Digital Identity for Online Learning (DI4OL)

PRIVACY IMPACT ASSESSMENT

Including use of the National Student Number (NSN)

Author: Alan Heward

Version: V1.0

Release Date: 12th September 2022

Table of Contents

Figures

Tables

Document Information

Revision History

Version	Date	Author	Description of Changes
1.0	August 2022	AH	Iterated to v1 for signing. v1 distributed to all named stakeholders.
1.0	September 2022	AH	Updated executive summary. Added Addendum 1.

Distribution List

Name	Role (Ministry of Education unless otherwise specified)	Date
Jonathan Shennan	Senior Manager ICT Strategy, DI4OL Business Owner	v0.4 2/05, v0.6 7/06, v0.7 21/07
Stuart Wakefield	Chief Digital Officer, DI4OL SRO	v0.4 2/05, v0.6 7/06, v0.7 21/07
Steve McDowall	DI4OL Project Manager	v0.3 7/04, v0.6 7/06, v0.7 14/07
Mike O'Connor	Enterprise Architect – Security	v0.3 7/04, v0.7 14/07
Tracey Morton	Manager Application Delivery and Digital Identity PO	v0.3 7/04, v0.6 7/06
Louise Hull	Policy Advisor	v0.7 14/07
9(2)(a)	Senior Privacy Advisor	v0.3 19/04 & v0.6 7/06, v0.7 14/07
Chris Stoddart	Senior Privacy Advisor	v0.7 23/08
9(2)(a)	Head of Health Safety Security & Privacy	v0.6 7/06, v0.7 14/07
Aaron McIntosh	Head of Health Safety Security & Privacy	V1.0 12/09
9(2)(a)	Manager Information Management	v0.3 19/04
Clare Ruru	Principal Information Management Analyst subsequently Manager Information Management	v0.5 18/05 & v0.6 7/06 v0.7 14/07
Alison Anderson	Principal Advisor Business Improvement	v0.3 19/04, v0.6 7/06, v0.7 14/07
Heidi van Wyk	Principal Advisor Information Management	v0.3 19/04
Catherine Gavigan-Binnie	Solicitor Legal services	v0.3 19/04, v0.6 7/06, v0.7 14/07
Andrea McDonald	Chief Data Steward	V0.4 17/05, v0.6 7/06, v0.7 21/07
Robyn Cargill	Chief Advisor Schooling Policy	v0.3 19/04 & v0.6 7/06
Maria Kirkland	Governance, Legislation and Accountability (GLA)	v0.3 19/04
Neville Bannister	Senior Manager ICT Assurance	v0.3 19/04, v0.6 7/06, v0.7 14/07
Mark Horgan	Principal Advisor to the CDO	v0.3 19/04
Kate Rickerby	Office of the Privacy Commissioner	v0.4 2/05, v0.6 7/06, v0.7 August
Katrine Evans	Office of the Government Chief Privacy Officer	v0.4 2/05, v0.6 7/06, v0.7 August
Prashant Bakshi	NZQA – Chief Customer Officer, Business owner and SRO	v0.3 19/04, v0.6 7/06, v0.7 August
Penny Roulston	NZQA – Privacy officer	v0.3 19/04 & v0.6 7/06
Andrew Wood	NZQA – Senior Advisor Information Security and Risk	v0.3 19/04 & v0.6 7/06
Hamsa Lilley	NZQA – Information Management	v0.4 2/05

References

Title	Date	Source and Link	Comment
PIA Using the NSN to establish verified digital identities	2015	Ministry internal 2015 NSN PIA	Aka 2015 NSN PIA
Crown Law advice	2015	Ministry internal	
Regulatory Impact Statement (RIS)	2015	Ministry internal	Establishing and managing verified student identities to support students' access to online services
MoE Information Security Controls catalogue	2021	Ministry internal	Derived from Secure Controls Framework (SCF) catalogue
Schools Records Retention / Disposal Information Pack	2022	Archiving and disposing of school records – Education in New Zealand	https://assets.education.govt.nz/public/Records/School-Records-Retention-and-Disposal-Schedule-All.pdf
NSN Notice 2019	2019	Education (National Student Numbers) Notice 2019 - 2019-go3573 - New Zealand Gazette	Planned to be replaced with an updated Gazette *NSN Notice 2022* to reflect 'online learning' purposes.
Education and Training Act 2020, Schedule 24 (ETA Sch 24)	2020	Education and Training Act 2020, Schedule 24 National student numbers	Where online learning is used to refer to the purpose within the ETA the words are encapsulated with a single apostrophe:

			'online learning'.
About the NSN	2021	National Student Number (NSN): for schools – Education in New Zealand	
Google assurance documentation	Vas	cloud.google.com/security/compliance/compliance-reports-manager & Privacy & Security Center | Google for Education	ISO Certifications, SOC2 reports, CSA questionnaires. Google for Education privacy policy.
Microsoft assurance documentation	Vas	docs.microsoft.com/en-us/compliance/regulatory/offering & Privacy and Security for Schools - Microsoft Education	ISO Certifications, SOC2 reports, CSA questionnaires. Microsoft for Education privacy overview links to Microsoft Trust Center
Azure IRAP	2021	Microsoft Azure IRAP Cyber.gov.au - IRAP	Aus IRAP issued August 2019, replaced with Aus CSP in 2021.
Azure GCDO	2021	Microsoft on NZ Security and Privacy Considerations	
MoE Digital Identity Strategy	2022	Ministry internal DI Strategy	Inc appendix of 135+ MoE DI initiatives
Digital Identity Strategy for NCEA Learners	2022	Ministry internal Identity strategy	
Te Poutāhū: Hybrid learning position paper	2022	Ministry internal Paper	Position on online learning terminology from Derek Wenmoth
DI4OL Introduction	2022	Ministry internal paper	Introduction to DI4OL, DI terminology and technology
DI4OL Project Initiation Document (PID)	2022	Ministry internal PID	Summarises and links to Cab papers, Business Case, Benefits, Scope statement.
DI4OL NSN Options analysis	2021	Ministry internal NSN Options Analysis	
DI4OL High Level Design	2022	Ministry internal HLD	
DI4OL Information Classification memo	2022	Ministry internal ICM	Approved by CDS.
DI4OL C&A memo	2022	Ministry internal C&A memo	Includes Security Risk Assessment of DI4OL
DI4OL Glossary of terms	2022	Ministry internal DI4OL - Definitions	Existing DI4OL Glossary is 10 pages in length and not repeated here.
ESL CA & Information Classification memo	2022	Ministry internal	Education Sector Logon C&A memo from January 2022
RealMe PIA	2020	DIA	PIA focussed on the re-platform work
GCDO IMS	2022	Identification Management Standards	
GCDO Digital Identity Trust Framework (DITF)	2022	DISTF Bill Identification Management Standards Draft Rules January 2022 (not public).	Now known as Digital Identity Services Trust Framework (DISTF) CAB-20-MIN 0324
Azure B2C IdP integrations	2021	IdPs supported by AzureB2C	
DPUP	vas	Data Protection and Use Policy	Reference links from Part 4 DPUP
Student privacy pledge	2020	Signatories 2.0 - Pledge to Parents and Students (studentprivacypledge.org)	Independent USA org campaigning to protect student privacy.
International Association of Privacy Professionals (IAPP)	Vas	Childrens_Privacy_Whitepaper	Various resources relating to Children's privacy
Common Sense	2021	common-sense-2021-state-of-kids-privacy	Manage a Privacy assessment framework focussed on children's apps & EduTech
UK Information Commissioners Office (ICO) Age appropriate design	2021	Age appropriate design: a code of practice for online services | ICO	
Island Bay School privacy policy	2022	Privacy Collection Statement	Exemplar of a detailed Privacy policy
OPC/GCPO feedback on DI4OL	2022	Documented feedback	
Privacy Concerns and Sharing Data survey	2018, 2020	Privacy-concerns-and-sharing-data-survey-Mar-Apr-2018.pptx Privacy-concerns-and-sharing-data-OPC-reportApr-20.pdf	NZ specific survey data on public attitudes and perceptions relating to privacy.
Sixth Periodic Report by the Government of New Zealand	2021	New Zealand (ohchr.org)	
UN Convention on the	1989	Convention on the Rights of the Child |	Convention on the Rights of the Child text |

Rights of the Child		UNICEF	UNICEF The Convention on the Rights of the Child: The children's version | UNICEF

Approvals

The following people endorse and acknowledge that the appropriate privacy risks and privacy enhancing controls have been identified:

Name and Position	Signature	Date
9(2)(a)	9(2)(a)	18/05/2022
Chris Stoddart Senior Privacy Advisor Health Safety Security and Privacy	Approval provided by email	12/09/2022
9(2)(a)	9(2)(a)	8/06/2022
Clare Ruru Manager, Information Management	Approval provided by email	24/8/2022

The following people endorse and acknowledge the identified risks and recommended privacy enhancing controls:

Name and Position	Signature	Date
Jonathan Shennan Senior Manager ICT Strategy, DI4OL Business Owner	Approval provided by email	25/08/2022
Tracey Morton Manager Application Delivery and Digital Identity product owner	Approval provided by email	18/05/2022 & 25/8/2022

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

Name and Position	Signature	Date
Stuart Wakefield Chief Digital Officer, DI4OL SRO	Approval provided by email	30/09/2022

Additional approvals/acknowledgements

Name and Position	Signature	Date
Neville Bannister Manager ICT Assurance	Approval provided by email	31/08/2022
Aaron McIntosh Head of Health, Safety and Security, Privacy	Approval provided by email	14/09/2022
Andrea McDonald Chief Data Steward	Approval provided by email	25/05/2022 & 8/09/2022

Executive Summary

The Ministry's Digital Identity for Online Learning (DI4OL) seeks to improve digital access for Learners. The DI4OL project was initiated from a proposal to the Covid Response Relief Fund (CRRF) to reduce the stress on students sitting online assessments. For an NZQA online exam to commence, all learners must be logged in to the NZQA assessment. In the heat of the moment of the exam, some students inevitably forget their NZQA-provided login names and/or password, creating additional stress. Further Background to the DI4OL project, and an introduction to Digital Identity terminology and concepts can be found in the *DI4OL Introduction* paper.

The first objective of DI4OL – as assessed in this Privacy Impact Assessment – is to enable NCEA Learners at secondary school to use their school-provided credentials to access NZQA's digital assessments. Additionally, school-provided credentials will also be able to be used to access the Learner's NZQA Record of Achievement.

The technical implementation to allow this will involve a Ministry hosted "Identify Broker" application. When a student initiates a login, the broker application will digitally receive and confirm the student's school login with the system in which that login information is held (i.e. Microsoft 365 for Education or Google for Education) and then communicate verification to NZQA systems to permit access. This transaction is secure and privacy respecting.

Once a student leaves school, they will be able to use a personal account (Apple, Google, Microsoft, or RealMe) to continue to login in the same manner. This overall approach is now quite common, with many online applications allowing authorisation through an existing third-party account login.

DI4OL has the ability to subsequently be extended to other learning applications in schools. While alluded to in this Privacy Impact Assessment, any such future extensions would be subject to further privacy assessments.

A key focus of the DI4OL solution is the planned use of the National Student Number (NSN) to help establish verified digital identities for the purpose of enabling students to access online learning and services. It has been agreed by the Ministry of Education (the Ministry) and NZQA that the 'online learning' purpose stipulated in the Education and Training Act 2020 (ETA) includes the 'assessment' of learning, and that the business process for 'submission' of Learners work for assessment is included within that.

The Ministry has defined online learning in the context of other commonly used terms, see the *Te Poutāhū: Hybrid learning position paper*, and this is used as a working definition through this PIA. In the wider education ecosystem and IT industry generally the term online learning is broadly used and has multiple different interpretations. This makes a useful legal definition for Gazetting purposes impractical and means that an ability to stipulate Conditions or Restrictions within the Gazette notice will be limited.

A gap current exists between the ETA and the *NSN notice 2019* where Schedule 24 of the ETA includes a seventh permitted use:

> **4 Use of NSN** (1) (c) (vii) 'establishing and maintaining student identities to support online learning'.

Although the use of the NSN by NZQA for maintaining education records is already covered by **4 Use of NSN** (1) (c) (vi) 'ensuring that student educational records are accurately maintained', the fact that the sub-clause **4 Use of NSN** (1) (c) (vii) relating to 'online learning' has not yet been authorised through a Gazette notice introduces a difference that may lead to ambiguity or misinterpretation and will be resolved through an updated Gazette notice.

The Ministry will enable Learner access to NZQA services using the Learners school login credentials via an Azure B2C based Federated Identity Broker, delivering seamless access across a small number of carefully selected Identity Providers (Google and Microsoft both represented as school and personal Identity Providers (IdPs), with Apple and RealMe as personal IdPs only). Learners will no longer need separate NZQA credentials. Learner access to other online learning resources from providers other than NZQA will then follow the anticipated uptake of the DI4OL identity broker by schools. The existing National Student Number (NSN) will be used as the unique identifier across systems where there is a clear and approved business justification for this. While the ETA authorises the use of the NSN by specified users for specified purposes, that does not necessarily mean that the NSN should always be used simply because it is authorised. A Condition will be specified in the Gazette notice requiring schools to seek approval from the Ministry before using the NSN for 'online learning' purposes, unless an identity provider is on a published approved list. The default for DI4OL will be that the NSN is not shared and a pseudonymous identifier unique for each digital service provider application will be used.

The changes for Learners will be minimal from a privacy perspective and will indeed enhance privacy protections. The process for enrolment within school will remain the same, as will the information collected, the purpose for collecting, the use of that information by schools, and that it is shared with the Ministry. The change will be that a minimal and necessary sub-set of the information already shared by schools with the Ministry will be used for the Learners benefit in providing the DI4OL identity broker service. The DI4OL identity broker itself will be transparent to Learners and while there will be a slightly different user experience, this again will be an enhancement to the Learners existing experience.

A full change and communications plan is being developed to ensure that all stakeholders including school Board of Trustees, school principals, teachers, Learners themselves, parents & whanau, are informed about the DI4OL identity broker and the anticipated benefits for Learners as a result of schools opting-in. Consistent with the Ministry's School Leaders Bulletin, template communications will be included that schools can use with their Learners, parents and the local community as appropriate. Awareness raising communications will also be conducted with peak bodies such as NZ School Trustees Association (NZSTA), Secondary Principal's Associations, through the Education Gazette and School Leaders Bulletin.

During the pilot the Ministry will review school Privacy statements and provide guidance on whether the existing school Privacy statements or policies may need updating to reflect the additional purpose for which schools are opting-in to share information with the Ministry. Ultimately this will be a decision for the schools to make, consistent with the level of detail they provide to Learners and Parents.

Feedback will be sought from Learners, Teachers and other stakeholders during the pilot as to whether DI4OL adds value, achieves the expected benefits, or raises any concerns

We expect that a DI4OL page will be established on the Ministry's main education.govt.nz website, similar to other application and software pages, which will provide specific guidance to schools and other parties about DI4OL.

