

IPP 2	**IPP 2 requires agencies to collect personal information directly from the individual concerned unless an exception applies.** ***DIRECT collection:*** • **Assessment details:** The Ministry directly collects students' | ākonga personal information within SMART when students participate in assessments, scores are developed and assessment results are generated. • **Accessibility settings:** The Ministry also directly collects the personal information of students' | ākonga when they select their own accessibility options within SMART (e.g. larger text, higher contrast, text-to-speech) and save those preferences inside the solution. Automatically applying those settings each time the student uses SMART avoids repeated setup and ensures a consistent experience. It also minimises the collection of personal (including sensitive) information by storing only the accessibility feature required (e.g., "text-to-speech enabled"), not the underlying condition or diagnosis. ***INDIRECT collection:*** Most of the personal information in SMART is collected indirectly by the Ministry through schools. This will comply with IPP 2 to the extent a relevant exception applies. • **Student | ākonga SMS information:** The Ministry will collect student | ākonga personal information indirectly from schools, which collect, manage and store that data in their SMSs as part of their enrolment and teaching processes. Each school's SMS is the source of truth for student and class information for each school. The Ministry does not create new records but instead relies on schools' existing enrolment and teaching data that it imports into SMART as required. This helps ensure SMART always has the most current student and class information available for assessments. Once imported, this information is used in SMART to associate students with their classes and deliver assessments to the right group. o **Relevant exception: Non-compliance would not prejudice interests:** IPP 2(a) allows indirect collection where this would not prejudice the interests of the individuals	**Compliant**	N/A

Released Under the Official Information Act 1982

concerned. Importing personal information from school SMSs appears to support rather than undermine student and teacher interests. By relying on SMS updates rather than asking individuals to provide their personal information repeatedly, SMART can ensure that assessment data is always matched to the right student and class, minimising risks of misattribution and inconsistency or errors in duplicated data..

- **Relevant exception: Compliance is not reasonably practicable in the circumstances:** IPP 2(f) may also apply on the grounds that getting personal information directly from each student and teacher instead of through schools would be impractical for the Ministry because it would be administratively unworkable and resource-intensive given the volume of personal information involved. Each SMS is already the authoritative record of this information and importing from it to SMART avoids inefficiency, error and unnecessary duplication.

- **Student | ākonga SSO information:** The Ministry will collect student | ākonga personal information for SSO purposes indirectly through schools. When students enrol at a school, the school sets up a Microsoft or Google account for the student | ākonga using their name and email address. DI4OL (which is operated by the Ministry) accesses that information in the school's Microsoft/Google environment and uses it to set up SSO access, which authenticates students | ākonga and ensures results are delivered and reported correctly.

  DI4OL is not yet available for primary school students and is yet to be fully adopted in secondary schools. In the interim, teachers will be able to use SMART to generate a one-time code for each student to access SMART based on information drawn from their SMS. The code is printed off and given to students who then enter it in SMART to be matched with their school record. This avoids the need to collect identity details directly from students.

  - **Relevant exception: Non-compliance would prejudice the interests of students (IPP 2(a)):** The Ministry's indirect collection of personal information in the context of DI40L and one-time passes is unlikely to prejudice the interests of students | ākonga because the information is drawn from details already provided to schools, meaning new information does not need to be collected. Using school-provisioned accounts

Released under the Official Information Act 1982

	avoids duplication and errors that could arise if students had to supply these details again. The data is used only for authentication purposes to ensure assessments and results are matched to the correct learner, which is ultimately beneficial for students | ākonga and ensures others cannot access their SMART profiles. o **Relevant exception: Compliance is not reasonably practicable in the circumstances (IPP 2(f)):** Directly collecting SSO identifiers from each student | ākonga would require duplicating school account processes and constant re-verification. It is not reasonably practicable and using school-created accounts or teacher-issued codes provides accurate, efficient authentication without added burden on students | ākonga. • **Teacher SSO information (ESL):** The Ministry collects the personal information of teachers and school administrators indirectly via schools so it can set them up with SSO access to Ministry systems, including SMART, using its Educator Sector Logon (**ESL**) service. o **Relevant exception: Non-compliance would not prejudice interests (IPP 2(a)):** Collecting teacher | kaiako and school | kura administrator information indirectly through schools to provision access to ESL does not prejudice staff interests because the information is only used for identity verification and secure, role-based access to SMART, and not for school purposes. Indirect collection ensures authentication is accurate and consistent, avoiding duplication and additional burden on staff. • **Helpdesk information (N4L):** The Ministry may collect the personal information of teachers and school administrators indirectly via the N4L help desk service. On occasion, student |ākonga personal information may also be collected. This information is used to respond to requests for assistance in relation to SMART. o **Relevant exception: Non-compliance would not prejudice interests (IPP 2(a)):** The Ministry's receipt of teacher and administrator details from N4L's helpdesk does not prejudice their interests, as the information is only used to resolve the individual's support request and is consistent with what they would expect when seeking help. Indirect collection through N4L also avoids teachers needing to provide the same details separately to the Ministry, supporting data minimisation principles.		

