Regulatory Impact Statement

Establishing and managing verified student identities to support students' access to online services

Agency Disclosure Statement

This Regulatory Impact Statement has been prepared by the Ministry of Education.

This Regulatory Impact Statement provides an analysis of the options to establish and manage verified student identities that students can continue to use as they progress through the education system, including re-engaging in education after completing tertiary education.

The Ministry completed an extensive analysis of the options for establishing a verified and persistent student identity and logon. The analysis draws on the Ministry of Education's knowledge of the environment from our previous engagement with the sector, experience of identity and access management technologies and approaches. Time constraints prevented gathering feedback on the current environment across education providers. The options have been costed using the Ministry's expertise and experience of the system and process resource requirements for each option.

Consultation on the options to establish a persistent student identity and logon to support a sector approach to student identity and access management was undertaken with the Government Chief Privacy Officer (GCPO) and the Office of the Privacy Commissioner (OPC). The Department of Internal Affairs has also been consulted.

A privacy analysis was completed of the options to establish the student identity and associated logon. A privacy impact assessment (PIA) was completed of the sector approach to student identity and access management. The PIA was reviewed by the GCPO and OPC and there will be ongoing engagement with them. The Ministry considers that the identified privacy risks can be managed through system design and business processes.

The Ministry considers this document to be a fair representation of the analysis of available options. There will be ongoing engagement with the sector through its representative organisations to finalise business requirements to inform the phased implementation of the sector approach to student identity and access management.

Ben O'Meara, Group Manager, Schooling Policy, Ministry of Education

Glossary of systems referred to in this RIS

System	Definition
Early Learning Information System (ELI)	Collects and stores information on enrolment and attendance in Early Childhood Education for approximately 180,000 children throughout New Zealand.
e-asTTle	An online assessment tool, developed to assess students' achievement and progress in reading, mathematics, writing, and in pānui, pāngarau, and tuhituhi.
Education Sector authentication and authorisation Service (ESAA)	Provides identity management and centralised authentication and authorisation information for connected online services for the education sector workforce.
ENROL	ENROL is a register of student enrolments. It lets schools update enrolments as students enrol, change schools or leave the school system. All schools must use it.
National Student Index (NSI)	The NSI is a database maintained by the Ministry of Education. The purpose of the application is to allocate a unique identifier, the National Student Number, to every student enrolled in an education provider in New Zealand.
Progress and Consistency Tool (PaCT)	Online system supporting dependable teacher judgments in relation to the New Zealand Curriculum's reading, writing, and mathematics standards.
Progressive Achievement Tests (PAT)	Assess students' mathematics, listening comprehension, punctuation and grammar, reading comprehension, and reading vocabulary. PATs are a series of standardised tests developed specifically for use in New Zealand schools some of which are available online.
Student Management System (SMS)	Systems used by education providers to manage student information and functions such as registration, enrolment, reporting, attendance and lesson planning.

Executive Summary

1. The online learning environment is part of the New Zealand education system. Students use digital channels to access applications, services, tools, content and forums as part of their personal education and learning programme.

2. Current identity and access management practices are determined by the needs of the schools and/or providers resulting in multiple usernames, passwords and update processes for students.

3. We need to provide students with a trusted and persistent verified identity and associated logon that they can continue to use to access online services as they progress through the education system. This will support the current online learning environment.

4. This Regulatory Impact Statement considers four options to establish a persistent verified student identity:

    - Amend the legislation to allow the National Student Number (NSN) to be used
    - Use another persistent unique identifier
    - Undertake data matching between existing systems holding student identity data
    - Use RealMe to create the student identity.

5. The options were assessed against operational, fiscal, compliance and privacy considerations. Following this assessment, the Ministry recommends that Part 30 of the Education Act 1989 be amended to authorise the NSN to be used to verify and manage students' identities as the basis for a trusted logon for individual students to access online services.

6. The Ministry considers that the proposed use is consistent with the overall purpose for the NSN: *use by authorised users of the national student numbers for specific purposes, in order to facilitate the accurate use and transfer, by authorised users, of information relating to individual students.*[1]

[1] Section 341 of the Education Act 1989.

Context

7. This Regulatory Impact Statement analyses options to establish and manage verified student identities as the basis for a trusted logon (ie, username and password) for individual students to access online services.

8. The process of establishing and managing student identities and associated logons for the purpose of managing access to services is broadly described as 'identity and access management'.

9. The Ministry of Education (Ministry) manages the Education Sector Authentication and Authorisation (ESAA) system, which provides IAM services for staff and administrators across the sector, such as:
    - teachers and school administrators: to access selected systems (eg, ENROL, e-asTTle). Teachers and school administrators use the single logon created in ESAA (following an approved application form for access to a service) to access the systems they have authorisation for.
    - tertiary providers' administrators: to access a range of services from the Ministry, Tertiary Education Commission and NZQA.
    - early childhood services staff: to access the Early Learning Information system and the National Student Index.

Status Quo

10. The online learning environment is part of the New Zealand education system. This applies across the education system, particularly in schooling, tertiary and for lifelong learning.[2] In the online learning environment students use digital channels to access applications, services, tools, content and forums as part of their personal education and learning programme.

11. Current IAM practices are driven by the particular needs of each education provider and education agency. There is not a sector approach or a student-centric approach to student IAM. As a result, the status quo is characterised by:
    - multiple usernames and passwords for students to access different online services while at the current education provider
    - multiple logon creation and update processes in each education provider to enable students to access the online services
    - requiring new usernames and passwords for the same services when a student transfers to another education provider or is participating (onsite or virtually) in classes at another education provider.