The DI4OL project completed a Privacy Threshold Assessment (PTA) to determine the level of privacy risk associated with the technology Proof of Concept (PoC), piloting with schools, and intended production use. Risks associated with collection and storage of information were assessed as low at the PTA stage. This was reviewed as the scope of the PoC and pilot evolved. Due to the number of records involved for production deployment, hosting within Australia, and the exchange of information across the education sector, the PTA indicated that a Privacy Impact Assessment (PIA) was required. A PIA was also seen as crucial to support the expected Gazette notice relating to the use of the National Student Number (NSN) for 'online learning' purposes.

A total of nine (9) privacy risks were identified through the PIA analysis. With only one (1) being Moderate against the Ministry's risk framework. This risk relates to schools having ineffective or insufficient information security controls, and beyond the impact to a school and it's Learners the potential for reputational impact to the Ministry. The other eight (8) risks are rated as Low, with effective mitigations included in the design and implementation of the DI4OL identity broker. The overall assessment of the risk level is consistent with the Ministry's aversion to risk for Information Security and specifically the protection of Privacy and Confidentiality.

Following the MoE Digital Identity strategy, the DI4OL project team have incorporated privacy by design principles into the design at all phases and have closely aligned with the DIA Digital Identity Services Trust Framework (DISTF) Identification Management Standards and draft Rules to ensure compliance with anticipated future Government expectations. This approach ensured that privacy risks were identified early enabling privacy enhancing mitigations to be designed into the overall project and solution delivery.

Introduction

This report presents the findings of the Privacy Impact Assessment (PIA) of the Digital Identity for Online Learning (DI4OL) identity broker solution. As articulated in the objective for DI4OL, the scope of this PIA is NCEA aged Learners accessing NZQA applications.

This PIA identifies and assesses the privacy risks associated with the collection, processing, use, disclosure, and storage of personal information (including the NSN) for use by the Azure Business to Consumer (B2C) based DI4OL identity broker that is being implemented. Planned integrations with specific digital service provider[1] applications including NZQA, Google, Microsoft, DIA (RealMe), and Apple are considered. The DI4OL identity broker service will be an opt-in service for schools, initially to allow Learners to access the NCEA digital assessment and Record of Achievement (RoA) portals provided by NZQA. In the future additional Learner applications will be available from other digital service providers that are commonly used across the education sector. Additional education providers are anticipated to opt-in to the DI4OL identity broker, such as tertiary education providers. These future use cases are referenced at a high level, actual implementation will require further Privacy and risk review.

The findings and recommended privacy enhancing controls in this report are not a legal opinion.

Note that the DI4OL identity broker is distinct from other existing services, most specifically the Education Sector Logon (ESL), that the Ministry operates which also use Azure B2C services from Microsoft. This PIA does not consider the ESL use case to avoid the confusion referring to both would cause. The ESL service is used by the education sector workforce (i.e., teachers, staff, some third-party providers). The main difference between the DI4OL identity broker and ESL is that the ESL maintains its own identity store of users for authentication and authorisation purposes. The DI4OL identity broker facilitates the exchange of information that supports authentication and authorisation but does not itself perform authentication and authorisation of Learners. Key ESL enabled services and an elaboration of the ESL can be found in the ESL Certification & Accreditation (C&A) memo and ESL website here.

A full glossary of digital identity terms and DI4OL project terminology is available in the DI4OL Glossary.

Methodology

This Privacy Impact Assessment (PIA) has been completed following the guidance produced by the Office of the Privacy Commissioner for completing Privacy Impact Assessments[2]. This PIA is an input to the System Certification and Accreditation/ATO process. This PIA has been completed by the Ministry of Education and substantially updates the previous PIA for *Using the National Student Number to establish verified digital identities* from July 2015, hereafter referred to as the '2015 NSN PIA'. In particular the IPP analysis and risk assessment from the 2015 NSN PIA has been reviewed in detail to ensure that the previous recommendations are reflected in the current DI4OL identity broker design. The conclusion is that almost all the 2015 NSN PIA proposed Privacy responses and recommended controls are being implemented as part of the DI4OL solution. See Appendix 5 2015 NSN PIA Risks, Privacy Responses, and Recommended Controls for a full comparative analysis.

Given key similarities between DIA's RealMe service and the DI4OL identity broker, the RealMe PIA has been reviewed in detail. Including comparison of recommendations (controls).

The Ministry has adopted and is in the process of implementing the Data Protection and Use Policy (DPUP) developed by the Social Investment agency[3]. The principles of the DPUP have also been considered in this assessment where appropriate. The Security Classification and the impacts to privacy of that classification have also been considered.

This PIA has been completed within the DI4OL project team. Advice and guidance have been provided by Privacy, EDK Information Management and Data Stewardship teams. Advice has also been provided by external stakeholders including the Office of the Privacy Commissioner (OPC) and the Government Chief Privacy Officer (GCPO). This assessment has been completed on the most current documentation available.

Legal Context

The Ministry must comply with the Privacy Act 2020 (the Act) when collecting, using, storing, and disclosing personal information. The Act protects information about individuals and applies to every agency (public and private) that

[1] Digital service provider is used here to represent the group of IT services, whether Identity Providers or Application Providers, working in an education context.
[2] Refer to the OPC's PIA Handbook for more information - www.privacy.org.nz/news-and-publications/guidance-resources/PIA handbook/
[3] Now referred to as the Social Wellbeing Agency

deals with 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.

The Ministry must also operate in accordance with the Education and Training Act 2020 (ETA), and the Public Records Act 2005.

Under the Privacy Act schools are accountable for PI that they collect and use. Digital service providers that schools consume services from are responsible for the information entrusted to them and in the case of a Privacy breach those digital service providers would be responsible for remediating and notifying said breach. While the school would also be accountable for ensuring the same breach was notified to OPC, Learners, their parents and other effected individuals. The Ministry as steward of the education sector may be considered accountable by some stakeholders. Where the Ministry is also a service provider to schools, with multiple different Ministry systems used by schools today and in the future including the DI4OL identity broker service, shared responsibility similarly applies. The Ministry, and its service providers where applicable, would be responsible for any privacy breach of Ministry systems including the DI4OL identity broker, with obligations to notify OPC and schools.

The DI4OL identity broker solution may also need to align with, or fully Accredit against, the future Digital Identity Services Trust Framework. As of April 2022 this has progressed to a second reading, following the Select Committee's report. Depending upon the continued progress of the Bill and DI4OL pilot, further updates to this PIA may be required before a production deployment.

Summary of findings

Summary of Privacy Risks

A total of nine (9) privacy risks were identified through the PIA analysis. The overall assessment of the risk level is consistent with the Ministry's aversion to risk for Information Security and specifically the protection of Privacy and Confidentiality. The privacy risks identified are shown below. There is no overall change in the level of risk as the controls recommended from the PIA are being included as part of the design and implementation.

For the risk that remains rated as Moderate **P-03,** the unchanged overall risk level is driven by an unchanged impact with the potential extent of unintended disclosure and need for reporting of a privacy breach to OPC. Along with an unchanged likelihood given there are ~2,500 schools with the risk applicable to any school.

Table 1 Summary of Privacy risks

Current Risk Rating	Risk Description	Residual Risk Rating after controls
Moderate	**P-03** There is an existing business risk that Schools have ineffective or insufficient safeguards implemented to ensure the security of PI stored within School IT systems, third party IT systems that Schools use and configure.	Moderate
Moderate	**P-09** Schools may not be transparent with Learners or their parents on the detail of the purpose for collecting information, or the detail of what information is shared with the Ministry for specific purposes. An individual feels that their Privacy rights have been infringed.	Low
Moderate	**P-01** Excessive items of PI are collected for no clear purpose, or without the knowledge of the individual.	Low
Low	**P-04** There is an existing risk that individual may have ineffective or insufficient safeguards implemented on their Personal credentials, to ensure the security of their Personal IdP, or any information they store in the account.	Low
Low	**P-07** An individual can be identified from a number of aggregated or anonymised data sets, or through the NSN unique identifier.	Low
Low	**P-06** Personal information is used or disclosed by education providers, or their authorised IdP or digital service providers, outside of the specified legal purpose for which it was collected. Specifically, the NSN is used by non-specified users or for non-specified purposes.	Low

Low	**P-05** Personal information is used or disclosed by the DI4OL identity broker outside of the specified legal purpose for which it was collected. Specifically, the NSN is used by non-specified users or for non-specified purposes.	Low
Low	**P-02** The DI4OL solution does not implement effective or sufficient safeguards to ensure the security of PI stored within the DI4OL identity broker.	Low
Low	**P-08** Schools may not be transparent with Learners or their parents about the purpose for collecting and sharing the information with the Ministry for DI4OL. Resulting in a Privacy complaint being raised against the Ministry.	Very Low

Summary of Privacy Enhancing Controls

A total of fifteen (15) privacy enhancing controls were identified and are recommended to reduce either the likelihood or the impact of the Privacy risks identified. Control Catalogue references are drawn from the Ministry's information security controls catalogue.

Table 2 Privacy enhancing controls

Control Reference	Control Description	Linked Risks	Relevant IPP
DCH-03.1	Sharing a pseudonymous identifier unique to each application, thus not sharing the NSN, prevents the NSN from being used as an authoritative unique identifier across applications, vendors, or longitudinally over time.	P-02	IPP5, IPP13
GOV-01	Compliance requirements – Ministry information security and Privacy requirements and recommendations to be articulated to other parties, to be embedded in contracts if possible (**SR02** SLAs and Contracts).	P-01, P-03, P-06, P-07	IPP1, IPP5, IPP10, IPP11, IPP13
HRS-03	Advice and guidance is provided to School Board, Teachers, staff, as to their responsibilities for Privacy and Security of school information and systems.	P-01, P-03, P-06, P-08, P-09	IPP1, IPP3, IPP10, IPP11
IAC-08	Role Based Access Control – Ministry access to the DI4OL identity broker will be limited to privileged administrators only. Other than Learners, there will be no standard user access.	P-02, P-05	IPP5, IPP10, IPP11
IAC-15	User Account Lifecycle Management – Identity idle accounts, disable them, and define re-authorisation process	P-01, P-02, P-03	IPP1, IPP5
IRO-09	Communications plan - A full change and communications plan is being developed to ensure that all stakeholders are informed about the DI4OL identity broker. Awareness raising communications will also be conducted with peak bodies.	P-01, P-03, P-06	IPP1, IPP5, IPP10, IPP11
PRI-01, PRI-02	Policies for information security and Privacy Policy – Existing Ministry and NZQA information security and privacy policies, practices, processes, education and awareness training, applicable for all staff involved in the design, operation, and management of the end-to-end service.	All risks	IPP1, IPP5, IPP10, IPP11, IPP13
PRI-01, PRI-02	Schools have existing Privacy policies; these may need updating in line with the new 'online learning' purpose.	P-01	IPP1
PRI-01.5	Legal obligations, identified in ETA Sch 24 NSN relating to specified users and specified purposes for using the NSN are a key control. Offences relating to use of the NSN are specified in the ETA §661.	All risks	IPP1, IPP5, IPP10, IPP11, IPP13
PRI-01.6	Privacy by design inc. data minimisation, evidence checked rather than evidence retained.	All risks	IPP1, IPP5, IPP10, IPP11, IPP13
PRI-04	Collection of PI from older children is for identified purposes	P-08	IPP3
PRI-05	Retention requirements – agree an approach to retaining PI in a 'lifelong learning' context.	P-01, P-02, P-05, P-06	IPP1, IPP5, IPP10, IPP11
PRI-06	Personal information permission – the Learner has access to review and update directly the information stored about them in the DI4OL identity broker linking portal.	P-01	IPP1

PRM-01	Within the Ministry's overall digital strategy are several initiatives to help schools under the Strengthening Cyber Security and Digital Support for Kura & Schools programme, including Te Mana Tūhono, Cyber security for schools, Network for Learning (N4L), Safer Technology for Schools (ST4S).	All risks	IPP1, IPP5, IPP10, IPP11, IPP13
SAT-02	Security awareness training – MoE Strengthening Cyber Security and Digital Support for Kura & Schools programme has a specific workstream for awareness raising within the education sector.	P-03, P-06	IPP5, IPP10, IPP11
SAT-02	There is extensive engagement in the education sector from NZ organisations such as Netsafe, NZ Police, OPC, CERT NZ on basic cyber security and privacy awareness applicable to children. This is in addition to similar engagement from international organisations such as Apple, Facebook, Google, Microsoft etc.	P-03	n/a

Summary of Impact Assessment Controls

A further seventeen (17) controls are recommended to reduce the likelihood or impact of Privacy risks identified. Although these do not directly improve privacy:

Table 3 Additional security controls

Control Reference	Control Description	Linked Risks	Relevant IPP
CHG-01	Change control – Change control, approvals processes, pre-deployment testing as per normal Ministry processes will be implemented to minimise inadvertent misconfiguration.	P-05	IPP10, IPP11,
CHG-02	Configuration management – integral with change control will be technical configurations implemented to prevent sharing of PI or the NSN except where configured, tested and approved.	P-02, P-05, P-06, P-07	IPP5, IPP10, IPP11, IPP13
CPL-01	Due Diligence - Ministry expectations for Assurance reporting to be articulated and a framework established to enable reporting. Including RACI matrix to clarify shared responsibility obligations.	P-01, P-03, P-06	IPP1, IPP5, IPP10, IPP11
CPL-01	Due Diligence – The Ministry will perform Assurance reviews of Google and Microsoft as school IdP vendors to ensure they meet Ministry expectations.	P-03, P-04	IPP5
CRY-03	Transport Layer Security – all data is encrypted in transit between the DI4OL identity broker and external connections, and within the DI4OL identity broker service itself.	P-02	IPP5
CRY-05.1	Storage data security – all information and data is encrypted at rest and in storage.	P-02	IPP5
GOV-01	Identify compliance requirements – inc. Certification and Accreditation (C&A) of the DI4OL identity broker solution and end to end service.	All risks	IPP1, IPP5, IPP10, IPP11, IPP13
GOV-02 & PRI-07	DI4OL reduces system wide risk by implementing a consistent standards-based approach to disclosing PI to digital service providers.	All risks	IPP1, IPP5, IPP10, IPP11, IPP13
GOV-03	Information security reviews - Perform a risk assessment, particularly in concert with major changes of scope, solution capability etc.	All risks	IPP1, IPP5, IPP10, IPP11, IPP13
GOV-03	Information security reviews – NZQA will undertake an independent review of DI4OL C&A artefacts to ensure that they meet NZQA's requirements. Part of this NZQA review may include a review by an independent security consultancy.	All risks	IPP1, IPP5, IPP10, IPP11, IPP13
GOV-03	Information security reviews - The project will engage an independent auditor to perform Technical Quality Assurance (TQA) and project IQA.	All risks	IPP1, IPP5, IPP10, IPP11, IPP13
IAC-06	Multi Factor Authentication (MFA) – All Ministry administrative users will be required to use MFA	P-02, P-03	IPP5
IAO-05	Digital service providers will be reviewed against criteria (specifics of which are TBD), before being permitted to connect to the DI4OL identity broker	P-01	IPP1

IAO-05 & PRI-14	Operational Assurance Plan. Along with the assurance requirements identified of school and personal IdPs, digital service providers, the Ministry will agree a formal assurance plan covering the end-to-end DI4OL identity broker service.	All risks	IPP1, IPP5, IPP10, IPP11, IPP13
IRO-04	Incident response plan – Ministry incident response plans cater for information security and privacy incidents, including escalation, communications, notification to effected parties.	All risks	IPP1, IPP5, IPP10, IPP11, IPP13
MON-02	Logging and Auditing – the DI4OL identity broker will implement full logging of all system and user events. These logs will be fed in to monitoring and alerting tools.	P-02	IPP5
MON-02.3	System monitoring and alerting – the identity broker will be monitored, and alerts generated using existing Ministry tools.	P-02, P-05	IPP5, IPP10, IPP11,
MON-02.3	Security Incident and Event Management (SIEM) – in addition to creation of anomaly reporting criteria within the Ministry SIEM solution, operational and business reporting will be defined.	P-02, P-04, P-05	IPP5, IPP10, IPP11,
OPS-03	Service Management RACI & SoPs to be established	P-02, P-05, P-06, P-07	IPP5, IPP10, IPP11, IPP13
VPM-07	Security testing – Perform security testing, remediate findings to an acceptable risk level.	All risks	IPP1, IPP5, IPP10, IPP11, IPP13

Consultation and Agreed Privacy Enhancing Controls

After consultation with Jonathan Shennan and Stuart Wakefield the following recommended privacy enhancing controls will be implemented:

Control Reference	Control Description	Linked Risks	Relevant IPP	Actions
All 32 controls	As above	As above	As above	Controls to be implemented as applicable for pilot and production deployments. Jonathan Shennan Accountable, Tracey Morton & Steve McDowall Responsible.