Released under the Official Information Act 1982

IPP	Assessment	Compliance Rating	Risk ID
	Similar arguments apply in relation to student | ākonga personal information. Help desk staff will only have limited access to this information where delegated by a teacher | kaiako so help desk staff can provide appropriate support and assistance. Help desk staff will never have access rights to set assessments or the ability to see all student information.		
IPP 3	**IPP 3 requires agencies to be open about why they are collecting personal information and what they will do with it. This means the Ministry must take reasonable steps when directly collecting personal information to make sure relevant individuals know why their information is being collected, who will receive it, whether giving the information is compulsory or voluntary and what will happen if the information isn't provided. Certain exceptions may apply if there are good reasons for not letting a person know about the collection.** IPP 3 applies to the direct collection of personal information by the Ministry. Indirect collection is addressed below in relation to IPP 3A. At this early stage, the Ministry is not sufficiently prepared to be appropriately transparent with students | ākonga about the way their personal information is collected, stored, accessed or used in SMART in respect of assessment results and accessibility settings. A Privacy Statement about the collection and use of student personal information in relation to assessment results and accessibility settings in SMART is yet to be developed. It is expected that a notice similar to the e-asTTle Privacy Statement[5] will be made available on the Ministry website.	**Non-Compliant**	R01

[5] See https://newzealandcurriculum.tahurangi.education.govt.nz/e-asttle-overview-and-access/5637219681.p?activeTab=tab:2

Released under the Official Information Act 1982

IPP 3A[6]	**IPP 3A (which comes into force on 1 May 2026) will apply to the indirect collection of personal from an individual. It will require any agency collecting personal information from a source other than from the individual concerned to take reasonable steps to ensure that the individual is aware of the information required under IPP 3, unless an exception applies.** The Ministry collects most of the personal information in SMART indirectly through schools as set out below. Those indirect collections are permitted to the extent the identified exceptions apply. On that basis, these collections are likely to comply with IPP 3A. However, we note the risk of a residual perception of a lack of transparency by the Ministry, hence Risk R02. 1. **SMS data imported into SMART:** The Ministry indirectly collects student | ākonga personal information through school | kura SMSs. Unless an exception applies, IPP 3A will require the Ministry to ensure students | ākonga (and ideally their parents/whānau) are aware that personal information supplied to schools will also be imported into SMART for assessment-related purposes. The exception in IPP 3A(3) provides that such notice is not required if the individuals concerned have previously been made aware of the agency's indirect collection of the information. That will not be the case here as this is a new indirect collection by the Ministry. In addition, it will require that schools' enrolment privacy notices explicitly state that student information will be disclosed to the Ministry for assessment, which is unlikely to be the case. However, the Ministry can argue it is not reasonably practicable for the Ministry to notify each student | ākonga directly that their enrolment details will be imported from the school SMS into SMART (IPP 3A(4)(e)). This is because schools are legally separate entities and manage their own enrolment processes, meaning the Ministry does not have direct contact with students and families at the point of collection. While the Ministry could issue general privacy statements and even template privacy notices to schools (and we recommend that it does), it cannot *require* schools to incorporate this messaging into their enrolment notices. Given the scale of students across New Zealand schools, and the reliance on schools as the "source of truth" for enrolment data, the Ministry may reasonably argue that direct compliance with IPP 3A is not practical. 2. **DI4OL - Student | ākonga information collected by schools:** The Ministry accesses student | ākonga name and email address information from school-provisioned Microsoft/Google accounts	**Compliant**	R02

Released under the Official Information Act 1982

Released under the Official Information Act 1982

[6] Upcoming new requirement relating to indirect collection of personal information. Amendment not yet passed or in force. See: Privacy Amendment Bill 292-1 (2023), Government Bill Explanatory note – New Zealand Legislation

to facilitate SSO access for those individuals using DI4OL. Unless an exception applies, IPP3A will require the Ministry to tell students | ākonga (and their families | whānau) that school-created accounts and one-time passcodes will also be used for authentication into SMART.

Much like in relation to SMS data, the exception in IPP 3A(3) that notice is not required if the individuals concerned have previously been made aware of the agency's indirect collection of the information is unlikely to apply here. There does not appear to be a privacy notice available for DI4OL. In addition, we understand a separate PIA for this service is in the process of being updated and finalised, which identified a medium-rated risk relating to transparency with students | ākonga and their parents/guardians | whānau about the purpose of collection and disclosure to the Ministry.

The Ministry can, however, argue it is not reasonably practicable to notify every student | ākonga directly that their Microsoft/Google account details (name and email address) will be accessed by DI4OL for single sign-on (IPP 3A(4)(e)). Those accounts are created and managed by schools as part of student enrolment and school ICT provisioning, processes over which the Ministry has no direct control. The Ministry cannot require schools to consistently communicate the Ministry's role in authentication at the point accounts are established. Given the scale of account creation across schools and the fact that DI4OL is only gradually being rolled out, the Ministry can reasonably argue that direct compliance is not practical. Instead, alternative steps such as including privacy information in Ministry-level notices, providing template wording for schools and giving clear information when students first use DI4OL should be used to meet the intent of IPP 3A.

3. **SMART one-time passes - Student | ākonga information collected by schools:**

For schools | kura not yet using DI4OL (i.e. the majority of them), teachers | kaiako can generate one-time pass codes in SMART for students sitting an assessment in SMART. Those codes are based on information from the relevant SMS and involve the transfer of some limited personal information into SMART from the SMS to enable authentication.