12. The prevalence of online services that require individual student logons is evident in the schooling sector in the '2014 Digital Technologies in Schools' survey, which highlights the significant changes that have occurred in the digital technology space since the 2011 survey. The Ministry estimates that students would access 10-20 online

2 Early childhood education also uses digital technologies but the requirement for individual logons is less of an issue in this sector.

services on a regular basis. The online services in the 2014 survey support personalised learning programmes.[3]

- 2011: internet services include: social networking (eg, Facebook, Google+, Linkedin), social software (eg, blogs, wikis, RSS feeds, etc), closed online communities (password protected) and open online communities
- 2014: future-focused learning applications, particularly TED talks, online assessments, gamification and Khan Academy.[4]

13. In the school sector, there are large numbers of students changing schools who will require a new logon often to access the same services. A manual process coordinated by the old and new school is required to maintain access to the student's previous account and work. Approximate student numbers are:
    - 114,000 students change schools at key transition points[5]
    - 30,000 students changed schools once during the school year[6]
    - 3,700 transient students changed schools two or more times per year[7]

14. Secondary students are also participating in tertiary programmes, which is likely to require access to additional online services. In 2013:
    - 13,670 students: Secondary-Tertiary Alignment Resources Programme
    - 14,014 students: Gateway
    - 4,034 students: Trades Academies.

15. The need for multiple logons also exists in the tertiary sector with nearly 28,000 students attending two or more tertiary providers at the same time.

16. There is an opportunity to improve efficiencies and practices in how IAM services are delivered in the sector:
    - administrative burden of managing logons and passwords that is diverting resources from education and learning. Anecdotally, the Ministry is aware that individual teachers decide not to use an online service if the registration process is complex or cumbersome.[8]
    - avoiding rescheduling e-asTTle assessments due to password issues
    - enabling students to continue to access their content when they change schools rather than schools having to manually do this
    - variability of online security practices due to the volume of logons and password resets which compromises privacy and security, particularly for higher value

3 The 2014 survey shows that students in: 94% of schools are accessing online learning resources and/or using online learning games, 44% of schools are using online collaborative networks and projects, 34% are accessing social web resources; 59% are using GoogleApps (as an example of a utility application).

4 TED talks: nonprofit, global community to foster information sharing and discussion using technology, entertainment and design. Gamification: uses games to engage users in solving problems and increase users' contributions; game-based learning is to make education more engaging and relevant to students. Khan Academy: nonprofit organisation providing practice exercises, instructional videos, personalised learning dashboard. Adaptive technologies are used to identify gaps and weaknesses and adjust the programme.

5 Based on July 2014 roll return data; approximately 57,000 transition from primary, to intermediate and secondary each year. This is indicative as some students will be in full primary and composite schools.

6 Based on Ministry of Education data for 2013.

7 http://www.educationcounts.govt.nz/indicators/main/student-engagement-participation/transient-students

8 This view aligns with a US article on K12 schools found the management of separate logons for multiple online services resulted in a tendency to use fewer services. District Administration 2012, 481(1).

services such as summative online assessment and inhibits the sector's ability to adopt these online services.

Problem definition

17. Students' identities and associated logons to access online services are managed by their current education providers. The identities and logons cannot follow the student as they change education providers and progress through the education system.

18. This means that students have to get new identities and logons to continue to access the online services they need, and may lose access to content held in online services. The education providers' IAM systems may not provide the appropriate protections to enable their students to use high value online services (eg, undertake NCEA online assessments).

Policy objectives

19. The primary policy objective is:

    Students have a trusted and persistent verified identity and associated logon that they can continue to use to access online services as they progress through the education system. The persistent identity and logon will support the current online learning environment, and education sector online services will be able to rely on the trusted and verified identity.

20. The secondary policy objectives for a sector approach include[9]:
    - reducing the administrative burden for education providers and education agencies of managing students' identities and logons
    - education providers and education agencies can leverage the sector IAM infrastructure to enhance their own identity and access management processes.

21. Achieving the primary policy objective requires:
    - a system that establishes and manages a persistent verified student identity and associated logon
    - an accurate, efficient and secure means of ensuring the integrity of students' identities and associated logons.

Options to establish a persistent verified student identity

22. The Ministry considered four options to provide the accurate, efficient and secure means of establishing and maintaining the integrity of students' identities and associated logon:
    A. Amend the legislation to allow the National Student Number (NSN) to be used
    B. Use another persistent unique identifier
    C. Undertake data matching between existing systems holding student identity data
    D. Use RealMe to create the student identity.

23. The following criteria were used to assess each option to establish and maintain students' identities:

[9] Appendix 1 provides an overview of the proposed sector approach to student IAM.

Operational criteria

a. enables persistence of identity: students can continue to use the identity and associated logon as they progress through the education system
b. maintains the accuracy and integrity of the student's persistent identity
c. enables education providers to manage their students' identity records in their own systems for their purposes, and to maintain the sector persistent identity and logon

Fiscal and compliance

d. indicative fiscal costs: indicative build and operating costs for establishing and maintaining the verified student identity
e. compliance impacts for education providers

Privacy considerations

f. privacy considerations: the degree to which options comply with the Privacy Act 1993: a comparative analysis against the Information Privacy Principles is in Appendix 3.

24. The status quo is not a viable option as it does not achieve the three operational criteria.

Regulatory options

A Amend the Education Act to allow the NSN to be used

25. The NSN is the primary identifier for students in the education sector. It was established to facilitate the accurate use and transfer, by authorised users, of information relating to students for specific authorised purposes. The proposed use is not covered by the existing authorised purposes for the NSN. Appendix 2 provides background information on authorised users and authorised purposes for the NSN.

26. This option collects the NSN, along with identity data (names, date of birth and gender). The expected identity data sources are: ENROL for school students, tertiary providers' student management systems (SMS) for tertiary students, and potentially in the future, the Early Learning Information (ELI) system for children in the early learning sector.[10]

27. The NSN would be a core attribute of the identity record to ensure the continuity (or persistence) of that identity across sector and education providers' systems. The use of the NSN facilitates the accurate and efficient retrieval of additional data (eg, school, class, teacher) where it is required to authorise access to online services from authoritative sources. The likely data sources for this data are the education providers' SMS. The NSN will only be passed to authorised users to support existing authorised purposes.