Assessment Part 1 – Project/System Information

Key Stakeholders

Business Owner (Risk)	Stuart Wakefield, Chief Digital Officer
Project Owner (System)	Jonathan Shennan, Senior Manager ICT Strategy, Planning and Architecture
Other Stakeholders and Service Providers	NZQA, Schools with NCEA candidates, OPC, GCPO, other Education providers (in the future). Unify, Google, Microsoft, Apple, DIA.

Project Overview

This Privacy Impact Assessment (PIA) considers the Digital Identity for Online Learning (DI4OL) identity broker solution being implemented by the DI4OL project and using the National Student Number (NSN) as part of 'online learning' including 'assessment' and 'submission' business functions. During late 2021 and early 2022 the project undertook work on a technology proof of concept and during 2022 is progressing to an initial pilot phase with two schools, and potentially a second pilot phase with up to twenty schools included. Subject to pilot success, and timing agreement with NZQA considering exam season, full production deployment of the DI4OL identity broker solution to schools across NZ is expected to commence in 2023.

The initial objective for the Ministry's Digital Identity for Online Learning (DI4OL) service is to improve digital access for secondary school Learners by enabling NCEA Learners to use their school provided credentials to access cloud applications – specifically NZQA's digital assessments and Record of Achievement (RoA). This includes the submission of coursework for subsequent assessment that supports lifelong learning in the education system. Future extension to other online services that support lifelong learning may include websites, web applications, mobile applications.

The DI4OL identity broker solution is based on learners authenticating using their school issued usernames and passwords whilst enrolled at school and migrating to using personal Identity Providers (IdPs) when they leave school. Learners will no longer need a separate NZQA credential which is infrequently used.

For learners that move schools the NSN will enable them to continue to access NZQA services even though they now have a different username and password at a new school. For learners that have left school they will be asked to link a personal IdP to their DI4OL identity broker profile, enabling them to use this to authenticate after they no longer have a school issued credential. Initial options for this personal IdP are expected to include Gmail from Google, iCloud from Apple (as Apple allow federation this Apple ID may be linked to another provider such as Xtra), Outlook.com (and potentially 'onmicrosoft.com' associated with Office365 subscriptions) from Microsoft, and RealMe from DIA. Noting that RealMe does not provide an email address. Additional options are expected to become available as the NZ Digital Identity Services Trust Framework is established and third-party providers join the digital identity ecosystem. In either case the administrative effort and burden of updating the Learners specific NZQA credentials will be removed. In the future Learners entering Tertiary education may also link their Tertiary institution credentials with the DI4OL identity broker.

A full change and communications plan is being developed to ensure that all stakeholders including school Board of Trustees, school principals, teachers, Learners themselves, parents & whanau, are informed about the DI4OL identity broker and the anticipated benefits for Learners as a result of schools opting-in. Consistent with the Ministry's School Leaders Bulletin, template communications will be included that schools can use with their Learners, parents and the local community as appropriate.   Awareness raising communications will also be conducted with peak bodies such as NZ School Trustees Association (NZSTA), Secondary Principal's Associations, through the Education Gazette and School Leaders Bulletin. Feedback will be sought from Learners, Teachers and other stakeholders during the pilot as to whether DI4OL adds value, achieves the expected benefits, or raises any concerns.

Similar to existing pages on the Ministry's main website (ESL has Catalogue of tools & online services | Applications & Online Systems (education.govt.nz), ICT & Digital services for schools Digital technology – Education in New Zealand), we expect the DI4OL will have a webpage providing information consistent with the communications material provided to schools and other stakeholders. This will link to NZQA, the Ministry's existing NSN & NSI pages and other associated sites.

Project Scope, objectives, issues, deliverables

The scope of this PIA is the DI4OL service being established within the Ministry's Australian Azure B2C tenancy. Along with integrations to school identity providers (Google Workspace for Education and Microsoft Office365 for Education), the NZQA Assessment Master and Record of Achievement (RoA) systems, and personal identity providers from Apple, Google, Microsoft and RealMe (DIA). The PIA is focussed on the near term pilots with schools and anticipated production adoption during 2023. Subsequent to the pilots, this PIA may be updated with any additional privacy related risks or controls that are recommended as part of the production adoption. For clarity, this PIA does not address any anticipated future changes for DI4OL as listed on the following page; any such changes would require further privacy assessment prior to implementation.

A more detailed description of the DI4OL project's alignment with the Ministry's Digital Identity Strategy, existing pain points, issues to fix and the expected benefits can be found in the *MoE Digital Identity Strategy*, the *Digital Identity Strategy for NCEA Learners* and the Project Initiation Document (PID). The following project overview is taken from the PID.

> "*The Ministry provides a digital identity service for the teaching workforce through the Education Sector Logon (ESL)*[4] *but kura and schools provide and manage their own digital identity services. Existing digital identity services, including the ESL, are no longer fit for purpose ... There are multiple manual digital identity processes, services and profiles in the education system delivered in a disconnected way and applied with variable capability. It is not cost effective to upgrade ESL.*
>
> *The Ministry's Digital Identity Strategy has determined that there is an opportunity to design and implement a "green-fields" sector-wide identity service which is inclusive of a much wider range of user cohorts and sector on-line services. It has a service vision to "Enhance and streamline online experiences and interactions by ensuring the delivery of a secure and trusted digital identity for authentication and authorisation".*[5]
>
> *It is important to distinguish between the Ministry's Digital Identity Strategy, and the Digital Identity for Online Learning (DI4OL) project... DI4OL will establish the foundations for future DI work but will not complete all the planned integrations and migration off ESL which appear as aspirations in other strategy documents.*
>
> *As a first step of implementing the necessary DI foundations and under the COVID 19 funding package, the Minister approved the release of $22.7m in Budget 2020 to deliver digital identity services to senior secondary learners through a Digital Identity for Online Learning (DI4OL) project. The DI4OL project primarily aims to achieve the following two outcomes:*
>
> - Ensure secondary school students can sit NCEA online exams securely.
> - Ensure a student can access their academic record securely (additional scope added by MoE[6]).
>
> *The DI4OL project objectives are to improve trust and confidence that only legitimate users are accessing education digital services and enable easier access to those services whilst reducing the risk of privacy breaches. The project also aims to reduce the time and cost of access to multiple digital identity services and enable changes to be made to digital identity services more easily.*
>
> *The project will address the following critical issues (refer to the Problem Statements*[7]*):*
>
> - *Student stress around exam time due to confusion around which logon credential are required to sit an exam online.*
> - *High levels of administration that schools need to do to manage logons (and resolve logon issues) for sitting online exams.*
> - *Greater continuity of access to education digital services when moving or leaving school.*
>
> *These issues result in:*
>
> - *poor user experience, such as significant time and effort for users to secure access*
> - *high costs to operate digital identity services*
> - *increased risk of privacy breaches*
> - *inflexibility when needing to implement policy changes*
> - *loss of confidence by users.*

[4] The Ministry provided identity management, authentication, and authorisation solutions, providing a secure and seamless link to Education Sector Applications used by the education workforce (teachers, staff etc.).

[5] Refer Current Services Discovery Pack

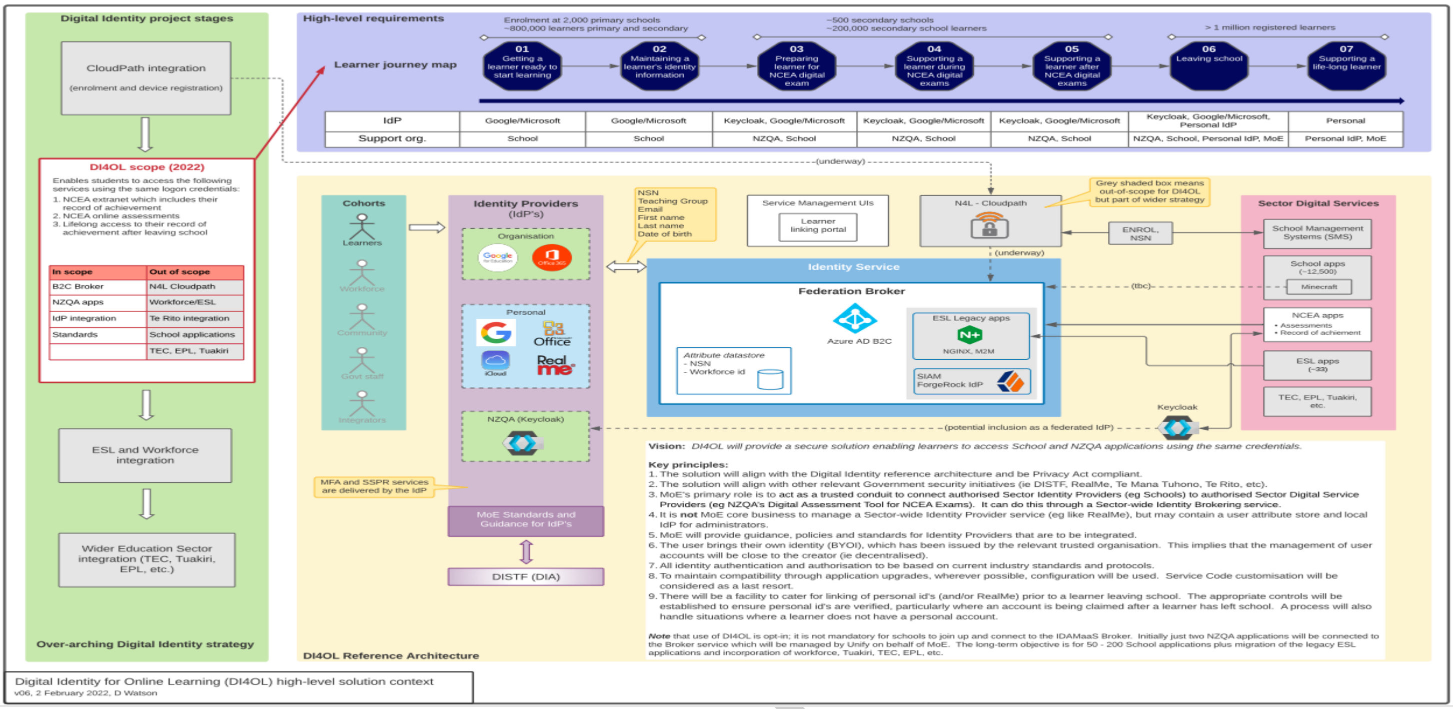
[6] Refer to the approved DI4OL Scope Statement

[7] DI4OL Problem Statement

Key deliverables of the project are:

- *Foundational platform (supporting wide range of digital identity functionality).*
- *Identity Provider integration, Digital identity services and relying party integration.*
- *Digital identity services' processes aligned to the use cases delivered.*
- *Standards, rules, and guidelines for operationalising the digital identity service(s)."*

A high-level business context diagram is in Figure 1 below and repeated in Appendix 4 in a larger size.


Digital Identity project stages
CloudPath integration
(enrolment and device registration)
DI4OL scope (2022)
ESL and Workforce integration
Wider Education Sector integration (TEC, Tuakiri, EPL, etc.)
Over-arching Digital Identity strategy
High-level requirements
Learner journey map
Enrolment at 2,000 primary schools
~800,000 learners primary and secondary
~500 secondary schools
~200,000 secondary school learners
> 1 million registered learners
01 Getting a learner ready to start learning
02 Maintaining a learner's identity information
03 Preparing learner for NCEA digital exam
04 Supporting a learner during NCEA digital exams
05 Supporting a learner after NCEA digital exams
06 Leaving school
07 Supporting a life-long learner
(underway)
Cohorts
Learners
Workforce
Community
Govt staff
Integrators
Identity Providers (IdP's)
Organisation
Google for Education
Office 365
Personal
Office
iCloud
Real me
NZQA (Keycloak)
MFA and SSPR services are delivered by the IdP
MoE Standards and Guidance for IdP's
DISTF (DIA)
NSN
Teaching Group
Email
First name
Last name
Date of birth
Service Management UIs
Learner linking portal
N4L - Cloudpath
Grey shaded box means out-of-scope for DI4OL but part of wider strategy
ENROL, NSN
(underway)
Identity Service
Federation Broker
Azure AD B2C
Attribute datastore
- NSN
- Workforce id
ESL Legacy apps
NGINX, M2M
SIAM ForgeRock IdP
(tbc)
Keycloak
(potential inclusion as a federated IdP)
Sector Digital Services
School Management Systems (SMS)
School apps (~12,500)
Minecraft
NCEA apps
• Assessments
• Record of achiement
ESL apps (~33)
TEC, EPL, Tuakiri, etc.
DI4OL Reference Architecture

Enables students to access the following services using the same logon credentials:
1. NCEA extranet which includes their record of achievement
2. NCEA online assessments
3. Lifelong access to their record of achievement after leaving school

In scope	Out of scope
B2C Broker	N4L Cloudpath
NZQA apps	Workforce/ESL
IdP integration	Te Rito integration
Standards	School applications
	TEC, EPL, Tuakiri

	01	02	03	04	05	06	07
IdP	Google/Microsoft	Google/Microsoft	Keycloak, Google/Microsoft	Keycloak, Google/Microsoft	Keycloak, Google/Microsoft	Keycloak, Google/Microsoft, Personal IdP	Personal
Support org.	School	School	NZQA, School	NZQA, School	NZQA, School	NZQA, School, Personal IdP, MoE	Personal IdP, MoE

Vision: *DI4OL will provide a secure solution enabling learners to access School and NZQA applications using the same credentials.*

Key principles:
1. The solution will align with the Digital Identity reference architecture and be Privacy Act compliant.
2. The solution will align with other relevant Government security initiatives (ie DISTF, RealMe, Te Mana Tuhono, Te Rito, etc).
3. MoE's primary role is to **act as a trusted conduit to connect authorised Sector Identity Providers (eg Schools) to authorised Sector Digital Service Providers (eg NZQA's Digital Assessment Tool for NCEA Exams). It can do this through a Sector-wide Identity Brokering service.**
4. It is **not** MoE core business to manage a Sector-wide Identity Provider service (eg like RealMe), but may contain a user attribute store and local IdP for administrators.
5. MoE will provide guidance, policies and standards for Identity Providers that are to be integrated.
6. The user brings their own identity (BYOI), which has been issued by the relevant trusted organisation. This implies that the management of user accounts will be close to the creator (ie decentralised).
7. All identity authentication and authorisation to be based on current industry standards and protocols.
8. To maintain compatibility through application upgrades, wherever possible, configuration will be used. Service Code customisation will be considered as a last resort.
9. There will be a facility to cater for linking of personal id's (and/or RealMe) prior to a learner leaving school. The appropriate controls will be established to ensure personal id's are verified, particularly where an account is being claimed after a learner has left school. A process will also handle situations where a learner does not have a personal account.