The exception in IPP 3A(3) (which applies where individuals have already been made aware of the indirect collection) is unlikely to apply because there is no evidence that schools communicate how, why and when they collect student personal information in this context.

Released under the Official Information Act 1982

IPP	Assessment	Compliance Rating	Risk ID
	The Ministry can argue that it is not reasonably practicable for the Ministry to notify each student directly (IPP 3A(4)e)) because passcodes are generated locally by teachers as part of a decentralised process across thousands of classrooms. This makes it difficult for the Ministry to require the inclusion of an appropriate privacy notice. 4. **ESL - Teacher | kaiako & administrator details:** Schools collect teacher | kaiako and administrator name and email address information via forms that the Ministry accesses to provision ESL and SMART access. The Ministry can argue that the exception in IPP 3A(3) applies because individuals were previously made aware of the collection of their personal information for SSO purposes by the ESL privacy statement, available at https://applications.education.govt.nz/education-sector-logon-esl/esl-application-privacy. 5. **N4L - teacher | kaiako & administrator details:** N4L collects the personal information of teachers, administrators and (where relevant) students through its helpdesk to respond to SMART support requests. Where a query cannot be resolved by N4L, it is passed to the Ministry along with the relevant details and, if required, on to Janison. Unless an exception applies, IPP 3A will require the Ministry to ensure individuals are clearly informed that their helpdesk information may be disclosed to the Ministry (and Janison) to enable resolution of SMART-related issues. The exception in IPP 3A(3) is likely to apply on the grounds that the relevant individuals were previously made aware of the collection of their personal information. N4L has a privacy statement[7] available on its website that explains that when individuals contact its Helpdesk, N4L will collect their personal information and may disclose it to the Ministry where necessary to resolve queries relating to Ministry services (such as SMART). This indicates that teachers and administrators contacting the Helpdesk have already been made aware that their details may be passed to the Ministry for this purpose, which would mean the Ministry would not need to notify again under IPP 3A. The N4L privacy statement is available at https://www.n4l.co.nz/privacy-statement/.		

[7] https://www.n4l.co.nz/privacy-statement/

Released under the Official Information Act 1982

IPP	Assessment	Compliance Rating	Risk ID
IPP 4	**IPP 4 requires agencies to collect personal information in a way that is lawful and seen as fair and reasonable in the circumstances. What is fair depends on circumstances such as the age of the individuals concerned (e.g. children), the sensitivity of the information, the purpose for collection and the degree to which the collection intrudes on privacy. OPC guidance provides that it may not be fair to collect information from children in the same manner as you would from an adult. Special care may be required with the information of young people to address any power imbalance.** **Lawful purpose:** The Ministry's collection and use of personal information in SMART is lawful on the basis that part of its role is provide support and resources for teachers, including resources for learning and assessment using platforms like SMART. SMART supports school board compliance with section 165 of the Education Act and regulation 21 of the Education Regs. **Fairness:** Large volumes of personal information about children across New Zealand will be collected and processed by SMART, including sensitive personal information like gender and ethnicity. The main fairness challenge is ensuring appropriate transparency, namely making sure students and their family | whānau understand how, when and why children's personal information is being collected. Given that most of that information is collected directly by schools on enrolment, this is primarily the responsibility of the schools. The Ministry should support this transparency as recommended in R01 and R02. Risks of unfair intrusion into the privacy of young people are managed by avoiding the collection of more personal information than the Ministry needs, including through accessing SMS data. There is no use of coercion or misleading practices to collect personal information.	**Compliant**	N/A

Released under the Official Information Act 1982

IPP 5	**IPP 5 requires agencies to ensure reasonable safeguards are in place in the circumstances to prevent loss, misuse or disclosure of personal information. The OPC states that if an organisation has a notifiable privacy breach, it must notify them as soon as possible (within 72 hours)[8].** Relevant considerations include physical, electronic and operational security, as well as security during transmission and destruction. What is appropriate in the circumstances depends on the sensitivity of the personal information involved, how it is being used, the available security measures and the consequences for individual if the information is not kept secure. SMART does not yet have current Certification and Accreditation, which would provide a level of assurance that security safeguards are reasonable in accordance with IPP 5. We understand this process is currently underway and recommend following the more detailed security findings that assessment will produce. From the evidence provided, the Ministry's use of SMART appears to be compliant with IPP 5 due to the following measures. However, we note potential risks associated with manual processes for updating RBAC when a Ministry staff member changes roles as discussed in R03. • **Data storage in New Zealand:** All personal information is stored in Microsoft Azure data centres in New Zealand, with the exception of the disaster recovery back up in Australia. • **Segregation of data:** Ministry data is kept in a separate, secure section of the Janison network, isolated from other customers. This prevents data mingling and accidental disclosure and supports privacy protection. • **Database and storage security:** The use of enterprise-grade cloud storage with government-level compliance certifications is consistent with reasonable safeguards. • **Encryption:** All personal information is encrypted while it is stored in SMART. It is also encrypted in transit when personal information travels across the network (e.g. from a school to SMART, from SMART to the Ministry, or between systems inside Azure). • **Access controls:** Role-based access controls linked to Ministry identity providers (DI4OL, ESL, Entra ID), multi-factor authentication at the infrastructure level and privileged access	**Compliant**	R03