28. Use of the NSN would be consistent with the overall purpose of the NSN, which is to facilitate the accurate use and transfer of personal information related to individual students. It would minimise system and process changes for education providers as the NSN is already an integral part of their ICT systems and processes.

10 ENROL and ELI are the national enrolment systems for the schooling and early childhood sectors respectively. Tertiary education providers do not have a national enrolment system and their SMS would be the identity data sources. Education providers in schooling and early childhood also use SMS to manage their own enrolments.

29. The analysis against the evaluation criteria is:

Criteria	Allow use of the NSN
Enables persistence of identity	Yes. The NSN is used by all education providers and education agencies for individual students and is an integral part of the education system.
Ensures data quality & identity integrity	Yes. The NSN is held in key sector and education provider systems holding identity data. Existing enrolment and data quality processes identify and resolve any potential errors (eg, duplicate records), which minimises the amount of manual exception handling required.
Enables education providers to manage identity records in SMS & maintain persistence	Yes. Education providers continue to manage identity records for their own students' in their SMS, while maintaining the persistence required for the identity and associated logon to follow the student.
Indicative fiscal costs	Indicative one-off costs $1.4m Indicative operating costs $0.5m
Compliance impacts	Low. Changes to SMS to enable the data required to authorise access to be retrieved will be managed via SMS product updates. A lower number of exceptions to resolve are expected.
Privacy considerations: summary of assessment against Information Privacy Principles	• Collection of personal information: Low impact as students and parents/caregivers would be notified by leveraging processes. • Storage and security: existing processes would be built on to manage the potential risk of unauthorised use or disclosure of the NSN and associated data if there was a security breach. • Access and correction: Ministry and education providers could leverage existing processes for this use. • Accuracy: the NSN is an integral part of existing processes to continually monitor and maintain data quality and accuracy. • Retention: the NSN will be part of the identity which is intended to persist throughout the individual's engagement with education. Processes to identify and manage inactive records would be required. • Use and disclosure: potential risk of unauthorised use and disclosure of the NSN and associated identity data would be mitigated by system design (for security breaches), conditions on use, education and guidance • Unique identifier: use of NSN for this purpose needs to be included in section 344 of the Education Act 1989.

B Use another persistent unique identifier

30. A new persistent unique identifier would be established and managed, potentially as part of the sector student IAM system, or in a separate system (eg, similar to the NSI). The system would use attributes sourced from education provider systems to establish the verified identity (eg, names, date of birth, gender, education provider) and assign a new unique identifier to each student identity. The NSN would not be used in this option.

31. This option would have to establish business processes to maintain the accuracy of the current education provider data to resolve identity record exceptions. This would replicate the existing business processes between the NSI and sector enrolment systems (eg, ENROL, ELI) and education providers' SMS to resolve duplicate records, as the NSN is used for these processes.

32. Legislative change would be required to authorise the unique identifier to be used by education providers and education agencies to provide the ongoing link between the sources of identity data and the sector student IAM system. Amending the legislation to add another unique identifier for students would effectively duplicate the NSN and create confusion.

33. As for Option A (NSN), Option B would also need to retrieve additional data where it was required to authorise access to online services from education providers' SMS. The detail of how the additional data would be collected and managed would need to be defined.

34. A new unique identifier for students would avoid further expansion of the authorised purposes of the NSN, but risks creating confusion for education providers with the NSN. A privacy code could be used to establish a new unique identifier, rather than legislation. However, the Office of the Privacy Commissioner has previously expressed reservations about a new education sector privacy code.

35. The analysis against the evaluation criteria is:

Criteria	Use a new persistent unique identifier
Enables persistence of identity	Yes. Once the unique identifier is in place.
Ensures data quality & identity integrity	Yes. Once the unique identifier is in place and business processes to resolve exceptions are in place. However, reliance on data matching processes to populate the new unique identifier increases the risk of errors.
Enables education providers to manage identity records in SMS & maintain persistence	Yes. Education providers continue to manage identity records for their own students' in their SMS, while maintaining the persistence required for the identity and associated logon to follow the student.
Indicative fiscal costs	Indicative one-off costs $2.3m Indicative operating costs $0.9m
Compliance impacts	Medium. Will require a greater level of change to education provider and education agencies systems to include the new unique identifier for all students, as well as retrieving data required to authorise access to online services (managed via SMS product updates). A lower number of exceptions to resolve are expected once the new unique identifier is fully implemented.
Privacy considerations: summary of	• Collection of personal information: low impact as students and parents/caregivers would be notified by leveraging existing

Criteria	Use a new persistent unique identifier
assessment against Information Privacy Principles	processes. • Storage and security: existing processes would be built on to manage the potential risk of unauthorised use or disclosure of the new unique identifier and associated data if there was a security breach. • Access and correction: Ministry and education providers could leverage existing processes for this use. • Accuracy: new processes would be required to maintain the links between the student and current education provider. • Retention: the new unique identifier would be part of the identity which is intended to persist throughout the individual's engagement with education. Processes to identify and manage inactive records will be required. • Use and disclosure: potential risk of unauthorised use and disclosure would be mitigated by system design (for security breaches), conditions on use, education and guidance. • Unique identifier: requires a legislation mandate or a privacy code to be compliant.

Non-regulatory options

C Data matching of sector systems

36. This option would collect student data from ENROL to establish the initial identity. Ongoing data matching processes would be necessary to establish and maintain the students' identities. The data would include student names, date of birth, gender, education provider. The NSN would not be used.