Note that use of DI4OL is opt-in; it is not mandatory for schools to join up and connect to the IDAMaaS Broker. Initially just two NZQA applications will be connected to the Broker service which will be managed by Unify on behalf of MoE. The long-term objective is for 50 - 200 School applications plus migration of the legacy ESL applications and incorporation of workforce, Tuakiri, TEC, EPL, etc.

Digital Identity for Online Learning (DI4OL) high-level solution context
v06, 2 February 2022, D Watson

Figure 1 DI4OL Business Context view

Anticipated future changes for DI4OL

Referenced though this PIA are future possibilities outside of the current DI4OL project scope focussing on NCEA Learners. Foreseeable changes that would require review include:

- Extending DI4OL identity broker usage to pre-NCEA Secondary Learners
- Integration with prioritised digital service providers in the Secondary school sector
- Integration with Ministry applications used by Learners, for example e-asTTle
- Extending DI4OL identity broker usage to the existing Education Sector workforce (i.e., replace ESL)
- Extending DI4OL identity broker usage to Tertiary Learners, Tertiary education institutes, their IdPs and internally owned applications, Eduroam, Tertiary Education Commission (TEC), or Tuakiri applications
- Extending DI4OL identity broker usage to Primary Learners
- Extending DI4OL identity broker usage to ECE's and other pre-school services, particularly teachers/staff
- Extending DI4OL identity broker usage to include parents accessing applications, including any form of delegation framework
- Impact to DI4OL solution of the Ministry's other strategic work such as Te Mana Tūhono, the Strengthening Cyber Security and Digital Support for Kura & Schools programme.
- Integration with other personal IdPs supported by Azure B2C (beyond Apple, Google, Microsoft, and DIA's RealMe)
- Adoption of future technologies such as digital wallets for presenting verified credentials, blockchain as a distributed key store, self-sovereign identity, self-issued claims e.g., Self-Issued OpenID Provider (SIOP)
- Any direct use of biometrics by DI4OL identity broker. E.g., for identity verification at assessment time where remote assessments are undertaken
- Integration with other NZ Government digital identity credentials such as MyHealthAccount, MyIRD or education sector related services such as StudyLink, or with federation identity brokers that may exist as a part of DIA's DISTF ecosystem.

Extending the scope for the Tertiary sector may identify valid use cases for sharing the NSN, and as elaborated further in this PIA whether the NSN will be shared or not via the DI4OL identity broker is subject to approval from, and managed by, the Ministry.

Logical view and Data flow

Focussing on the first objective with NZQA, a future state view is shown in Figure 2 below. Here the school populates their specific IdP (Google or Microsoft) with the Learners Official name, preferred (known as) name, school email address, and also their Date of Birth (DoB) and NSN. When a Learner accesses the NZQA Learners Extranet they may be an automatic login (equivalent to the Single Sign-On experience in a corporate environment), or they will be presented with a choice to login with school credentials or login with personal credentials. The DI4OL identity broker will then take that request and forward it to the appropriate IdP, for the Learner to then provide their password for authentication. Once successful that authentication success is passed back to the NZQA Learners extranet via the DI4OL identity broker.

The DI4OL identity broker will only know about a Learner and facilitate their access if that Learner is accessing a digital service provider's application that is brokered by the DI4OL service. Outside of the initial use case of NZQA services, if a Learner is accessing another service then the DI4OL identity broker will not be involved in the transaction, and will not store information about that Learner unless they have accessed NZQA services. Particularly for composite schools with a wider age range of Learners, the DI4OL identity broker will not know about nor store information relating to pre-NCEA aged Learners – until such time in the future as additional digital services providers used by pre-NCEA aged Learners are onboarded to the DI4OL identity broker service.

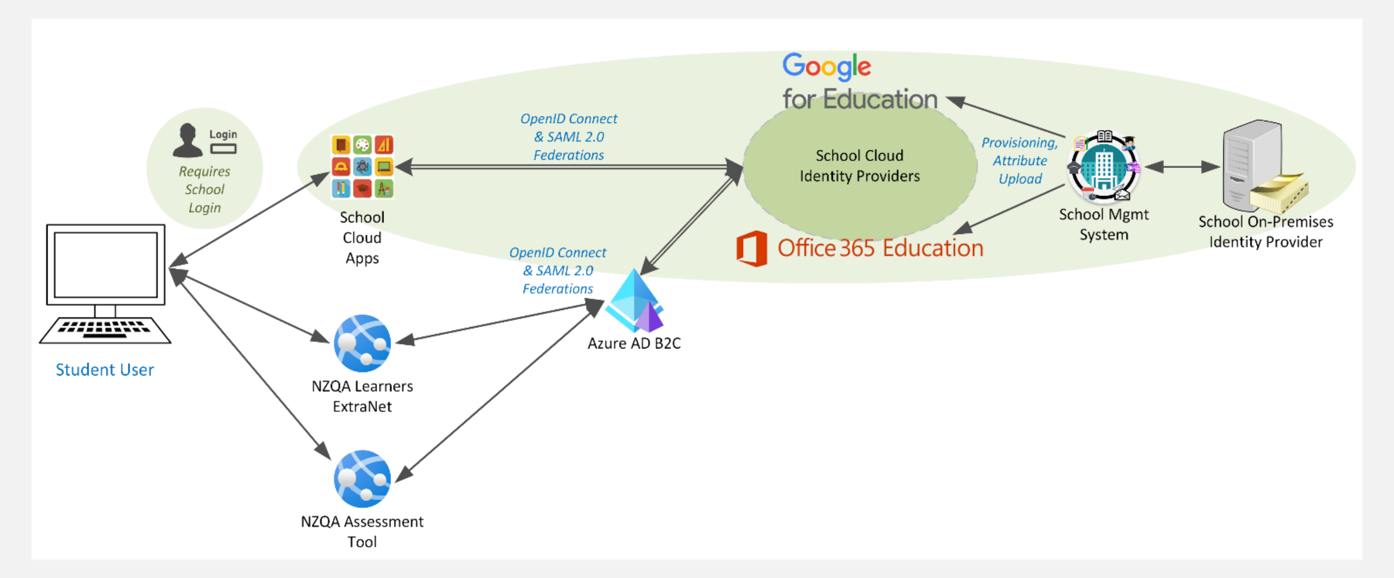

Google for Education
Login
Requires School Login
OpenID Connect & SAML 2.0 Federations
School Cloud Identity Providers
Provisioning, Attribute Upload
School Cloud Apps
School Mgmt System
School On-Premises Identity Provider
Office 365 Education
OpenID Connect & SAML 2.0 Federations
Student User
Azure AD B2C
NZQA Learners ExtraNet
NZQA Assessment Tool

Figure 2 DI4OL identity broker with NZQA

A more technical data flow showing NZQA applications is represented in Figure 3 below. Learners will be authorised by the NZQA services requesting authentication via the DI4OL identity broker service to the school IdPs, which will then authenticate the learner and return attributes (see Collection of Personal Information on page 22) about the learner including their NSN via the DI4OL identity broker to the NZQA services. A full data flow diagram with further detail for all components is Figure 7 on page 62 in Appendix 4 Full DI4OL data flow diagram.

Figure 3 below provides an example flow of information starting with a Learner choosing to login to NZQA using their school credentials (**1**), that login request being sent to the identity broker (**2**) for onward forwarding to the school's IdP (**3**). The Learner authenticates themselves (**4**), with confirmation of successful credential verification being passed back to the identity broker along with applicable attributes (**5**) and thence the NZQA application (**6**). A similar flow would apply for RealMe, iCloud or any other personal IdP that is approved for use. Considering a future state view, the NZQA application could be substituted for any other application used by schools, e.g., Minecraft for Education.

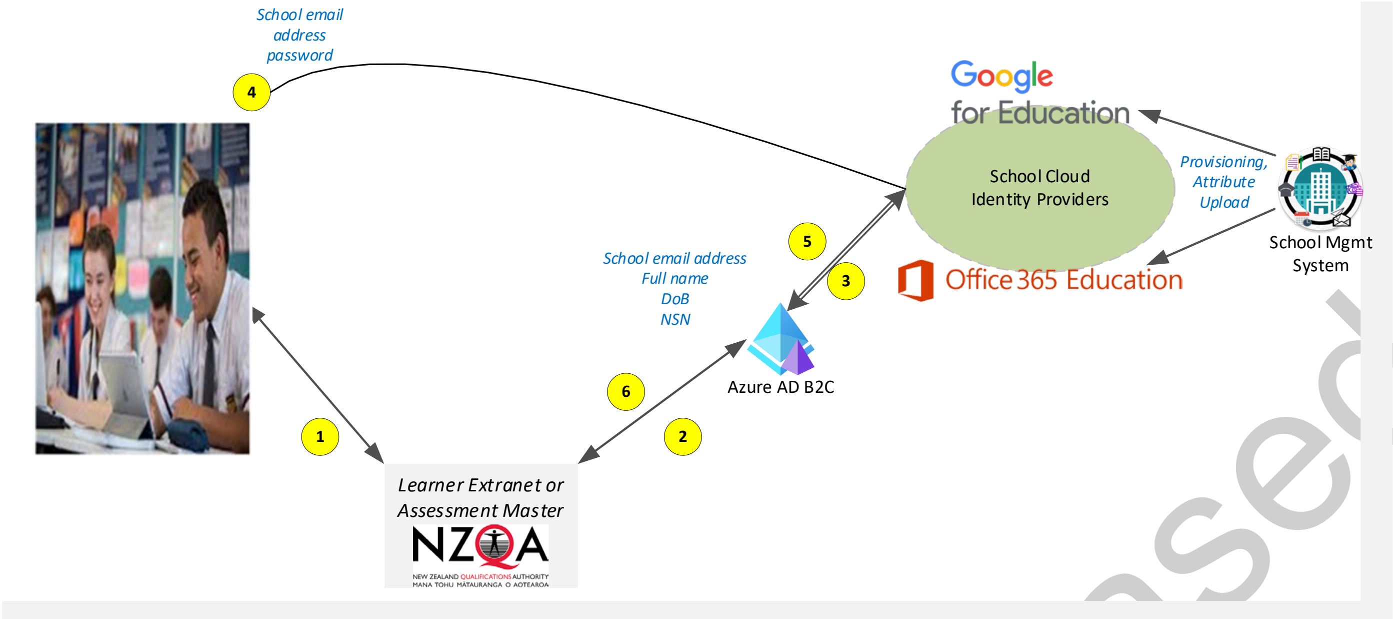
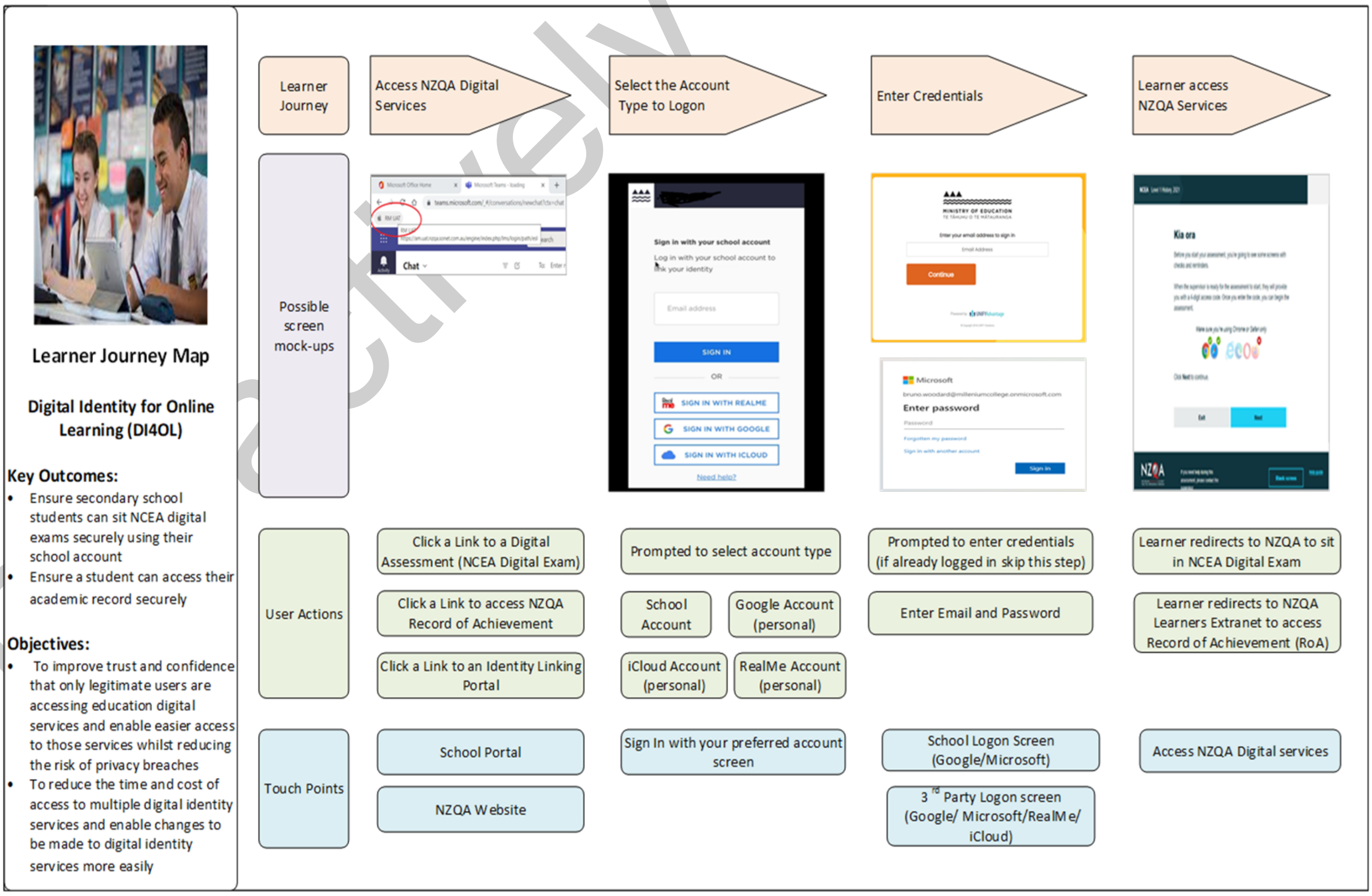

School email address password
4
Google for Education
School Cloud Identity Providers
Provisioning, Attribute Upload
School Mgmt System
Office 365 Education
5
3
School email address
Full name
DoB
NSN
Azure AD B2C
6
2
1
Learner Extranet or Assessment Master
NZQA
NEW ZEALAND QUALIFICATIONS AUTHORITY
MANA TOHU MĀTAURANGA O AOTEAROA

Figure 3 Data flow school IdP - DI4OL identity broker - Applications (NZQA)

Currently the NSN is stored in School Management Systems (SMS's), but not in the School IdP's. Part of the change required by the DI4OL solution will be to populate the NSN & DoB as attributes in the School's IdP, which enables the IdP to then share those attributes which are relevant to the DI4OL identity broker. [See NSN Options Analysis explaining this approach]. Use of a custom attribute effectively masks the existence of the NSN in the IdP, preventing it being shared to any application that does not know the custom attribute exists. In the case of NZQA being a specified user with a specified purpose (per ETA Sch 24), the DI4OL identity broker shares the NSN & DoB as attributes to NZQA.