Released under the Official Information Act 1982

IPP	Assessment	Compliance Rating	Risk ID
	management for sensitive roles help ensure access is only given to those with a legitimate need to access personal information and reduces the risk of employee browsing and accidental access. However, we note that RBAC is not automatically updated when an individual changes roles and instead there is a reliance on manual processes, introducing scope for oversight or human error. • **Monitoring and logging:** Continuous monitoring by Janison of SMART access attempts and the regular auditing of logs provide accountability and rapid detection of unauthorised access attempts. • **Third-party restrictions:** Contractual clauses are currently under negotiation but are expected to prevent Janison from using or disclosing personal information for its own purposes. External experts such as psychometricians and item developers do not receive any personal information.		

[8] https://www.privacy.org.nz/privacy-principles/5/

Released under the Official Information Act 1982

IPP	Assessment	Compliance Rating	Risk ID
IPP 6	**IPP 6 provides individuals with the right to request confirmation an agency holds their personal information and access to that information.** Access to personal information will be available as follows. • **SMS-held data:** Most of the personal information in SMART is collected and stored by schools | kura in their SMSs. Students | ākonga and teachers | kaiako should therefore follow existing school IPP 6 and IPP 7 processes to access and correct this information at its source. • **SMART results:** Student | ākonga personal information in the form of assessment results, accessibility settings and progression information is collected directly by the Ministry and can be accessed directly within SMART. • **SSO tools:** Students | ākonga and teachers | kaiako can follow existing IPP 6 processes for each of DI4OL, ESL and N4L to access their information.	**Compliant**	N/A

Released under the Official Information Act 1982

IPP	Assessment	Compliance Rating	Risk ID

IPP 7	**IPP 7 provides individuals with the right to ask an agency to correct information about them if they think it is wrong. If an organisation does not agree that the information needs correcting, an individual can ask that an agency attach a statement of correction to its records, and the agency should take reasonable steps to do so.**
	
	Individuals will be able to request correction of their personal information as follows.
	
	• **SMS-held data:** Most of the personal information in SMART is collected and stored by schools in their SMSs. Students and teachers will therefore follow existing school IPP 6 and IPP 7 processes to access and correct their information.
	
	• **SMART results:** Student personal information in the form of assessment results, accessibility settings and progression information can be corrected within SMART as follows.
	
	  ○ Student | ākonga progression details can be corrected within SMART, which synchronises with and updates the relevant SMS.
	
	  ○ Incorrect assessment details (e.g. entered incorrectly by a teacher) can be corrected directly by a teacher | Kaiako in SMART.
	
	  ○ Student | ākonga accessibility settings can be changed directly by a student | ākonga or teacher | kaiako in SMART.
	
	• **SSO tools:** Students | ākonga and teachers | kaiako can follow existing IPP 7 processes for each of DI4OL, ESL and N4L to correct their information.
		Compliant	N/A

Released under the Official Information Act 1982

IPP	Assessment	Compliance Rating	Risk ID
IPP 8	**IPP 8 requires agencies to check personal information is accurate, up to date, complete, relevant and not misleading before using or disclosing it.** Schools | kura are responsible for checking the quality of SMS and SSO data before they use or disclose it, noting school compliance with IPP 8 is out of scope for this assessment. Given the Ministry is indirectly collecting this information through schools, it too has IPP 8 obligations to take reasonable steps in the circumstances to ensure the personal information in SMART is accurate, up to date, complete, relevant and not misleading before using it. Insufficient information was available to ensure a fully informed view of whether the Ministry is taking reasonable steps to ensure the personal information in SMART is accurate and reliable. The Ministry has taken the following steps to comply with IPP 8, which are the basis of the "partially compliant" assessment. • Recognition of data integrity as critical in the Business Impact Assessment, which says a loss of data integrity (e.g. incorrect reporting on student progression) would be "extremely harmful". • Correction mechanisms are built into SMART (see the IPP 7 analysis). Data retention standards also play an important role in avoiding the retention of outdated or misleading information, noting the "non-compliant" rating for IPP 9. See the further discussion around accuracy risk under R04 in the Risk Assessment section of this report (section 8).	**Partially Compliant**	R04

Released under the Official Information Act 1982

IPP	Assessment	Compliance Rating	Risk ID
IPP 9	**IPP 9 requires agencies not to keep personal information for longer than it is required for the purpose for which it may lawfully be used.** • The Schools Retention Schedule sets out PRA record keeping requirements for schools | kura, which are outside the scope of this PIA. The Ministry is responsible for ensuring proper recordkeeping processes are in place for SMART and data in the EDW that satisfy PRA retention requirements. • We note the application of the Temporary Care Instruction, which the Ministry's Records Services team has advised applies to records in SMART and supersedes the requirements of the Schools Retention Schedule. The Temporary Care Instruction provides that child care records must be held **indefinitely** until Archives NZ can give specific instructions. That instruction is temporary and may change at a later date, so this does not remove the need for SMART to have disposal functionality. • Similarly, SMART personal information in the EDW must be retained **indefinitely** in accordance with the EDW Schedule, as confirmed by the Ministry's Records team. Irrespective of any minimum retention requirements, the Ministry is responsible for defining appropriate criteria and processes are in place in respect of **maximum** retention periods to ensure the appropriate removal / deletion of personal information from SMART in compliance with IPP 9. Janison has advised that it will provide the Ministry with the capability to remove information from SMART in compliance with its IPP 9 obligations. However, we understand such criteria and processes are yet to be defined (but are likely to be in place prior to the deployment of SMART).	**Non-Compliant**	R05