37. Alternative mechanisms would be required in the tertiary sector to obtain the required identity data. This option could not leverage the existing business processes for conflict resolutions (eg, between NSI and ENROL, which uses the NSN) and would need to establish new processes.

38. The resulting identity record for each student (names, date of birth, gender, education provider) would be held in the sector student IAM system. In addition to core identity data, the data required for access authorisation purposes (eg, class, teacher, etc in a school context) would be retrieved from the SMS. This would require the sector student IAM system to generate and send an internal system code specific for each student to the current education provider.

39. A new internal system code would have to be generated when students moved to a new education provider. The alternative is to use multiple data attributes for data matching and retrieval processes.

40. The data matching option is not dependent on a legislation change, avoids further expansion of authorised purposes for the NSN and does not create a unique identifier that is shared with multiple agencies.

41. The analysis against the evaluation criteria is:

Criteria	Data matching of sector systems
Enables persistence of identity	Partial. Only after significant data matching effort. Requires that data from the source systems be available to enable the data matching process to identify and remove duplicates.
Ensures data quality & identity integrity	Partial. Reliance on data matching processes across multiple systems increases risks of errors. Resolving large numbers of exceptions is also likely to affect data quality and integrity.
Enables education providers to manage identity records in SMS & maintain persistence	Partial. Education provider can manage identity in their own SMS, but this does not maintain a persistent identity.
Indicative fiscal costs	Indicative one-off costs $2.6m Indicative operating costs $1.8m
Compliance impacts	High. Changes required for the system-generated internal identifier to be held for the retrieval of data required to authorise access (managed via SMS product updates). Likely to be higher volumes of exceptions to resolve (eg, duplication, errors), which will require input from education providers
Privacy considerations: summary of assessment against Information Privacy Principles	• Collection of personal information: low impact as students and parents/caregivers would be notified by leveraging processes. • Storage and security: potentially creates another repository of identity data solely for data matching purposes to establish the student identity. • Access and correction: Ministry and education providers could leverage existing processes for this use. • Accuracy: relies on ongoing data matching processes and an associated internal system-identifier to maintain the necessary links with the current education provider. There is a greater risk of errors occurring with these processes. • Retention: the identity is intended to persist throughout the individual's engagement with education. Processes to identify and manage inactive records would be required. • Use and disclosure: potential risk of unauthorised use and disclosure from repository of identity used for data matching would be mitigated by system design (for security breaches) and conditions on use. • Unique identifier: does not require a unique identifier that is used or assigned by another agency.

D Use RealMe to create identity

42. RealMe was investigated as an option. The Department of Internal Affairs (DIA) has advised that, although RealMe provides authentication and verified identity services, it is not a full identity and access management system. Organisations using the RealMe login service use other software or services to meet their full identity and access management requirements.

43. RealMe complies with relevant security and authentication standards applicable to the delivery of government services online. This includes the password standard, which mandates the use of a complex password. As a result, the RealMe login is not suitable for use by younger students and would almost certainly result in increased user support. Additionally, parental consent is required for children under the age of 14 to apply for a RealMe verified identity. For these reasons the RealMe services, as they exist today, cannot satisfy all the requirements of the education sector.

44. To support the needs of younger students, the education sector needs solutions that allow for delegated administration privileges, where a teacher might reset a student's password or change access permissions in a classroom. .

45. The Ministry and DIA are continuing to work collaboratively to take a sector wide approach to the use of RealMe and explore opportunities to leverage the education sector logon and RealMe services as students start to engage more broadly with other government services.

Summary of analysis of options to establish the student identity

46. The key differences between using the NSN (Option A) and a new unique identifier (Option B) are the indicative fiscal costs and compliance impacts as the NSN is already in use in the education sector. Data matching does not rate highly on any of the evaluation criteria. The following table summarises the assessment process undertaken across the three options that were evaluated. The criteria and scoring used in the assessment is in Appendix 4.

	Options		
Criteria	**Use the NSN**	**New Unique Identifier**	**Data matching**
Operational			
Enables persistence of identity	5	5	2
Ensures accuracy & integrity of persistent identity	4	4	2
Enables education providers to manage identity & retain persistent identity	5	5	3
Fiscal & compliance			
Indicative fiscal costs	4	2	1
Compliance impacts	4	3	2
Privacy considerations			
Minimises privacy impacts	3	3	2
Total	**25**	**22**	**12**

47. The preferred option is Option A (use NSN) to provide an accurate, efficient and secure means of ensuring the integrity of persistent student identities and associated logons established and managed in an IAM system. This option requires that Part 30 of the Education Act 1989 be amended to authorise the NSN to be used to verify and manage students' identities as the basis for a trusted logon (ie, username and password) for individual students to access online services.

Options to implement a sector approach to student identity and access management

48. Three scope options were considered to implement the proposed authorised purpose for a sector approach to student IAM:

	Implementation scope	Authorised users (as set out in Appendix 1)
1	Sector student IAM system: centralised repository of the verified, persistent student identity and associated logon, and where necessary, data required to authorise access to online services	Ministry of Education or their agent, if delivered by a contracted service provider
2	Plus, identity and access management systems operated by education agencies	As above, plus, education agencies (NZQA, Tertiary Education Commission, Careers NZ)
3	Plus identity and access management systems operated education providers	As above, plus, education providers

49. The privacy impact assessment (PIA) considered, Option 3, which would allow all authorised users to use the NSN for the proposed purpose, once approved by the Secretary for Education by notification in the Gazette. The PIA highlighted that the wider scope resulted in multiple instances of IAM systems. This resulted in an increase in the:
    - likelihood that one will be breached
    - likelihood that the provider of a system will breach a privacy principle either through collection and notification, security and storage access, retention, use and disclosure
    - complexity and effort of governing and assuring privacy practices and security controls
    - likelihood that information will be accidentally or deliberately inappropriately used or disclosed
    - volume and quantity of personal information collected and stored about students.