When illustrated as a user journey Figure 2 & Figure 3 are represented as Figure 4 below.



Learner Journey Map

Digital Identity for Online Learning (DI4OL)

Key Outcomes:

- Ensure secondary school students can sit NCEA digital exams securely using their school account
- Ensure a student can access their academic record securely

Objectives:

- To improve trust and confidence that only legitimate users are accessing education digital services and enable easier access to those services whilst reducing the risk of privacy breaches
- To reduce the time and cost of access to multiple digital identity services and enable changes to be made to digital identity services more easily

Learner Journey	Access NZQA Digital Services	Select the Account Type to Logon	Enter Credentials	Learner access NZQA Services
Possible screen mock-ups				
User Actions	Click a Link to a Digital Assessment (NCEA Digital Exam) Click a Link to access NZQA Record of Achievement Click a Link to an Identity Linking Portal	Prompted to select account type School Account Google Account (personal) iCloud Account (personal) RealMe Account (personal)	Prompted to enter credentials (if already logged in skip this step) Enter Email and Password	Learner redirects to NZQA to sit in NCEA Digital Exam Learner redirects to NZQA Learners Extranet to access Record of Achievement (RoA)
Touch Points	School Portal NZQA Website	Sign In with your preferred account screen	School Logon Screen (Google/Microsoft) 3^{rd} Party Logon screen (Google/ Microsoft/RealMe/ iCloud)	Access NZQA Digital services

Figure 4 User journey view of DI4OL

A simplified view of all components in the end-to-end DI4OL solution are shown in Figure 5, this represents a future state beyond the pilot involving NZQA and reflects other digital service providers. Figure 5 below illustrates that multiple IdPs will be connected to the DI4OL identity broker, which will then connect to multiple education sector applications, facilitating Single Sign-On (SSO) to those applications using the Learners chosen credentials from their education provider or personal IdP.

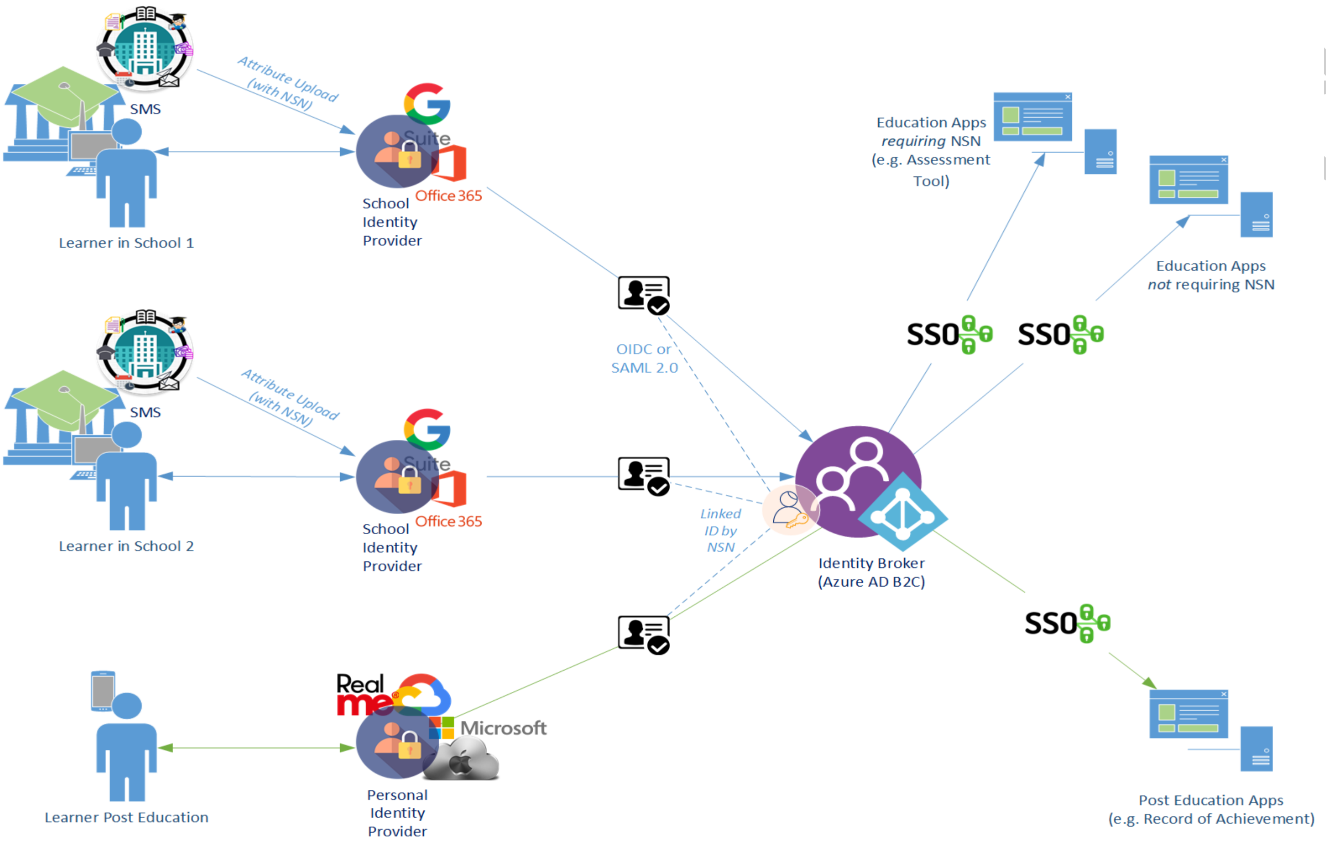

SMS
Attribute Upload (with NSN)
Learner in School 1
Suite
Office 365
School Identity Provider
SMS
Attribute Upload (with NSN)
Learner in School 2
Suite
Office 365
School Identity Provider
Learner Post Education
RealMe
Microsoft
Personal Identity Provider
OIDC or SAML 2.0
Linked ID by NSN
Identity Broker (Azure AD B2C)
Education Apps *requiring* NSN (e.g. Assessment Tool)
Education Apps *not* requiring NSN
SSO
SSO
SSO
Post Education Apps (e.g. Record of Achievement)

Figure 5 DI4OL simplified solution view

Where a digital service provider is not a specified user, nor acting for a specified user, the NSN and Date of Birth (DoB) will not be shared by the DI4OL identity broker, and this will be enforced through technical configuration. The DI4OL identity broker will only share the email address attribute by default. The NSN and DoB attributes are custom attributes and will only be shared with digital service provider applications approved by the Ministry to receive one or both attributes. One nuance to this is where a digital service provider is acting as an agent for an education provider and there is a need for that digital service provider to have a record of the NSN for specified purposes that the education provider requires. The configuration of all applications connecting to the DI4OL identity broker will be managed by the Digital Identity operational team within the Ministry. They will be able to confirm whether a digital service provider is acting for a specified user.

Government Digital Identity context

In July 2020, Cabinet agreed to establish a Trust Framework to address the regulatory gaps in New Zealand's digital identity system[8]. The Digital Identity Trust Services Framework (DISTF) Bill was introduced into Parliament in late 2021 and will establish an opt-in regulatory regime for the provision of regulated digital identity services. Under the Trust Framework, rules will be developed that opted-in accredited parties must follow. These will cover identification management, information and data, security and risk management, privacy requirements, and requirements for facilitation services. The Ministry is considering the applicability of the DISTF within the education sector for education providers and the Ministry has yet to formerly decide whether Ministry digital services will seek accreditation or only align with the DISTF. Until the Bill becomes an Act and the rules are finalised the DI4OL project team will keep a watching brief on progress.

[8] The Digital Identity Trust Framework (DITF) now referred to as the Digital Identity Services Trust Framework (DISTF) CAB-20-MIN 0324

While the Trust Framework will provide a regulatory framework to underpin consumer confidence and support trust, it does not directly create secure digital identity tools and systems. In June 2021, Cabinet directed the Department of Internal Affairs (DIA) to develop a detailed business case to assess the investment options for modernising government digital identity infrastructure.

The DI4OL project will leverage the DISTF as it is implemented and maintain the existing alignment of DI4OL principles[9] with the digital identity service experience principles outlined below:

- People and culture-centred – Digital identity services are equitable and designed and developed by understanding the needs of those who benefit from and support service delivery.
- Adaptive and Improving – Digital identity services are continuously improved and adapted to better serve those who benefit from and support their delivery.
- Simple – Users can easily access services within the education system using their digital identity and workforce, third parties and Education Agencies can easily deliver services.
- Seamless – Digital identity services are joined-up and provide a unified, end-to-end service experience for workforce, third parties and Education Agencies.
- Trusted and collaborative – Digital identity services are designed to be trusted and secure and have been developed collaboratively with input from users.
- Valuable – A single, consistent digital identity is of value to workforce, and third parties and improves users experience within the education system.

Review and analysis of the existing Identification Management Standards (IMS), the proposed DISTF Bill and draft DISTF Rules (February 2022) has identified a few high-level organisational risks for the Ministry. These include:

- Legal liability to the Secretary for Education, particularly in the context of DI4OL being a federation provider
- Risk to ETA not being 'digital ready' including specified purposes for NSN
- Privacy risk
- Relationship risk between the Ministry and Schools, as well as other education providers
- Risk to Learner trust and willingness to attend school
- Equity and Inclusion risks where Digital Identity entry requirements may impede attendance or participation
- Risk to customer service expectations if the Ministry does not align with, or accredit to, DISTF.

Detailed analysis of the DISTF draft Rules has identified some Rules that the Ministry is unlikely to adhere to as written. This may exclude the Ministry from seeking accreditation under the DISTF in the future. Consultation with DIA to date indicates that as the Ministry and the DI4OL identity broker will align with the spirit of these rules, this may be sufficient. A determination based on the final set of published rules by the DISTF Accreditation authority will be required. This will likely happen after the DI4OL identity broker has gone live.

There are also controls within the Identification Management Standards that the Ministry may not include within scope of the end-to-end DI4OL service or a formal Statement of Applicability (SoA). Analysis of the shared responsibility between education providers, the Ministry, and application service providers is being performed to identify how practical affect could be achieved. Where DISTF controls are tightly coupled with specified roles in a Digital Identity ecosystem, this may preclude formal accreditation of all participating parties (e.g., ~2,500 schools, ~200 tertiary institutes) in the DI4OL identity broker ecosystem for the education context.

A final point in relation to the DI4OL identity broker is that there will be no use of biometrics by the DI4OL identity broker itself. This is briefly considered under IPP4 on page 31 and in relation to recommendation 5.1.7 from the *2015 NSN PIA* on page 67. Biometrics may be implemented by education providers or individuals to authenticate to their devices and depending on the implementation this may be relied upon by an education providers IdP as Multi Factor Authentication (MFA). However, the DI4OL identity broker will not be using any biometric info. If in the future use of biometrics is encouraged or recommended as part of the DI4OL identity broker, this PIA and the security risk assessment will be reviewed.

[9] DI4OL Principles are elaborated within Figure 8 DI4OL Business Context view (A3 size) on page 57

Legislative Context Application of Education and Training Act 2020

The Education and Training Act 2020 (ETA, referred as 'the ETA' in this PIA to avoid ambiguity) includes §621, which refers directly to Schedule 24 specifying how the National Student Number (NSN) can be used. Education and Training Act 2020 No 38 (as of 01 January 2022), Public Act Schedule 24 National student numbers – New Zealand Legislation. The seven permitted purposes are:

i. Monitoring and ensuring student enrolment and attendance:
ii. Encouraging attendance at early childhood services:
iii. Ensuring education providers and students receive appropriate resourcing:
iv. Statistical purposes:
v. Research purposes:
vi. Ensuring that students' educational records are accurately maintained:
vii. Establishing and maintaining student identities to support online learning.

Pre-dating (31/07/2019) the ETA is a Gazette notice (NSN Notice 2019), which gave effect to use of the NSN under the Education Act 1989 (Part 30 §341-§347 about the NSN) for purposes (i-vi). The ETA and *NSN Notice 2019* are the two main legislative instruments relating to the use of the NSN applicable to the DI4OL identity broker.

Use of the NSN by specified users and education providers is governed by the ETA. The Secretary for Education (or their appropriately authorised delegate) is able to authorise specified users to use NSNs for specific purposes via a Gazette notice. The Secretary may also stipulate restrictions or conditions for that use via the Gazette notice. The pilot and operational production phases of the DI4OL project will need to ensure that the Ministry and other involved parties adhere to the ETA.

Outside of this requirement, Schedule 24 has clause 5 **Person may use or disclose own national student number**. This permits the individual that the NSN relates to, to disclose their NSN to any party for any purpose. For example, an individual could disclose their NSN to DIA as part of a digital wallet, which is used by a Tertiary institute. Here DIA is acting as an agent of the Learner and is not using the NSN in its own right, thus DIA may not need explicit authority under the ETA to receive the NSN, as the individual is implicitly authorising DIA to receive the NSN.

Of note is a gap between the ETA and the *NSN notice 2019* where Schedule 24 of the ETA includes a seventh permitted use:

> **4 Use of NSN** (1) (c) (vii) 'establishing and maintaining student identities to support online learning'.