Released under the Official Information Act 1982

IPP 10	**IPP 10 requires agencies to only use personal information for the purposes for which it was originally collected, with limits on the use of personal information for different purposes. Other usage may be permissible, such as use that is directly related to the original purpose, with consent or under another exception to IPP 10.** The Ministry is yet to develop a privacy statement for SMART, which would typically specify the purposes for which personal information collected by the platform will be used. However, the relevant **purposes** for collection described in this assessment can be summarised as follows. • To provide a system to conduct assessments and record results that can be reported to student | ākonga, families | whānau, teachers | kaiako, schools | kura and the Ministry. • To inform the student | ākonga, teachers | kaiako and schools | kura of the progression aligned to the NZC | TMoA and help inform teaching practices. • To help the Ministry identify where educational resources are needed across the country. • To provide accessibility features so all students | ākonga can participate. • To ensure assessments in SMART are valid, fair and unbiased across diverse student populations by support the analysis of item performance in assessments. • To enable single-sign on authentication for secure access to SMART. At this early stage, the expected **uses** of personal information in SMART are expected to align with those purposes. But the Ministry will need to take care to ensure that it: a) defines its purposes with sufficient breadth to ensure all expected uses are captured (including future usage); b) communicates those purposes and uses in its privacy notices and communications; and c) implements appropriate measures to manage the risk of scope creep. Existing measures are discussed in section 6.9 of the main body of this PIA and appear to be largely sufficient at this stage, though scope creep risks remain. See the further discussion in relation to R06 in the Risk Assessment section.	**Partially Compliant**	R06

Released under the Official Information Act 1982

IPP	Assessment	Compliance Rating	Risk ID
IPP 11	**IPP 11 requires agencies to only disclose personal information for the purposes for which it was originally collected. Available exceptions include disclosure for a directly related purpose, disclosure with consent or where the relevant individuals will not be identified.** The Ministry discloses Student | ākonga assessment results and related personal information from SMART to schools | kura. Schools then share that information with students | ākonga and their families | whānau. This aligns with the original purposes for collection. Janison is a third party with access to personal information in SMART, but only as an "agent" (data processor) under section 11 of the Privacy Act. So this does not constitute the "disclosure" of personal information from SMART and IPP 11 will not apply. We are not aware of any other personal information from SMART being shared with other agencies or third parties.	**Compliant**	N/A
IPP 12	**IPP 12 provides that agencies may only disclose personal information outside New Zealand if they check that the receiving organisation will adequately protect the information (e.g. using appropriate contractual terms) or is subject to privacy laws that provide comparable safeguards to the Privacy Act.** The Ministry will not disclose any personal information overseas. Even though primary data is stored in New Zealand, disaster recovery backups in Australia mean personal information could be subject to Australian jurisdiction and legal access regimes (e.g. Australian law enforcement requests). However, provided Janison maintains its status as a data processor/agent under section 11 of the Privacy Act, this will not constitute a disclosure of personal information that requires compliance with IPP 12.	**Compliant**	N/A

Released under the Official Information Act 1982

IPP 13	**IPP 13 requires agencies to only assign unique identifiers to people when that is necessary for its functions. Agencies cannot assign a unique identifier that has already been assigned to that individual by another agency but they can record and use a person's unique identifier to communicate with another organisation about the individual. Organisations must also take reasonable steps to protect unique identifiers from misuse and make sure they verify someone's identity before assigning a unique identifier.** **National Student Numbers:** NSNs are centrally assigned by the Secretary for Education under the Education and Training Act 2020, as authorised in the NSN Notice. They are the official unique identifier for all students in New Zealand. Under the NSN Notice, the Ministry and registered schools are authorised to use those unique identifiers for various purposes, including ensuring students' educational records are accurately maintained. The Ministry is also authorised to establish and maintain student identities to support online learning, which includes submission, assessment and moderation. The Ministry handling of NSNs in SMART appears to be consistent with IPP 13 for the following reasons. • NSNs are not assigned by SMART. They are assigned and maintained by the Secretary for Education under statutory authority. • SMART does not reassign NSNs or generate derivative identifiers. It uses the existing NSN as the official unique identifier for lawful, education-related purposes. • Students | ākonga are not asked to disclose their NSN directly to SMART. Instead, NSNs are provided via school SMS or Ministry data sources. • The Ministry takes reasonable steps to safeguard NSNs from misuse by treating them as "In-Confidence" information, applying access controls and Single Sign-On (SSO), encrypting data, hosting SMART securely in New Zealand, undertaking regular penetration testing, monitoring access with audit logs, and ensuring incident response processes are aligned with ISO 27001.	**Compliant**	N/A

Released under the Official Information Act 1982

Student IDs: Student IDs are school-assigned identifiers generated in each school's SMS. In SMART, they are used only to build and manage groups of students (e.g. classes, reading groups) and ensure assessment results are correctly matched and returned to the school's SMS.