50. Scope risks can be managed through a phased implementation, along with appropriate controls. Authorised users would be progressively approved to use the proposed authorised purpose through the existing Gazette notification process (section 344(3) of the Education Act 1989). The phased implementation will be supported by education and training for education providers and prescribed requirements for all authorised users when approved to use the proposed authorised purpose, along with monitoring through governance processes.

51. The PIA highlighted that the key privacy risks for students arise from the implementation of the legislation amendment through the sector approach to IAM and the sector student IAM system. These include:
    - use of the NSN as an identifier for unauthorised purposes by authorised users and third party service providers. This extends the scope of the NSN beyond the authorised purposes and beyond the student's own ability to use and disclose the NSN

- breach of the sector student IAM system provides access to multiple online services connected to the single logon for a student or students. Such a breach could result in malicious use of the logon or corruption of the content
- unauthorised use or disclosure of personal data (with or without the NSN), including logons, which is used for other purposes (eg, targeted advertising of potentially inappropriate services or content, or malicious activity)
- unnecessary collection and retention of personal data that increases the privacy risks in the event of unauthorised use or disclosure, or a security breach
- 'institutional creep' by agencies. This risk arises as agencies identity other uses for the data held in the IAM system without appropriate approval or notification.

52. The following controls have been identified, along with system security controls, to prevent and mitigate the privacy risks. The identified controls and the PIA will inform the system design process and implementation project.
    - Prescribing obligations for authorised users such as: privacy and security practices for third party service providers, data management practices, approval process for online service to connect to sector IAM systems using the NSN, including data required to authorise access to the online service.
    - Enhancing guidance on privacy and security for student data (including the NSN) for education providers to increase their awareness of obligations relating to student data and improve practices generally.
    - Using Privacy by Design guidelines to design and implement measures to address the identified privacy risks associated with system security.
    - Implementing a governance structure in the Ministry to provide oversight of the sector student IAM system and of compliance by other authorised users.

53. The existing provision in section 344(3) allows the Secretary for Education to set conditions on authorised users for specific authorised purposes. The conditions will cover matters that authorised users will be required to comply with to address privacy and security risks identified in the PIA.

Consultation

54. The Ministry has previously engaged with the school sector (representative organisations and 13 schools) in 2012[11] to develop high level business requirements for a sector identity and access management system following the approval of the managed network for learning business case. This included requirements for students. There was support for a sector approach to identity and access management.

55. The Department of Internal Affairs was consulted on the ability of RealMe to meet the education sector's IAM requirements. The outcome is summarised in the Options Analysis section.

56. The Office of the Privacy Commissioner (OPC) and the Government Chief Privacy Officer (GCPO) were consulted on the options to establish a verified and persistent student identity and associated logon.

57. A draft privacy impact assessment (PIA) was reviewed by the Office of the Privacy Commissioner (OPC) and the Government Chief Privacy Officer (GCPO). A key focus

11 This process followed Cabinet approval of the UltraFast Broadband in Schools business case to implement the managed network for learning. Identity and access management was identified as a core service in the business case.

of the PIA was to identify the privacy risks associated with implementing a sector student IAM system. Due to timing constraints the PIA was based on using the NSN to establish the verified student identity.

58. The OPC is, in principle, comfortable with the use of the NSN to create a single student identity, provided the detailed design process address the privacy risks associated with a single logon that provided access to multiple services. The GCPO is broadly supportive of the proposal, the moderate expansion of the NSN and the phased implementation approach. The GCPO supported the approach to sector student IAM as it is incremental and establishes a platform that other parts of the sector could build on as needed.

59. Both the OPC and GCPO identified that the privacy impact assessment needs to inform the design of the implementation, and further privacy assessments should be completed at each stage, along with ongoing monitoring of the risks identified. There will be ongoing consultation with the OPC and GCPO as implementation progresses.

60. Engagement with the wider sector will occur as part of the implementation project, along with specific consultation with schools and other key stakeholders to gather requirements to inform the first phase of implementation.

61. The Ministry will engage with DIA on wider identity management practices to inform system design and the development of business processes to support achieving the primary objectives.

Conclusions and recommendations

Conclusion on options to establish a verified student identity

62. Following the analysis of the options to establish the verified identity and the completion of the PIA the Ministry recommends Option A (NSN):
    - amend Part 30 to authorise the NSN to be used to verify and manage students' identities as the basis for a trusted logon (ie, username and password) for individual students to access online services.

63. The Ministry considers that the proposed use is consistent with the overall purpose for the NSN: *use by authorised users of the national student numbers for specific purposes, in order to facilitate the accurate use and transfer, by authorised users, of information relating to individual students*'.[12]

64. Use of the NSN for the proposed purpose would improve the integrity of the student identities by enabling authorised users to:
    - accurately establish and maintain a persistent, verified student identity
    - accurately retrieve additional data (eg, school, class, teacher) from sector and education providers' systems where this is required to authorise access to specific online services for individual students
    - efficiently provide the NSN to existing authorised users when required for existing authorised purposes as part of the access authorisation process.

65. The Ministry does not propose:

12 Section 341 of the Education Act 1989.

- adding any new users to the existing authorised users, as defined in s342 of the Act
- any changes, beyond the new purpose that is proposed, to the existing authorised purposes in s344 of the Act.

66. The primary risk associated with the recommended option is that the NSN in the IAM systems is used as a unique identifier for unauthorised purposes, along with the associated identity data. The Ministry considers that this risk will be managed through the controls that will be implemented through a sector approach to student IAM (eg, education and training for education providers, prescribed obligations on authorised users).

Conclusions on implementation of the proposed authorised purpose

67. The Ministry proposes a phased implementation of the proposed authorised purpose beginning with the development and implementation of the student sector IAM system in the school sector.