Although the use of the NSN by NZQA for maintaining education records is already covered by **4 Use of NSN** (1) (c) (vi) 'ensuring that student educational records are accurately maintained', the fact that the sub-clause **4 Use of NSN** (1) (c) (vii) relating to 'online learning' has not yet been authorised through a Gazette notice introduces a difference that may lead to ambiguity or misinterpretation and needs resolving.

NSNs can only be used by specified users for the purposes authorised by the Secretary under the Gazette notice. The Ministry, NZQA and education providers all play a role in establishing and maintaining the students' online identities under DI4OL, and all parties requires access to the NSN in order to do so. Therefore all of these parties have a role in maintaining students' identities for the purpose of online learning. A Condition will be specified in the Gazette notice requiring schools to seek approval from the Ministry before using the NSN for 'online learning' purposes, unless an identity provider is on a published approved list.

The Ministry and NZQA have agreed that an updated Gazette notice will be published to support the 'online learning' use of the NSN which is critical to DI4OL identity broker implementation. The new Gazette notice will clarify that 'online learning' includes the business processes within NZQA that are referred to as 'submission' and 'assessment', since it is implicit that Learners must submit evidence of their learning for assessment. Although it is unlikely that a legally binding definition of assessment will be possible as assessments can be performed in a variety of formats online and in person, are not always standalone from the learning itself. For example, in Minecraft some learning modules include built in assessments that must be completed before the Learner progresses to the next step, with the summative assessment being by a teacher that a Learner has completed the module.

The Ministry has defined online learning in the context of other commonly used terms as;

- **Online learning** is accessed by the student via the internet whether remotely or onsite at school
- **Blended learning** is the combination of traditional classroom learning and online learning while students are onsite.

See the *Te Poutāhū: Hybrid learning position paper*. This is used as a broad working definition through this PIA. In the wider education ecosystem and IT industry generally the term online learning is broadly used and has multiple different interpretations. This makes a useful definition of what online learning consists of in a legal context, with clear and unambiguous boundaries for Gazetting purposes, impractical as the definition would need to be too broad and thus open to interpretation. This PIA is intended to support the process of publishing a Gazette notice[10].

Collection of Personal Information

The Personal Information (PI) collected by an education provider about a Learner is already collected as part of enrolment. PI used by the DI4OL identity broker is minimised to only what is needed, being:

- First name and surname, preferred name
- Date of Birth
- School email address
- NSN

For example:

- Thomas Kendall, Tom
- 25/4/2017
- tom.kendall@hohi.school.nz
- 314159265

After NCEA assessment time Learners will be encouraged to register a personal credential (e.g. email address) with access to the DI4OL identity broker linking portal. This is undertaken by individual Learner and is their choice to opt-in. This personal credential then replaces the school email address once a Learner leaves secondary education. When a Learner links a personal IdP they must first login using their school credentials, with the linking portal then allowing them to add a personal credential. The name attributes of the personal IdP will be checked in the linking portal, with the intention of preventing a third party from linking a random email account that does not match the individual's name. If a Learner chooses not to link a personal credential they will revert to existing NZQA business processes to obtain access to their RoA.

Additional transactional information may also be stored within the schools IdP and the DI4OL identity broker, such as TCP/IP address, non-PI device details including type and versions of OS, browser. In the future aligned to DISTF adoption there may be further non-PI attributes stored and shared. These DISTF attributes are not visible to any Learner and are technical information necessary for the proper functioning of the DI4OL identity broker in alignment with the DISTF. The DISTF attributes include a level of assurance which uses an integer 1-4 to reflect the level of assurance that can be obtained by Relying Parties about the:

- Binding of the individual to an identity
- Quality of information about an individual
- Authentication level for a specific logon transaction.

It is unlikely the Level of Assurance attributes relating to information will be included within the DI4OL pilot phase. It may be introduced during the production deployment depending on the progress of the DISTF and the Ministry's strategic compliance or alignment with DISTF.

One example of another attribute is whether Multi Factor Authentication (MFA) was involved in authenticating the login. Within schools it is possible, although unlikely, that MFA is used by Learners. Where personal IdP's are used for post school Learners, the Learner may have to setup their credentials to use MFA. As part of the logon process an attribute will be shared with the DI4OL identity broker to indicate whether an MFA challenge was made and successful passed. The nature of the MFA challenge or its form factor will not be known by the DI4OL identity broker, including whether a biometric was used for MFA. Use of MFA has a foreseeable flow on effect for digital service providers and will be important in the future when more digital service providers mandate the use of MFA.

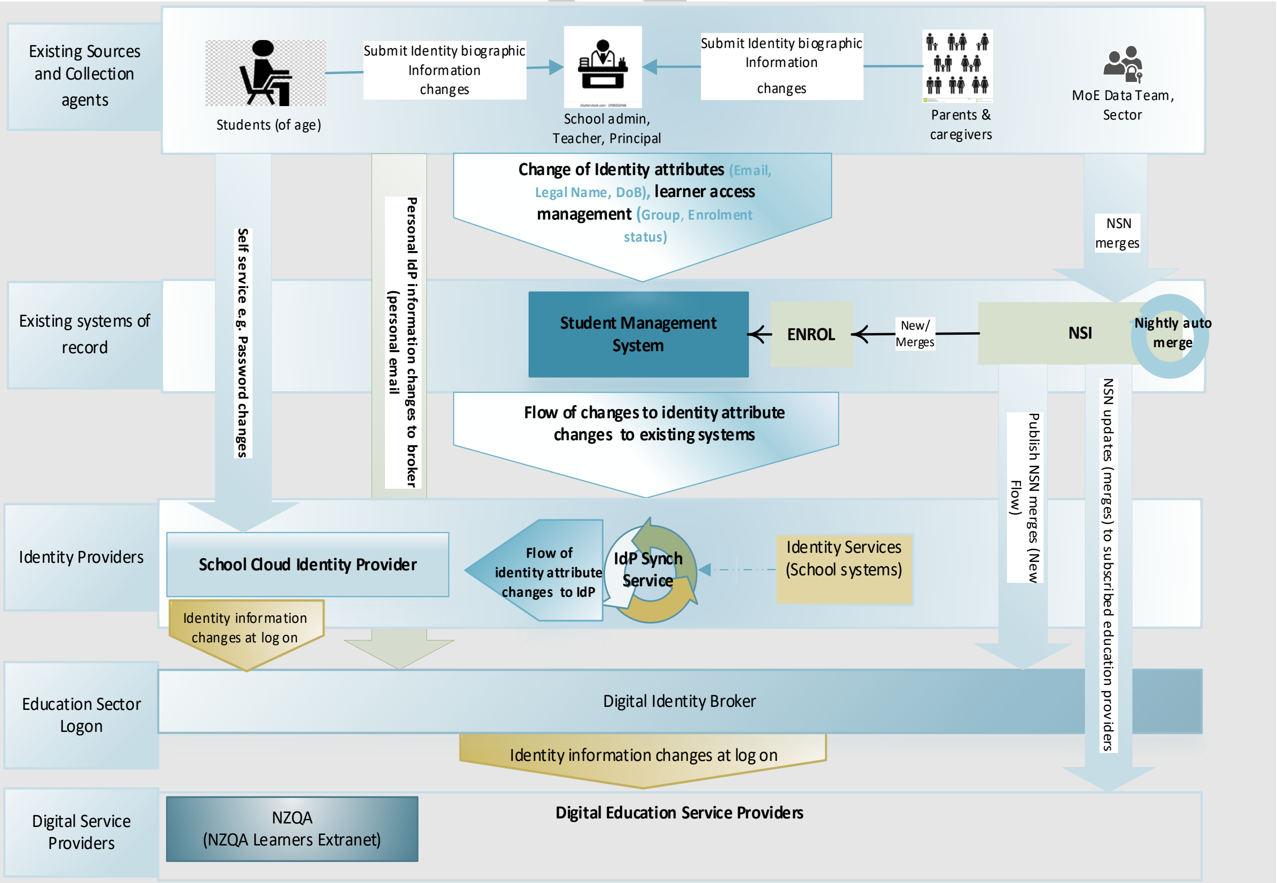
[10] The Gazetting process here is for the New Zealand Gazette, not the Education Gazette. Although project communications with schools may also include using the Education Gazette as a channel.

The Ministry and Schools collect extensive information about a Learner at enrolment time and subsequently through their learning journey. Pūwaha provides an overview of the nineteen (19) different Ministry systems that store or process information relating to enrolments. ENROL is considered the primary system, when a Learner is first enrolled at a school they are added to the ENROL system. Where an NSN does not yet exist or is unknown by the enrolling party, ENROL initiates the creation of an NSN within the National Student Index (NSI). Where an NSN does exist, the administrator enrolling a Learner performs (in digital identity terms) a binding between the Learner and the information held about them by the school and in the NSI and ENROL. Information collected about the Learner in ENROL is more than the DI4OL identity broker will subsequently use. High level data flow diagrams associated with systems can be found under their applicable Pūwaha entry. Publicly available guidance for users of ENROL is found on the Ministry's website.

The NSN itself is stored in twelve (12) different Ministry systems, three non-Ministry systems in the wider education sector, plus each school SMS.

The above description provides an example where the same information that the DI4OL identity broker uses is collected, along with additional information, and used as part of the Learners journey through education. During this journey Learner information could be stored in multiple different Ministry systems, potentially up to thirty-five (35) if we consider the range from Attendance Collection to the Youth Justice National Minimum Dataset. It is not the purpose of this PIA to describe the enrolment process or Learner's journey and all systems that may hold extensive information about the Learner, let alone their actual learning. Simply to highlight the self-evident axiom that information used by the DI4OL identity broker is already collected and held by schools and the Ministry.

Schools collect comprehensive information and demographics about a Learner at enrolment and throughout their time at the school, much of which is PI and some of which would be considered sensitive including emergency contact information, home address, medical issues, parents contact details etc. None of this will be used by the DI4OL identity broker. Figure 6 below provides a high-level representation of the collection process from a DI4OL identity broker perspective.



Existing Sources and Collection agents
Students (of age)
Submit Identity biographic Information changes
School admin, Teacher, Principal
Submit Identity biographic Information changes
Parents & caregivers
MoE Data Team, Sector
Change of Identity attributes (Email, Legal Name, DoB), learner access management (Group, Enrolment status)
NSN merges
Existing systems of record
Self service e.g. Password changes
Personal IdP information changes to broker (personal email)
Student Management System
ENROL
New/ Merges
NSI
Nightly auto merge
Flow of changes to identity attribute changes to existing systems
Publish NSN merges (New Flow)
NSN updates (merges) to subscribed education providers
Identity Providers
School Cloud Identity Provider
Flow of identity attribute changes to IdP
IdP Synch Service
Identity Services (School systems)
Identity information changes at log on
Education Sector Logon
Digital Identity Broker
Identity information changes at log on
Digital Service Providers
NZQA (NZQA Learners Extranet)
Digital Education Service Providers

Figure 6 Personal Information data collection flow

During the pilot we anticipate undertaking data quality reviews to assess school IdP data quality with SMS, ENROL and NSI data for the minimal fields that the DI4OL identity broker will be using (i.e. official and preferred name, DoB, NSN). Depending on the outcomes of this data quality review, the Ministry may recommend that education providers perform a data quality check before they are on-boarded to the DI4OL identity broker during the production deployment in 2023. Although such data quality checks should be performed by education providers on a regular basis, anecdotal information indicates that there remains a persistent data quality issue, likely caused by human error when inputting information to multiple different systems.

The scope of the DI4OL pilot is for between two and twenty schools, potentially up to ~3,200 Learners will be undertaking NCEA as a sub-set of all Learners at those schools. If the pilot is successful a full nationwide rollout, noting that DI4OL identity broker use is opt-in, could include up to ~2,500 schools and ~825,000 school learners in primary and pre-NCEA secondary education when additional applications beyond the NZQA use case are included. Any future rollout to tertiary education institutions including Universities, Te Pukenga, Wananga, (these three groups total 16 institutions with ~380,000 Learners out of the total Tertiary sector of 200 tertiary education providers with ~ 530,000 Learners), Industrial Training Organisations (ITOs) etc. is subject to further consideration and review outside the scope of the DI4OL project itself.

Use of Personal Information

The intended use of the personal information by the Ministry operated DI4OL identity broker is to facilitate Single Sign-On (SSO) using a Learner's school credentials to online learning resources. Use of the DI4OL identity broker remains opt-in for all education providers and digital service providers. We anticipate the benefits of SSO with improved usability and ease of access will make opting in an attractive option for schools and Learners. As schools opt-in we anticipate that the Ministry will review digital service providers and their applications against information security and privacy requirements to prioritise a list of which integrations with the DI4OL identity broker will be permitted.

As described in the Project Overview on page 14, the first use case focusses on NZQA applications relating to NCEA. After a Learner departs school, they will use either their school credentials (in the short term) or personal credentials (in the longer term) to access assessment results if they choose to continue to opt-in. Learners entering tertiary education will also be able link their tertiary institute credentials to the DI4OL identity broker, once those tertiary institutions integrate with the DI4OL identity broker, to maintain continued access to their Record of Achievement. Once the Ministry has integrated with digital service provider applications used in the tertiary education sector, this will enable Learners to access tertiary education resources again benefiting from SSO and being able to use tertiary or personal credentials. This approach will then continue with additional tertiary education provides such as ITOs. Post school Learners may choose to opt-out of using the DI4OL identity broker service, though they will need to maintain NZQA credentials to ensure access to their NCEA RoA or other Tertiary qualifications.

Overall, we anticipate that use of the DI4OL identity broker by education providers will be privacy enhancing and bring other improvements in security maturity to the education sector. As discussed elsewhere in this PIA, attributes shared by the DI4OL identity broker will be minimised to email address and a pseudonymous identifier as a default. As email addresses setup by education providers tend to be a person's name it is implicit that some or all of a person's name will also be shared by virtue of sharing their education provider email address. Only where a third-party application has been reviewed and approved by the Ministry will a Learners DoB or NSN potentially be shared via the DI4OL identity broker. As discussed under IPP's 10 and 13, pseudonymous identifiers are the default to be shared rather than the NSN.

Storage of Personal Information

Personal information collected by schools will be stored within SMSs and IdPs that are operated by the schools. The main change for schools introduced by the DI4OL identity broker is that NSNs will be stored within school IdPs where they may not be stored there today. Schools store additional PI in their IdPs beyond that needed by the DI4OL identity broker, and that is a school responsibility to manage.

Within the Ministry, the DI4OL identity broker will store the required PI within the Ministry's Azure tenancy in Australia. This will include school email address and, where linked by the Learner, one or more personal credentials to maintain access to their RoA. Only Ministry staff, or authorised service providers, that have been approved for privileged access to the Azure B2C broker functions will have any access to the data stored within the DI4OL identity broker. Individual Learners will have access to the DI4OL identity broker linking portal, and this will enable access to their own information.

Although the Ministry's consumption of Azure services has not yet been formally Accredited by the Ministry, the DI4OL project team have reviewed assurance documentation from Microsoft. This assurance documentation includes the most recent and past SOC2 Type2 reports, ISO27001 Certification, and Australian government Information security Registered Assessors Program (IRAP) audit reports. This Microsoft assurance documentation also covers IdP services consumed by schools. The different assurance processes and practices provides a high level of assurance that Microsoft has effective information security practices in place.