SMART's handling of school-assigned Student IDs is consistent with IPP 13 for the following reasons.

- Student IDs are not assigned by the Ministry or SMART. They are created and maintained by each school as part of SMS operations.
- SMART does not reassign Student IDs or treat them as Ministry identifiers. They remain school-specific and the Ministry simply records these unique identifiers assigned by schools for the sole purpose of communicating with schools about the individual.
- Students | ākonga are not asked to disclose Student IDs to the Ministry / SMART. Instead, IDs are transferred automatically from the school's SMS.
- The Ministry takes reasonable steps to safeguard Student IDs from misuse by treating them as "In-Confidence" information, ensuring their secure transfer between SMS and SMART, applying access controls and audit logging within SMART and not retaining them beyond what is needed to return results.

SMART IDs

SMART IDs are internally generated within the SMART platform to enable psychometricians to analyse student responses and item performance without reference to NSNs or school-assigned Student IDs. Each SMART ID is unique within SMART, has no meaning outside the solution and is not shared or used by other agencies. It is not an "official" identifier like an NSN, nor is it visible to schools or students.

SMART's handling of SMART IDs is consistent with IPP 13 for the following reasons.

- SMART IDs are only allocated to individuals where necessary to support the Ministry's legitimate functions of psychometric analysis and calibration of assessment items.

Released under the Official Information Act 1982

IPP	Assessment	Compliance Rating	Risk ID
	• They are not used or reassigned by other agencies and are only generated once a student's | ākonga identity has already been clearly established through their NSN and/or school-assigned Student ID. This ensures that identifiers are not created until the student's | ākonga identity is validated. • We understand the Ministry takes reasonable steps to safeguard SMART IDs from misuse in the same way as it protects other data, including by treating them as "In-Confidence" information and implementing access controls, encryption, secure hosting, audit logging of access and retention limits so data is only kept for as long as needed.		

Released under the Official Information Act 1982

8. Risk Assessment

The Ministry has an established Risk Assessment Methodology that must be used to assess privacy risks (see Appendix 1). The outcome of the risk assessment process is documented in the following table. As per advice from the Office of the Privacy Commissioner, the risk assessment does not set out to identify and eliminate every possible privacy risk. Its role is to identify genuine risks that are not unreasonably small or remote.

Definitions

Current risk: Level of risk based on current controls in place. If there are no current controls in place, then the current risk rating should be read as the inherent (uncontrolled) risk rating.

Residual risk: Level of risk once planned actions have been successfully applied.

Actions: Treatments or remediations that are planned but not yet underway or in place.

Recommended actions: Actions that the project/initiative will not or cannot commit to implementing. Recommended actions are included when the Privacy team has identified a need to communicate and document best privacy practice and/or future considerations.

Risk ID	Risk Description	Existing Controls	Current Risk			Actions	Residual Risk			Comments and Recommended Actions
			Likelihood	Impact	Rating		Likelihood	Impact	Rating	
R01	**Lack of transparency for direct collection** The Ministry is not sufficiently transparent about the way personal information is collected and handled in respect of assessment results and accessibility settings in SMART. This results in a complaint to the Office of the Privacy Commissioner, a breach of IPP 3, media attention and reputational impact for the Ministry and schools.	A Privacy Statement about the collection and use of student personal information in relation to assessment results and accessibility settings in SMART has not yet been developed. It is expected that a notice similar to the e-asTTle Privacy Statement[9] will be made available on the Ministry website.	Unlikely	Major	MEDIUM	1. Develop a compliant, age appropriate Privacy Statement about the collection and use of student | ākonga personal information in relation to assessment results and accessibility settings. This could be based on the e-asTTle Privacy Statement[10] but should also reflect the unique properties of SMART and be drafted in a way that makes it easily comprehensible by even young children. 2. Publish the Privacy Statement on the Ministry website and within SMART. 3. Provide age appropriate point in time privacy notices at relevant points within SMART.	Rare	Major	LOW	

[9] See https://newzealandcurriculum.tahurangi.education.govt.nz/e-asttle-overview-and-access/5637219681.p?activeTab=tab:2
[10] See https://newzealandcurriculum.tahurangi.education.govt.nz/e-asttle-overview-and-access/5637219681.p?activeTab=tab:2

Released under the Official Information Act 1982

Risk ID	Risk Description	Existing Controls	Current Risk			Actions	Residual Risk			Comments and Recommended Actions
			Likelihood	Impact	Rating		Likelihood	Impact	Rating	
-R02	**Perceived lack of transparency for indirect collection** IPP 3A exceptions are held not to apply or the Ministry is perceived as not being sufficiently transparent about the way it indirectly collected and handles personal information in SMART. This results in a complaint to the Office of the Privacy Commissioner, a breach of IPP 3A, negative media attention and reputational impacts for the Ministry and schools.	Reliance on IPP 3A exceptions	Possible	Major	MEDIUM	1. Support school compliance with IPP 3 by providing template privacy notice wording to schools that references the indirect collection of personal information by the Ministry. 2. Publish a SMART privacy notice as discussed in relation to IPP 3 3. Add age-appropriate, point in time privacy notices within SMART to clearly explain the Ministry's use of SMS data and other data collected by schools for SSO purposes.	Rare	Major	LOW	