68. Existing provisions in section 344(3) of the Education Act 1989 (notification by Gazette) will be used to progressively approve authorised users and to set conditions on authorised users for the proposed authorised purpose.

69. The privacy risks for students identified through the privacy impact assessment will be managed through:
- prescribing obligations for authorised users and their third party service providers
- enhancing guidance on privacy and security for student data (including the NSN) for education providers to increase their awareness of obligations relating to student data and improve practices generally.
- using Privacy by Design guidelines to design and implement measures to address the identified privacy risks associated with system security,
- implementing a governance structure in the Ministry to provide oversight of the sector student IAM system and of compliance by other authorised users.

Implementation plan

70. The timeframe to develop and implement the sector student IAM system is outlined in the table below.

Date	Phases
May 2015 – June 2016	***Preparation*** Consultation with key stakeholder organisations on sector approach to student IAM Consultation with school sector representatives on business functional and process requirements to inform system design. Identity and implement responses to privacy risks identified in the Privacy Impact Assessment to inform system design and conditions for authorised users. Develop business processes (governance, approval, etc)

Date	Phases
	Develop communications material for implementation Establish evaluation criteria and process to monitor achievement of policy objectives Develop operational policy for sector student IAM system
	Build *(dependent on the passage of legislation)* Finalise requirements Build system
	Pilot Implement pilots in the school sector to provide access to selected online services Review pilots based on evaluation criteria Update operational policy based on pilots
July 2016 onwards	***Full implementation*** Identification and prioritising of online services and student cohorts in the school sector. Review implementation against evaluation criteria

Appendix 1: Overview of a sector approach to student identity and access management

1. A sector student IAM system supports current practice of providing digital channels for learner-centric education services. The sector system will complement education providers' IAM systems that provide their students with access to their own networks, systems and online services that are not connected to the sector student IAM system.

2. The online services approved to use the sector student IAM system will evolve over time and are likely to have one or more of the following characteristics:

    - requiring an appropriate level of trust and confidence in the identity to protect the service (eg, digital assessments)
    - sector-provided services that are used by all students during their enrolment in education (eg, access to record of achievement at NZQA, e-asTTle)
    - foundational services that are prevalent across the school sector (eg, Google Apps, Microsoft 365, e-portfolio services)
    - access is required by lifelong learners after their engagement in formal education is completed (eg, to personalised careers advice).

3. The initial implementation focus for the sector student IAM system is for students in the school sector as this is the sector with the potential for the greatest benefits for students and efficiency gains for the sector.

4. There will be overlaps with other parts of the education system. For example, identities and logons established for school students could support student progression into the tertiary sector or for adults who wish to re-enter education or access education services and need to access the approved services. Implementation in other parts of the education system will be determined in consultation with the sector stakeholders.

5. The expectation is that the majority of students will need to be in an identity and access management system as online learning increasingly becomes an integral part of students' education pathway for students, including home schooled students.[13] Some students may have religious beliefs or other constraints that do not allow use of computers. This requirement already exists and is being managed by the education providers. The sector system will need to accommodate these individual situations.

6. The core functions in a sector student IAM system are:

    - identity management: hold an authoritative identity record for each student, along with a username and password (the logon details) that enables access to specified services provided by identified organisations
    - access management: provide confirmation of entitlement or authority to access an online service (eg, student is of right age, in the right class, registered with the appropriate provider).

7. The core data for each of these functions is likely to be:

    - identity management: an authoritative identity including full names, date of birth, gender, NSN

13 Schools are responsible for communicating their teaching and learning programmes, including the use of digital technologies to their students and parents as part of the initial enrolment and ongoing participation at that school. This should include how access is being managed and cyber safety policies.

- access management: additional data for this function includes for the school sector, as an example, school, class, teacher.

8. The SSIAM will generate a system unique identifier for each student identity that is specific to the online service provider to which the student is seeking approval to access. Each online service provider will have a different system unique identifier for each student. This prevents unrelated online service providers from matching identities using a consistent and unique identifier and will preserve privacy.

9. The data required to authorise access to the online services connected to the SSIAM will be approved by a governance group. Education providers using the NSN for IAM services will also be required to have approval processes for connected online services.[14]

10. At this stage, the data required for IAM is expected to be held in the sector student IAM system.[15] The design is not finalised and input will be gathered from education providers and education agencies across the education system to confirm the requirements for the sector student IAM system.

11. The sector approach to IAM must recognise the distributed model for delivering IAM services in the sector and responsibilities of education providers (eg, for managing student data, determining which online services students will use, collaborative arrangements between education providers).

14 This will be implemented through conditions notified in the Gazette, as outlined in paragraph 43.

15 Students' educational, enrolment, attendance records will not be held in IAM systems. The Ministry proposes to set conditions through section 344(3) of the Education Act to ensure only data required for the proposed authorised purpose is held in the IAM systems

Appendix 2: Background information on the National Student Number (NSN)

Section 341 of the Education Act 1989 prescribes the purpose of the NSN: 341 '*Purpose of this part is to authorise the use by authorised users of national student numbers for specific purposes, in order to facilitate the accurate use and transfer, by authorised users, of information relating to individual students*'.

The National Student Index (NSI) manages the assignment of NSN via the enrolment processes by education providers. Data collected to assign an NSN includes: names, date of birth, gender, residential status. Only the Secretary of the Ministry of Education can assign a NSN.

Authorised users of the NSN are set out in section 342 Education Act:

- Education provider (early childhood services, registered schools, tertiary education organisations as defined in the Education Act)
- Ministry of Education
- NZ Qualifications Authority
- Tertiary Education Commission
- Careers NZ

Authorised purposes are set out in (section 344(2) Education Act) [16]:

- Monitoring and ensuring student enrolment and attendance
- Encouraging attendance at early childhood services
- Ensuring education providers and students receive appropriate resourcing
- Statistical purposes
- Research purposes
- Ensuring that students' educational records are accurately maintained.