Similar assurance documentation from Google relating to Google Cloud IdP used by schools has been reviewed. This assurance documentation included the most recent SOC2 Type2 report, ISO27001 Certification, and IRAP audit reports.   The different assurance processes and practices provides a high level of assurance that Google has effective information security practices in place.

Assurance documentation relating to DIA's RealMe service has been reviewed. This provides a high level of assurance for the Ministry in consuming RealMe services, a key similarity is that the RealMe service is now based on an Azure B2C platform. The executive summary of the RealMe PIA notes:

> *"After assessing the project, our conclusion is that the changes DIA is making to the RealMe service via this project* [being the migration to Azure B2C] *do not have major privacy impacts. The main risk areas identified are around the technical security of the new platform, and the potential impact on the current social licence DIA holds from its RealMe users."*

Assurance documentation for the storage of PI, excluding the NSN, within Apple's iCloud service, has been requested and will be reviewed as part of the overall C&A process.

Responsibilities for the Ministry arising from these vendor assurance reviews will be noted in the information security risk assessment as part of the C&A process.

Apple and Google have signed the most recent version of the US student privacy pledge Signatories 2.0 - Pledge to Parents and Students (studentprivacypledge.org), while Microsoft are classified as a signatory to the legacy pledge. The material difference between legacy and 2020 pledges is two additional positive pledges to support educational institutes with resources relating to their products and incorporating security and privacy by design practices. Microsoft meet both in practice.

Disclosure and Sharing of Personal Information

The DI4OL identity broker will facilitate use and disclosure in a consistent standards-based manner, minimising the disclosure of PI, and enabling positive outcomes for Learners. As discussed above in the Project Overview and Use of Personal information sections, some PI (at least school email address) is already disclosed by education providers to digital service providers acting as agents for those education providers when schools are setting up accounts for Learners to use those applications. E.g. Mathletics, Minecraft. The disclosure being necessary for education providers to deliver instruction to Learners via those applications. Where the digital service provider has required an email address, that likely includes the Learners full name because the school IdP was not configured to provide a pair-wise identifier. In future the DI4OL identity broker will enable the use of a pseudonymous pair-wise identifier instead of any identifying information.

Digital service providers complying with the OpenID Connect (OIDC) standards can request in a Standard Claim transaction a variety of additional information from the IdP including a photo, physical address, or phone number where associated with the personal IdP credential, which the IdP may honour. With the DI4OL identity broker mediating the request, only the minimal information permitted by the DI4OL identity broker will be returned to the digital service provider.

Any disclosure of the NSN will be subject to review and approval by the Ministry, with an appropriate configuration enabled within the DI4OL identity broker to permit the sharing of the NSN only if approved.

Retention and Disposal of Personal Information

Until a Learner links a personal IdP through the linking portal, no information is persistently stored about the Learner within the DI4OL service. The DI4OL Service is purely transactional. (accepting the existence of necessary logging data). Per Collection of Personal Information on p22, when a Learner links a personal IdP in the DI4OL service, their Official name, preferred name, DoB, NSN are stored along with the Learners current school email address and their newly linked personal email address.

Information stored in the DI4OL identity broker is subject to the Ministry's Data Retention and Disposal Policy, as well as updated guidance provided to schools in May 2022 by the Ministry and Archives NZ entitled *Schools Records Retention/Disposal Information Pack*. This identifies a default retention period of seven (7) years for general school records about a Learner. As information about a Learner is keyed to their enrolment status with a school, when a Learner leaves school the attributes about a Learner associated with their former school will be removed. Similarly, attributes related to any Tertiary education institute a Learner attends will be removed as they exit Tertiary education.

In the context of lifelong learning, with a personal IdP associated to the DI4OL identity broker, the Learner can maintain access to their record of achievement/learning stored with NZQA. From that perspective retention of information within the DI4OL broker to facilitate access will be 'lifelong' and not disposed of. The planned AISA with DIA for sharing Births, Deaths and Marriages information will provide an input to permit the DI4OL broker to place a finite limit on retention of information by the DI4OL identity broker. At which point the Ministry's seven (7) year retention cycle would initiate. As the Ministry is not holding the formal public record of a Learner's achievement, simply facilitating access for the Learner, it will be with NZQA to follow their retention and disposal schedules for a deceased person's record of achievement.

Security Classification of Personal Information

As the information is about Learners and collected by schools, no formal classification of the information is conducted at source. The same applies to tertiary education providers and is likely to apply to private sector education providers such as ITO's. Instead, the DI4OL identity broker inherits the information classification established for the ESL solution. This is defined as SENSITIVE, given that ESL contains logon information that provides access to Ministry systems that contain SENSITIVE information.

See Assessment Part 5 – GCSB Information Classification for elaboration.

Assessment Part 2 – Privacy Principle Analysis

This assessment is of the DI4OL identity broker against the 13 Information Privacy Principles (IPP's) in the Privacy Act 2020. The Information Privacy Principles are detailed in Appendix 1.

IPP	Privacy Principle	Assessment against Privacy Principles	Compliance	Link to Risk
	Collection			
IPP 1	Information should be collected for a lawful purpose You should only collect the personal information that you need	The DI4OL identity broker will use information that has already been collected by schools, under the authority of the Education and Training Act 2020 (ETA). The purpose for which the DI4OL identity broker will use the information is clear. For the purposes of 'online learning' a Gazetting process is required to give effect to the legal authority contained within the ETA. Schools collect a wide variety of information about Learners for approved educational purposes. Most of this information is stored with School Management Systems (SMS), and in associated Ministry systems. Of the information already collected by education providers, only a minimal and necessary sub-set will be used for DI4OL purposes. As noted under Collection of Personal Information on page 22, the information to be used by the DI4OL identity broker has been minimised and is basic. Feedback will be sought from Learners, Teachers and other stakeholders during the pilot as to whether the additional purpose for sharing information with the Ministry for 'online learning' was expected, reasonable, or whether it raises concerns. Some of the information (name, email address) is also stored within a school IdP – in this case the technology provider of the IdP is acting as the school's agent. Similarly, some information (name, email address, possibly age where there may be licensing or content restrictions to consider) may also be stored with a digital service provider, for example to enable logon to the application, and again that digital service provider is acting as an agent for the school. A core assumption for the Ministry is that school Boards ensure their schools are following guidance provided by the Ministry. That schools are collecting PI in a manner consistent with the Privacy Act and the ETA; Learners & parents are appropriately informed of the necessity to collect information; processes to collect the information are not intrusive; and those forms (online or paper based) and school Privacy policies clearly articulate these topics. During the pilot the Ministry will review school Privacy statements and provide guidance on whether the existing school Privacy statements or policies may need updating to reflect the additional purpose for which schools are opting-in to share information with the Ministry. Ultimately this will be a decision for the schools to make, consistent with the level of detail they provide to Learners and Parents.	**Compliant**	**P-01**

IPP	Privacy Principle	Assessment against Privacy Principles	Compliance	Link to Risk
		Irrespective of any authorised purpose for collection under the ETA, a Learner may disclose their NSN to a third party for any purpose that the Learner decides to. See **ETA Schedule 24 Clause 5.** Implicit in this is that a Learner could be asked by an education provider or digital service provider to disclose their NSN as an optional information request, and if the Learner does disclose their NSN, then this is within the Learners purview to do so. The Ministry currently has no visibility of whether digital service providers are collecting NSN's as part of the services they provide today. Although this is highly unlikely. Adoption of the DI4OL identity broker will enable visibility of whether this is happening and introduce a technical capability to block digital service providers connected with the DI4OL service receiving the NSN in future. Only a minimal set of necessary information will be used or exchanged as part of DI4OL solution operating. Noting that where education providers use existing digital service providers today, that information collection and exchange is already taking place in the absence of the DI4OL identity broker. In practice the Ministry and education providers hold richer information about Learners in other systems that have greater direct human interaction than the DI4OL identity broker (see Collection of Personal Information on page 22). Specific to the NSN itself, given that IdP technology providers and digital service providers are acting as agents for education providers, the NSN remains under the education provider's accountability and authority to use as a specified user. The scope for new applications linked to the DI4OL identity broker to collect additional information without the user's consent (authorisation) or knowledge is managed in an exchange via the DI4OL identity broker but cannot be prevented once the Learner is using the application itself. There is the potential that in the future applications leveraging new technology will seek to collect additional information that may not be transparent to the Learner. Such as location information automatically from a mobile device to provide an easier logon experience for the user. Thus, there is a risk for additional information that may be PI to be collected.		
IPP 2	You should collect information directly from the person (unless an exception applies)	The DI4OL identity broker will only consume information that the school has collected directly from the Learner, or their appropriate representative (a parent, guardian, or teacher). Information collected by schools from Learners or their parents is already shared with the Ministry for a number of purposes that are mandated by the Education and Training Act. It is common sense that parents or guardians act for children that they are responsible for, and stipulated in law under Care of Children Act 2004, Section 17, *Child's father and mother usually joint guardians*. Where the child is unable to understand their own privacy interests, the parent can make an informed decision on whether information sought about the child is purposeful, has the parents' consent, is non-intrusive, is accurate and kept up	**Compliant**	**N/A**

IPP	Privacy Principle	Assessment against Privacy Principles	Compliance	Link to Risk
		to date. Obligations under the ETA stipulate that a parent or guardian are responsible for ensuring records that schools and the Ministry hold about their child(ren) are correct. When a Learner links their personal IdP of choice within the DI4OL identity broker linking portal, this will be an action by the Learner, and thus with their consent. The current scope for the DI4OL includes secondary school students undertaking NCEA, who are likely to have their own privacy interest separate from their parents. Beyond the common-sense provision that parents act for their children, it is possible from a Privacy Act perspective IPP2 exception (2)(a) or (f) could apply to collection of information. No material Privacy risk was identified in relation to the collection of information for the DI4OL identity broker, primarily as the use of this information is in line with the purposes for which the information was collected by schools through their enrolment processes and already shared with the Ministry for educational purposes.		
IPP 3	You should let people know that you are collecting personal information, what will be done with it, and what their rights are	Use of the DI4OL identity broker will be opt-in for schools. As mentioned previously a comprehensive communications and change plan will be developed to engage with schools, articulating the issues that use of the DI4OL identity broker will resolve for schools and their Learners. Once a school expresses an interest to opt-in further onboarding specific communications and planning will be conducted with the school, including templated communications that can be shared with other stakeholders such as Learners, parents, School Board of Trustee's etc. The communications will ensure that the Ministry is transparent with schools on the purpose for using the information, even though this is information that the school has already shared with the Ministry for other purposes. Technical pre-requisites will need confirming with the school, along with business process checks. Communications to schools will also include guidance outlining business process relating to adoption of the DI4OL solution. This will re-affirm (per ENROL guidance) the need to sight a birth certificate, and correct formatting and accurate entry of personal information (first name, surname, preferred name etc.) within SMS's (**PRI-10**). The guidance documentation will clearly explain the purpose for schools using the information in the context of the DI4OL service and provide links for where further information can be found. Schools may need to update their Privacy policies to reflect use of the NSN and other PI for 'online learning' purposes. As discussed regarding the communications plan and initial onboarding review, the Ministry will consider and provide guidance on whether existing school Privacy statements or policies may need updating to reflect the additional purpose for which schools are opting-in to share information with the Ministry. Ultimately this will be a decision for the schools to make, consistent with the level of detail they provide to Learners and Parents. With the Ministry providing this comprehensive package of communications, it will be for the school to decide what is appropriate for them to share with Learners, parents and their communities in a manner consistent with existing school communications. Information will be published on Education websites including the NSN page and	**Compliant**	**P-08** **P-09**

IPP	Privacy Principle	Assessment against Privacy Principles	Compliance	Link to Risk
		NSI landing page. This will allow Learners, parents, other interested to access information irrespective of what is communicated via Schools. The Ministry will not be expressly seeking consent from each Learner, or their parent, as it will not be practical to expect schools to seek explicit consent for the new specified purpose of 'online learning'. This would qualify under IPP3 exceptions (3) or (4 (a) & (d)). In providing the comprehensive package of communications that schools can use the Ministry is enabling schools to be clear and transparent with their Learners & parents, while also providing consistent publicly available information on the Ministry's websites if anyone is searching for information. Existing school privacy policies make broad reference to collecting information for 'educational purposes' many of which relate to online learning without specifying detail[11]. The DI4OL identity broker will only store information about a Learner and facilitate their access if that Learner is accessing a digital service provider's application that is brokered by the DI4OL service. Outside of the initial use case of NZQA services, if a Learner is accessing another service then the DI4OL identity broker will not be involved in the transaction, and will not store information about that Learner unless they have accessed NZQA services. Particularly for composite schools with a wider age range of Learners, the DI4OL identity broker will not know about nor store information relating to pre-NCEA aged Learners – until such time in the future as additional digital services providers used by pre-NCEA aged Learners are onboarded to the DI4OL identity broker service. No material Privacy risk was identified in relation to informing schools in a transparent manner about the collection of information, primarily as the use of information is in line with the purposes for which the information was collected by schools through their enrolment processes and shared with the Ministry. As a result of consultation with OPC & GCPO a risk was identified for the Ministry in relation to schools socialising the information the Ministry provides to them with their Learners and parents. If a school does not socialise in a transparent manner the information the Ministry shares relating to the DI4OL identity broker, then Learners and parents may feel they have not been appropriately informed on the additional purpose for which schools share information with the Ministry. Similar to existing pages on the Ministry's main website (ESL has Catalogue of tools & online services | Applications & Online Systems (education.govt.nz), ICT & Digital services for schools Digital technology – Education in New Zealand), we expect the DI4OL will have a webpage providing information consistent with the communications material provided to schools and other stakeholders. This will link to NZQA, the Ministry's existing NSN & NSI pages and other associated sites.		

[11] Island Bay School is the only example found of a school privacy policy that goes into specific detail of which applications a school uses.