Released under the Official Information Act 1982

Risk ID	Risk Description	Existing Controls	Current Risk			Actions	Residual Risk			Comments and Recommended Actions
			Likelihood	Impact	Rating		Likelihood	Impact	Rating	
R03	**Security breach** Given the volume and sensitivity of the personal information in SMART, some security risks remain around: 1. Manual updating of Role-Based Access Controls when staff change roles, which could result in "privilege creep" or the persistence of excessive or inappropriate access. 2. At the time of drafting this PIA, contractual clauses setting out Janison's obligations in respect of the personal information in SMART are still under negotiation. Until finalised, there is uncertainty as to the extent to which Janison will have enforceable obligations to support the Ministry's compliance with the Privacy Act. If these risks were to eventuate, this could result in complaints to the Privacy Commissioner, a notifiable privacy breach, a breach of IPP 5, a contractual dispute with Janison, media attention and reputational impact for the Ministry and schools.	The measures in place to safeguard the personal information in SMART include the formal categorisation of all SMART data as "In-Confidence", RBAC linked to SSO (thereby reducing the risk of unauthorised access or unauthorised use of identifiers), encryption, secure hosting in New Zealand, data segregation, database and storage security measures, regular penetration testing and reporting, incident response aligned with ISO 27001 and monitoring of system access and audit logging.	Unlikely	Severe	MEDIUM	1. Automate RBAC updates by integrating with HR/payroll systems and implementing quarterly access reviews to verify staff permissions are appropriate. 2. Finalise the contract with Janison so it is clearly identified as a processor under s 11, has robust obligations to protect personal information in SMART and provide prompt notification of any data/privacy breach and to is subject to audit rights by the Ministry. Establish regular contract performance reviews and include penalties for non-compliance.	Rare	Severe	MEDIUM	

Released under the Official Information Act 1982

R04	**Inaccurate personal information leads to errors, unfair outcomes and unreliable decision-making** Potential risks include: • Out of date / incorrect personal information imported from school SMSs results in assessment results being attributed to the wrong student | ākonga. • Inaccurate assessment results generated in SMART misrepresent student | ākonga performance, learning needs or progression, leading to poor teaching decisions or unfair disadvantage. • Misconfiguration errors and/or automated scoring of close-ended questions (e.g. multiple-choice - approximately 90%) and inconsistent marking by teachers of open ended, free-text answers (approximately 10%) may lead to incorrect outcomes misrepresenting results. • SMART data fed into the EDW is inaccurate or irrelevant, skewing system-level insights, affecting resource allocation or misinforming policy. • Authentication details collected by schools | kura are wrong, with individuals denied access to SMART or students | ākonga having their results linked to the wrong record. This results in complaints to the Privacy Commissioner, a breach of IPP 8, negative media attention, reputational impacts for the Ministry and schools and erodes trust in	Regular synchronisation between each SMS and SMART reduces the chance of outdated or mismatched records persisting. Assessment and system-level issues will be considered and addressed during user acceptance testing (UAT) and wider SMART system testing. For marking of open-ended questions, teachers | kaiako receive training and education on appropriate marking, including scoring sheets detailing the relevant criteria students | ākonga need to meet and exemplars of what teachers | kaiako should be looking for. At the end of each assessment period, psychometricians conduct a review of items/questions to see whether there any issues with the way items are presented and responded to by students | ākonga. That includes thorough testing of assessments to identify and address any misconfiguration and automated scoring errors for multi-choice, close-ended questions.	Possible	Severe	HIGH	SMS–SMART synchronisation means "garbage in" at the SMS level may still lead to "garbage out" in SMART and beyond. It should therefore look to do the following where feasible. 1. Implement automatic alerting of data mismatches or anomalies (e.g. same NSN linked to two schools; mismatched age/year). 2. Build error detection into SMART automated scoring to identify misconfigured items before they impact students. 3. Apply data quality checks before SMART pushes results to the EDW (e.g. reject incomplete or inconsistent records). 4. Regularly remind schools to strengthen validation rules in the SMS, including checking the accuracy of key fields.	Unlikely	Severe	MEDIUM	To that extent that generative AI is used in SMART (e.g. to score close-ended questions and assist teachers | kaiako reviewing answers to open-ended questions), conduct an AI Impact Assessment (e.g. using the AI Impact Assessment Toolkit at https://data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/algorithm-impact-assessment-toolkit. Any alternative form of AI risk assessment conducted needs to consider the same questions in relation to hallucination considerations. This will hep identify key risks and mitigants, including in relation to accuracy issues (e.g. "hallucinations") and bias risks.