By regulation under section 347 of the Education Act, the following authorised users have been added:

- Statistics NZ, for statistical and research purposes only
- Ministry of Social Development, StudyLink, for ensuring education providers and students receive appropriate resourcing.

The NSN can only be used by authorised users for specified authorised purposes after the Secretary has issues a notice in the NZ Gazette. Notices have not yet been issued for the following:

- Careers NZ: a NZ Gazette notice has not been issued approving it to use the NSN for any purpose
- Early childhood services: the 2013 NZ Gazette notice only approves the use of the NSN for monitoring enrolment and attendance and appropriate resourcing purposes.

16 These purposes were based on the Post-Compulsory Education Unique Identifier Code 2001

Appendix 3: Privacy impact analysis of the options to establish the persistent, verified student identity

IPP	Option A (NSN)	Option B (new Unique Identifier)	Option C (Data matching)
Information Privacy Principles	Amend Part 30 to allow the NSN to be used to verify, establish and maintain student identities.	Amend the Education Act to establish a new persistent unique identifier to verify, establish and maintain student identities.	Establish a central process/system to undertake data matching across multiple sector and education provider systems to verify, establish and maintain student identities.
Collection of personal information (IPP 1) Source of personal information (IPP 2) Collection of personal information from subject (IPP 3) Manner of collection of personal information (IPP 4)	The required personal information (including the NSN) will be sourced from the Ministry or education provider systems. The source of the information is from existing enrolment processes where education providers advise what the information collected is used for at the point of collection. No further information is being collected. The overall notification process of this option is the responsibility of the Ministry. The communications process must advise the new purpose, what data is collected, who holds the data (ie, online service providers), who will get access to it and other IPP3 requirements. Education providers using the NSN for their own or cluster IAM solutions must also communicate to students and parents/caregivers and cover the same information as the Ministry.	The required personal information will be sourced from education provider systems. The source of the information is from existing enrolment processes where education providers advise what the information collected is used for at the point of collection. No further information is being collected. Note: the NSN would not be collected with the other personal information. The Ministry will need to communicate the necessity of the new unique identifier, the authorised users and purposes and why it is necessary for the Ministry's functions.	The required personal information will be sourced from the Ministry systems. The source of the information is from existing enrolment processes where education providers advise what the information collected is used for at the point of collection. No further information is being collected. Note: the NSN would not be collected with the other personal information. The Ministry will need to communicate how the data being used for the data matching is being managed, including retention and who has access.
Storage and security	Under this option the NSN could be held in	The Ministry system that manages the new	The Ministry processes and system that

IPP	Option A (NSN)	Option B (new Unique Identifier)	Option C (Data matching)
of personal information (IPP 5)	multiple IAM systems, eg sector student IAM and those operated or contracted by education providers. This increases the risk that the NSN will be used for unauthorised purposes by unauthorised users. The IAM systems will need to meet acceptable security requirements to mitigate the risk of a breach. Authorised users (Ministry, education providers) will have to implement adequate controls to monitor and ensure security for IAM systems they manage. The NSI that manages the NSN is an existing system and no breaches have been identified.	unique identifier system will need to be kept separate from the NSN to mitigate unauthorised use of the NSN. The new unique identifier will be held in education providers' SMS to enable the ongoing maintenance of the student identity and to retrieve data required for access authorisation. The SMS also hold the NSN and this potentially enables education providers to link the new unique identifier with the NSN for unauthorised purposes. Education providers will need to ensure their IAM systems have appropriate security to protect the unique identifier and associated data. The Ministry system that assigns and manages the new unique identifier must meet GCIO mandated ICT requirements and Ministry IT requirements (ie, as applied to the National Student Index) to detect and prevent any security breaches.	extract the initial data and undertakes the ongoing data matching to establish the identity potentially creates a separate repository of identity data if managed outside the sector student IAM system. Multiple repositories of identity data increase the risk of a security breach. These systems and processes must meet GCIO mandated ICT requirements and Ministry IT requirements (ie, as applied to the National Student Index) to detect and prevent any security breaches.
Access to personal information (IPP 6) Correction of personal information (IPP 7)	The Ministry has existing processes that manage requests to access and correct information the NSN or information associated with the NSN. Education providers' existing processes to respond to requests for personal information	The Ministry's existing processes would be applied to a new system holding personal information. Education providers' existing processes to respond to requests for personal information would need to include IAM systems holding	The Ministry's existing processes would be applied to a new system holding personal information. This option does not create new data that must be managed by education providers and provided in response to a request.

IPP	Option A (NSN)	Option B (new Unique Identifier)	Option C (Data matching)
	would need to include IAM systems holding the NSN and any associated identity data. It is likely that there will be variability on how these processes are implemented.	the NSN and any associated identity data. It is likely that there will be variability on how these processes are implemented.	
Accuracy of personal information to be checked before use (IPP 8)	The NSN is an integral part of core education sector functions (enrolment, attendance, resourcing, maintaining the educational record) and education providers have a vested interest in maintaining its accuracy. Processes exist to identify and resolve exceptions. These are initiated by the Ministry and education providers. The integral nature of the NSN in education providers' systems ensures that retrieval of data required to authorise access is for the correct identity.	Providing that the population of the new unique identifier into education providers' SMSs is robust, the ongoing retrieval of data required to authorise access should ensure the data is for the correct identity. There is a risk that exceptions will be not identified as the new unique identifier will not be an integral part of the education providers' processes. New processes will be required to detect and resolve exceptions.	Data matching on multiple attributes increases the potential of errors occurring in maintaining the identity and retrieving the data required to authorise access. To mitigate this risk the sector student IAM system would need to generate an internal identifier that would be populated in the current education provider's SMS for each student at the point the identity was established. A new sector student IAM system-generated identifier would be required whenever the student changed schools to maintain the link and comply with IPP12. Using an internal system-generated identifier to maintain the link creates some risks as it relies on the accuracy of the data matching processes to identify the current education provider.
Retention (IPP 9) Personal information not to be kept for longer than necessary	The intention is that student identity established using the NSN would be persistent. The NSN is intended to be a persistent identifier. It is likely that many students will not use	The intention is that student identity established with a new unique identifier would be persistent. It is likely that many students will not use this identity once they leave the formal	The intention is that student identity established with a new unique identifier would be persistent. It is likely that many students will not use this identity once they leave the formal