Released under the Official Information Act 1982

Risk ID	Risk Description	Existing Controls	Current Risk			Actions	Residual Risk			Comments and Recommended Actions
			Likelihood	Impact	Rating		Likelihood	Impact	Rating	
	SMART (including potential loss of social licence for the SMART system).									
R05	**Personal information is retained excessively** Personal information is retained by the Ministry for longer than is operationally necessary, increasing exposure in the event of a security breach, prompting complaints to the Privacy Commissioner, a breach of IPP9, negative media attention and reputational impacts for the Ministry and schools.	• Janison will provide the Ministry with the capability to remove information from SMART to support the Ministry's compliance with its IPP 9 obligations to only retain personal information for as long as it is required for the purpose for which it may lawfully be used. • Janison has advised they will implement the removal of personal information using a combination of built-in platform functions and processes run at the Ministry's request based on the Ministry's requirements. • The Ministry is in the process of configuring SMART, which means retention and deletion requirements and settings are not yet defined or operational.	Possible	Major	MEDIUM	1. Define the criteria and processes for the retention and disposal of personal information in SMART for when the current Temporary Care Instruction is revised / removed. 2. Ensure Janison is contractually required to provide the Ministry with the capability to remove information from SMART to support its compliance with IPP 9, including obligations not to delete or alter records outside approved processes and to only retain personal information in accordance with Ministry instructions.	Unlikely	Major	MEDIUM	

Released under the Official Information Act 1982

Risk ID	Risk Description	Existing Controls	Current Risk			Actions	Residual Risk			Comments and Recommended Actions
			Likelihood	Impact	Rating		Likelihood	Impact	Rating	
R06	**Scope creep breaches purpose and use limitation requirements** At a later date, the Ministry uses SMART personal information for purposes beyond those originally defined. This results in complaints to the Privacy Commissioner, breaches IPP 1, 3 and 10 of the Privacy Act, attracts negative media attention, has reputational impacts for the Ministry and schools and erodes trust in SMART.	• Expected contractual obligations on Janison not to use or disclose the personal information in SMART for their own purposes. • All Ministry staff are given mandatory privacy training as part of the staff onboarding process. • SMART will generate and retain audit logs recording access to personal information. • Ministry staff use of SMART data will be subject to governance and operational processes required for all systems handling "IN-CONFIDENCE" personal information. • The Ministry's DPM team produce reports on user access to SMART data, working with the business to adjust access as necessary where there are reports of unusual access. • Other Ministry requests for access to SMART data will be managed by a SOP / process that is yet to be developed.	Possible	Major	MEDIUM	1. Document the Ministry's purposes for collecting personal information in SMART, including in SMART privacy notices. Ensure the purposes are defined with sufficient breadth to capture all current and expected future uses. 2. Maintain strict governance processes for approving requests for new uses of SMART personal information, including updated PIAs and privacy notice updates. 3. Ensure the agreement clearly documents Janison's role as a data processor who may not use or disclose SMART personal information for its own purposes (e.g. aggregated data analytics / reporting across its customer base). This should be supported by strong audit and enforcement provisions. 4. Prioritise the development and implementation of the use request SOP, with clear approval pathways, documentation and oversight to minimise risks of ad hoc access approvals that bypass purpose-limitation safeguards. 5. Conduct regular sampling of access log data. Consider adopting anomaly detection to highlight unusual access patterns.	Rare	Major	LOW	

Released under the Official Information Act 1982

Appendix 1: Ministry Risk Assessment Methodology

The following tables and matrix are used to assess the risks in Section 8 and are taken from the Ministry's Enterprise Risk Management Framework, issue date August 2022.

Table 1: Impact Assessment

	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.

Released under the Official Information Act 1982

	Harm & Safety	Service Delivery	Financial	Legislative	Trust & Confidence
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.

Released under the Official Information Act 1982

	Harm & Safety	Service Delivery	Financial	Legislative	Trust & Confidence
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.

Released under the Official Information Act 1982

	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.

Released under the Official Information Act 1982

	Harm & Safety	Service Delivery	Financial	Legislative	Trust & Confidence
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 of no media interest or coverage.

Table 2: Likelihood Assessment

Likelihood	Risk Level		
	Operational and Enterprise Risk	**Change Risk**	**Strategic Risk**
Almost Certain	Operational and Enterprise risk timeframes are often relatively short, reflecting their activity-based exposure. **Often expected in the next 1 – 2 years**	Change risk timeframes are dependent upon the length of the programme or project. **Within the change programme/project timeframe**	Strategic risk timeframes are often but not always longer reflecting their future delivery. **Often expected in the next 2 – 5 years**
Likely			
Possible			
Unlikely			
Rare			

Released under the Official Information Act 1982

Table 3: Risk Rating 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

Released under the Official Information Act 1982

Appendix – Data Elements

The following table details the personal information that will be collected, stored and used in SMART.

Stakeholder	Attribute	Source
Student | Ākonga	National Student Number	SMS
	School Student ID	SMS
	Name	SMS
	Gender	SMS
	Year / Level	SMS
	Ethnicity	SMS
	Accessibility settings	Set within SMART
	Assessment results	Created in SMART
	Email Address	Identity Provider (DI4OL)
Teacher | Kaiako	Name and email address	Identity Provider Education Sector Logon (ESL)
School Administrators	Name and email address	Identity Provider Education Sector Logon (ESL)

Released under the Official Information Act 1982

Te Tāhuhu o te Mātauranga
Ministry of Education

Released under the Official Information Act 1982

We **shape** an **education** system that delivers **equitable** and **excellent outcomes**

He mea **tārai** e mātou te **mātauranga** kia **rangatira** ai, kia **mana taurite** ai ōna **huanga**

education.govt.nz

Te Kāwanatanga o Aotearoa
New Zealand Government