IPP	Option A (NSN)	Option B (new Unique Identifier)	Option C (Data matching)
	this identity once they leave the formal education system (eg, after tertiary). Retaining inactive records creates risks of the data being used for purposes other than what it was collected for. It also increases the amount of data available if there is a security breach of the system holding the student identities.	education system (eg, after tertiary). Retaining inactive records creates risks of the data being used for purposes other than what it was collected for. It also increases the amount of data available if there is a security breach of the system holding the student identities.	education system (eg, after tertiary). Retaining inactive records creates risks of the data being used for purposes other than what it was collected for. It also increases the amount of data available if there is a security breach of the system holding the student identities.
Use (IPP 10) Limits on use of personal information	The inclusion of the NSN as a core attribute of the student identity in an IAM system increases the risk of unauthorised use by unauthorised and unauthorised users. There is a risk that the identity data held in the IAM systems is used for unrelated purposes. Authorised users (Ministry, education providers) will have to implement adequate controls to monitor and ensure compliance. The Ministry will need to establish controls to monitor compliance as the regulator of the NSN.	The new unique identifier will require a legislative mandate or an exemption to IPP12 through a privacy code. Both instruments will have to specific how the unique identifier can be used and who can use it. There is a risk of unauthorised use of the new unique identifier and associated identity data by approved and non-approved users. Approved users (eg, Ministry, education providers) will have to implement adequate controls to monitor and ensure compliance. The Ministry will need to establish controls to monitor compliance as the regulator of the new unique identifier.	The identity data used to establish the student identity, and the student identity itself, could be used for purposes other than those specified in the initial communications. The risk will only apply to the Ministry as this option does not provide education providers with any benefits over the status quo.
Disclosure (IPP 11) Limits on disclosure of personal information	The inclusion of the NSN as a core attribute of the student identity in an IAM system increases the risk of unauthorised disclosure by unauthorised and unauthorised users.	Once approved via legislation or a privacy code, there is a risk of unauthorised disclosure of the new unique identifier by approved and non-approved users. There is a risk that the associated identity	The identity data to establish the student identity could be disclosed for purposes other than those specified in the initial communications. The risk will only apply to the Ministry as this

IPP	Option A (NSN)	Option B (new Unique Identifier)	Option C (Data matching)
	There is a risk that the associated identity data held in the IAM systems is disclosed for unrelated purposes. Authorised users (Ministry, education providers) will have to implement adequate controls to monitor and ensure compliance. The Ministry will need to establish controls to monitor compliance as the regulator of the NSN.	data held in the IAM systems is disclosed for unrelated purposes. Approved users (eg, Ministry, education providers) will have to implement adequate controls to monitor and ensure compliance. The Ministry will need to establish controls to monitor compliance as the regulator of the new unique identifier.	option does not provide education providers with any benefits over the status quo.
Unique identifiers (IPP 12)	Provided that the use of the NSN for IAM purposes is mandated in the Education Act, it will be compliant with IPP 12.	The proposed unique identifier for this option would have to be mandated by legislation or via a privacy code to comply with IPP 12. The creation of another unique identifier for students, that is intended to be persistent and follow the student, risks creating confusion with the NSN.	This option does not create a unique identifier that is used by multiple agencies. An internal system-generated persistent identifier will be linked to each identity record. This identifier will only be used by the current education provider to maintain the link to the established student identity. If the student changes education providers, a new identifier is generated. This is similar to the RealMe approach.

Appendix 4: Criteria and scoring for assessment of options

The assessment covers the evaluation criteria for each option:

- Operational criteria
- Indicative fiscal costs
- Compliance impacts
- Privacy impacts

Operational evaluation criteria

5	fully supports the criteria
4	substantively supports; the differences do not affect the achievement of the criteria or have substantive adverse impacts on other criteria
3	generally supports the achievement of the criteria but there are areas of concern that create risks, or requires effort, for achieving the criteria and/or create risks for other criteria
2	ability to support the achievement of the criteria is substantively constrained and creates risks for achieving the criteria
1	none or limited support for achieving the criteria

Indicative cost of establishing and maintaining identity and enabling retrieval of attributes required to authorise access

5	< $1m
4	$1 – 2 m
3	$2 - 3 m
2	$3 – 4 m
1	$4 – 5 m

Compliance impacts on education providers

5	No impact
4	Low Impact
3	Medium impact
2	High impact
1	Substantial impact

Privacy impact analysis of options to establish, verify and maintain the identities

5	least privacy impacts / risk
4	has minor privacy impacts/risks that can be managed by existing processes
3	has moderate privacy impacts/risks that can be managed by existing processes
2	has moderate privacy impacts/risks that require new processes to manage
1	has substantial privacy risks that cannot be readily managed or are resource intensive to manage

Detailed privacy impact analysis rating for each option

(IPP – Information Privacy Principle in Privacy Act)

Criteria	Use the NSN	New Unique Identifier	Data matching
Collection IPPs 1-4	4	4	4
Storage & security IPP5	3	3	2
Access & correction IPP6 & 7	3	3	3
Accuracy IPP8	5	4	2
Retention IPP9	2	2	2
Use IPP10	2	2	2
Disclosure IPP11	3	2	2
Unique Identifiers IPP12	3	3	4
Median	**3**	**3**	**2**