IPP	Privacy Principle	Assessment against Privacy Principles	Compliance	Link to Risk
IPP 4	Information should be collected lawfully, and in a fair and reasonable manner	Collection of information by schools is made under the provisions of the ETA. Existing business processes for education providers to collect enrolment information will not change. In some cases schools use online enrolment forms, in other cases paper based forms completed at home or in person at school. In any case, the DI4OL service will not change this process, thereby maintaining the fair and reasonable manner that a school has chosen. Education providers are open and transparent when collecting information as to the intended purpose and use. Some education providers give specific detail (exactly which third party applications they use and thus information will be shared with, what information will be shared that is mandatory or optional, or where information sharing is entirely optional), while others provide higher level purposes for use (e.g. education purposes, communications, measuring Learner achievement, sharing with the Ministry, optional school clubs or activities). This is a decision by each education provider as to what is appropriate, fair, and reasonable for their Learners, parents and the community the operate in. Collection of information at school enrolment time will either be from parents, who are acting on behalf of their children and are able to make an informed assessment of the relevance of information sought; or from older children who may provide this information themselves. As noted under Collection of Personal Information on page 22, the information to be used by the DI4OL identity broker has been minimised and is basic. For example, the DI4OL identity broker will have no need to access information relating to parents, guardians, home address, joint custody arrangements, ethnicity, medical needs, food allergies etc. – all of which would be collected as part of enrolment at school. If for whatever reason a parent or older child does not provide the basic information at school enrolment time, then the enrolment process itself cannot complete. In terms of the Ministry collecting the required information from schools, this as a result of a school opting-in to using the DI4OL identity broker, therefore schools are actively choosing to share the information with the Ministry. Use of the DI4OL identity broker is not mandatory. It would likely be considered unreasonable or intrusive, by Learners and school principals or Boards of Trustees, if Ministry staff were to attend schools for the purposes of collecting the basic information required for the DI4OL identity broker and request this information from Learners. As well as potentially being inaccurate, prone to human error by adults unfamiliar with the Learners, and likely include double handling or processing of collected information. It would also disclose PI to individuals who have no need to know the PI, simply that they are collecting it. For these multitude of reasons, it is fair and reasonable that information is only collected once from Learners, by a teacher they are most likely familiar with, and shared by the school with the Ministry.	**Compliant**	**N/A**

IPP	Privacy Principle	Assessment against Privacy Principles	Compliance	Link to Risk
		Collection of information later in the Learner's journey, post final NCEA assessment time, will be initiated by the Learner themselves when they link a personal IdP credential to the DI4OL identity broker. The Learner is thereby opting-in to use the DI4OL identity broker themselves. This linking is in the Learner's interests, being able to access NCEA results, and will not require additional biographic information beyond the email address itself. Biographic information from the personal IdP will be verified in the linking portal to act as a soft control to confirm the personal IdP is owned by the Learner. This is consistent with existing processes for Learners registering with NZQA for an account. Linking via the DI4OL identity broker will provide an improved and more robust process for Learners to confirm their identity with NZQA and will avoid the risk that a Learner can claim (deliberately or accidentally) the NSN for another Learner with NZQA. At no point is biometric information required to be collected by education providers to enable DI4OL identity broker functionality. However, secondary schools or tertiary institutes may collect a photo of a Learner where they need to issue student ID cards used for example on public transport. This is outside the scope of DI4OL, although the existence of a photo ID card may be useful as evidence of identity in potential future scenario's relating to online NCEA assessments. No material Privacy risk was identified in relation to the manner of collection of information for the DI4OL identity broker, primarily as the existing enrolment process with schools is unchanged and no additional information is sought purely for DI4OL identity broker purposes. The collection of information from schools by the Ministry is only after a school has opt-in. Use of the DI4OL identity broker is not mandatory.		
	Protection			
IPP 5	Information should be protected from loss, unauthorised use, access and disclosure	Information collected for the DI4OL identity broker will be stored securely within the Ministry's Microsoft Azure tenancy in Australia. As noted previously, a key privacy by design principle is that information needed for the DI4OL identity broker to function has been minimised. A comprehensive security and risk review of Azure including the DI4OL identity broker will be part of the DI4OL security Certification and Accreditation (C&A) process undertaken both for pilot and production phases of DI4OL. The C&A scope includes policies, processes, procedures, and technical security controls relating to the DI4OL identity broker and obtaining assurance of the same for: 1. School Identity Providers (Google and Microsoft) 2. Applications (including NZQA assessment and Record of Achievement) 3. Personal IdPs (including as RealMe, Gmail (Google), Outlook.com (Microsoft), and iCloud (Apple)).	**Compliant**	**P-02,** **P-03,** **P-04,** **P-06**

IPP	Privacy Principle	Assessment against Privacy Principles	Compliance	Link to Risk
		In consolidating from two sets of credentials (School & NZQA) to a single school credential to access both, this may increase the potential impact if school credentials are compromised, i.e. compromise of school credentials gives access not just to school applications but now also to NZQA applications. This risk needs balancing against increased useability for the learner. Improved protections will be required, including school business processes, to ensure that school credentials are secure. This will have the associated benefit of making school systems already accessed via school credentials more secure. It is also noted there is clear evidence of credential re-use by individuals of all ages, especially as the number of credentials increases, which itself presents risks; these risks will be mitigated by single sign on. For the current PIA, additional exposure of the online assessment environment and the Record of Learning is considered outweighed by increased useability (taking mitigations into account). However, potential extension of DI4OL to other applications in future will require further assessment of this, based on the sensitivity of personal information in those applications. Per Storage of Personal Information on page 24: • Both Google and Microsoft hold ISO certifications for services provided to schools and the Ministry against ***ISO27001*** *Information Security Management System*; ***ISO27018*** *Information technology Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*; and ***ISO27701*** *Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines*. These independently audited industry standard certifications provide a significant level of assurance, above and beyond attested privacy pledges. • Both Google and Microsoft maintain SOC2 Type 2 audit reports for the services they provide to schools and the Ministry. These SOC2 reports provide the highest degree of assurance that defined processes and procedures are being correctly followed and that any deficiencies have an appropriate management plan. • Both Google and Microsoft have achieved IRAP Certification with the Australian Government. The rigour of the IRAP process exceeds the review processes typically undertaken by individual NZ Govt. Agencies, and is directly equivalent to the reviews performed by NZ's Govt Chief Digital Office (GCDO) Shared Services team of the 'as a Service' offerings made available to NZ Govt. Agencies. The Ministry will exercise control over which IdP's will be permitted to link to the DI4OL identity broker, with part of the authorisation process including a security and risk review. Standards are being developed for IdPs, SMSs, and Applications to ensure that third parties wanting to link their applications to the DI4OL identity broker do so in a consistent and suitably secure manner. As discussed further in IPP10 and IPP13, a pseudonymous identifier will be used by default instead of sharing the NSN with digital service providers. Only where a sufficiently robust use case is articulated, reviewed, and approved by the Ministry, will the actual NSN be shared with a third-party provider		

IPP	Privacy Principle	Assessment against Privacy Principles	Compliance	Link to Risk
		acting as an agent for an education provider. Digital service providers are not permitted to use the NSN for their own purposes. As use of the DI4OL identity broker will be opt-in for education providers and digital service providers, any potential security issues with applications or educational IT systems will already exist irrespective of using the DI4OL identity broker. The Ministry is not directly responsible nor accountable for the information security protections within Schools, School IT systems, third parties or their IT systems and applications. Therefore, there is an existing business and operational risk that School or third-party systems may not have equivalent or sufficient information protections despite seeking such assurances. A similar risk exists for Tertiary institutes, though given scale and the broader availability of IT support in tertiary institutes, tertiary IdP's should be more securely configured. Within the Ministry's overall digital strategy are several initiatives to help schools with their cyber security including Te Mana Tūhono, Strengthening Cyber Security and Digital Support for Kura & Schools programme, Network for Learning (N4L), Safer Technology for Schools (ST4S), Assurance Framework for Schools. Some initiatives implement preventative controls that protect information, others will implement detective or responsive controls to identify and help mitigate a security incident impacting education providers should that happen. In practical terms the responsibility will remain with Schools to implement appropriate protections and follow guidance. Comprehensive operational and business reporting is anticipated to be implemented. As part of the service management plan, operational reporting will provide assurance to Ministry stakeholders that the DI4OL identity broker is functioning correctly. Business reporting will provide Ministry and external stakeholders (including NZQA, education providers and key third-party service providers), assurance that overall service metrics are meeting objectives as well as providing an overview of service utilisation. Key security metrics will be identified and included within operational and business reporting.		
	Access and correction			
IPP 6	An individual should have access to their information	Learners will have access to a DI4OL linking portal that will allow them to view the minimal information stored within the DI4OL identity broker about them. As Learners leave school and transition to tertiary education or the workforce, Learners will continue to have access to the DI4OL identity broker through their personal (non-school) or tertiary institution credentials.	**Compliant**	**N/A**

IPP	Privacy Principle	Assessment against Privacy Principles	Compliance	Link to Risk
		The potential for information within the identity broker to become orphaned (the Learner leaves school and has not linked a personal IdP in the identity broker) exists, however the identity broker will not be storing much information about the Learner. Reporting will be in place to identify orphaned information due to school enrolment updates. If the Learner's school login has been de-activated and there is no personal IdP linked, and the Learner then wants to access their NZQA Record of Achievement, this can be achieved directly by the Learner working with NZQA. It is likely that appropriate Identity Verification steps will need to be performed to allow NZQA to confirm that the Learner attempting to access a record of achievement is not attempting to breach someone else's privacy. No material Privacy risk was identified in relation to accessing the information stored in the DI4OL identity broker.		
IPP 7	Information should be corrected if a person tells you that it is wrong	The information in the DI4OL identity broker is initially sourced from the applicable School Management System and will need updating at that source if there are any inaccuracies. Should a Learner spot that their date of birth or NSN is inaccurate, this will need updating in the source SMS to ensure accuracy of all educational records. Beyond accuracy, neither a person's DoB or NSN will change. Should a Learner change their official name the school will remain responsible for updates. The DI4OL identity broker will in the future support the ability to update information for post-school Learners, including updating their known as name, email address or linked personal IdP. Updates to an individuals official name will need to follow existing Ministry business processes and will likely involve similar action with NZQA. No material Privacy risk was identified in relation to the ability for a Learner to correct information stored about them in the DI4OL identity broker.	**Compliant**	**N/A**
	RELEVANCE AND RETENTION			
IPP 8	Personal information should be accurate, complete, up to date, relevant and not misleading before you use it	As noted for IPP7 Schools will remain responsible for ensuring that information about Learners is kept up to date in SMSs and the Ministry informed through existing business processes. It is an existing business risk that schools do not perform these updates in a timely manner, or that updates to various Ministry systems are not synchronised. Updating records within the SMS and IdP is an existing business process for schools, thus any risk that the information is not kept up to date is wider than simply the DI4OL identity broker. The Ministry and NZQA perform data quality checks with schools on a regular basis. A move to digital assessments performed during the year, rather than traditional end of year exams, will reduce the peak of data quality issues in need of remediation. Ensuring that at assessment time data quality, particularly relating to the NSN, will be good. The material aspect of keeping information up to date for DI4OL identity broker purposes is whether a Learner is enrolled with a school or not. As constraints already exist within the ENROL system to prevent a Learner being enrolled in multiple schools, there may be minor practical benefit in performing data analysis between DI4OL and	**Compliant**	**N/A**

IPP	Privacy Principle	Assessment against Privacy Principles	Compliance	Link to Risk
		ENROL systems to ensure that records are consistent. Even if inconsistencies are spotted, rectification remains the responsibility of the school and parents. The DI4OL identity broker solution is only using a minimal and necessary sub-set of information held by education providers about Learners. How education providers honour changes to preferred or official name, and how that is reflected in their logon ID's is a business process for the education provider. A Learners DoB and NSN will not change unless an error is being corrected. It is anticipated that the previously mentioned guidance document will re-iterate school obligations to ensure enrolment information held by the school and shared with the Ministry is accurate and kept up to date. And that DI4OL identity broker information accuracy is not a replacement for these existing obligations. No material Privacy risk was identified in relation to the DI4OL identity broker holding accurate information, beyond the existing risk relating to schools not keeping accurate records.		
IPP 9	Personal information should only be kept for the period for which it is required	Existing Schools Data Retention and Disposal policies set by the Ministry will apply to PI collected by schools. The purpose of the DI4OL identity broker is to enable continued access to a record of achievement for Learners throughout their lifetime, irrespective of educational provider they may obtain qualifications from. The period that the NSN and some PI may be retained in the DI4OL identity broker is therefore an individual's lifetime. During that time PI may change e.g., linked credentials, preferred or official name. IPP's 6-8 discuss the channels that a Learner can use to update their information. Data matching by the Ministry with DIA's register of Births, Deaths, and Marriages (BDM) is being used to manage 'active' NSNs within the National Student Index (NSI) system. It is anticipated that as the NSI is updated to identify an individual has deceased, any access through the DI4OL identity broker will be removed. Any checking by the Ministry will not deprovision or delete the access from personal IdP's to any education applications that had been established. The technical mechanism for implementing fraud checking has not been determined and is dependent on the BDM-NSI Approved Information Sharing Agreement (AISA). In the future when Evidence of Identity (EOI) is required to support DISTF Level of Assurance technical attributes, the DI4OL identity broker will only record that EOI has been sighted and verified, and where necessary what type of evidence this was (e.g., birth certificate, student photo ID card). A copy of the EOI will not be retained within the DI4OL identity broker, nor will the DI4OL identity broker have access to a copy of the EOI in other Ministry or School systems. Note that existing business processes for a School or the Ministry may retain a copy of EOI, for example to assist auditing of enrolment.	**Compliant**	**N/A**

IPP	Privacy Principle	Assessment against Privacy Principles	Compliance	Link to Risk
		No material Privacy risk was identified in relation to the length of time that a credential will remain active within the DI4OL identity broker.		
	Use and disclosure			
IPP 10	Personal information should only be used for the purpose for which it was collected, unless an exception applies	Analysis of this IPP is noted as Compliant, given the expected Gazetting process to authorise use of the NSN for 'online learning'. If a new Gazette notice is not published, then the NSN cannot be used by any entity for 'online learning' purposes. Beyond this, education providers already collect personal information for the purposes of enrolment and provision of education to Learners. As part of onboarding work with a school, their privacy policy and enrolment forms will be reviewed to confirm whether changes may be required to support online learning purposes. Feedback will be sought from Learners, Teachers and other stakeholders during the pilot as to whether the additional purpose for sharing information with the Ministry for 'online learning' was expected, reasonable, or whether it raises concerns. Personal information collected to enable Single Sign-On for Learners to education applications is minimised as discussed previously, while the use of the NSN is limited to specified users and for specified purposes identified in the Education and Training Act 2020, Schedule 24 Clause **1** and **4,** the Gazette *NSN Notice 2019*, and subsequent Orders in Council. Given that usage of the NSN is restricted by legislation, any potential use of the NSN outside of this explicit approval presents a possible legal risk. As noted in the analysis for IPP1, per **ETA Schedule 24 Clause 5**, a Learner may choose to voluntarily disclose their NSN if an education provider or digital service provider requests that information as a non-mandatory item. The Ministry has limited knowledge of school business processes at enrolment time outside of the procedural enrolment itself. Whether schools clearly articulate to Learners and their parents the purpose for collecting information, how much is mandatory for enrolment purposes vs. desirable for broader educational purposes, is unknown and outside the scope of this PIA. Parents may consider the information collected by schools implicitly necessary for education purposes. The basic information collected about a Learner for enrolment (name, DoB, etc.) is clearly required, with data minimisation for DI4OL identity broker purposes fitting within that basic information. Where a digital service provider is a specified user or acting as an agent for a specified user (e.g., IT provider acting for an education provider), the DI4OL identity broker may share the DoB and NSN attributes as part of the authentication data flow. By default, the DI4OL identity broker is configured to share an OIDC 'pairwise' identifier instead of the NSN itself. This will provide a unique identifier for access and linking of any future recording of achievement outside of the existing NZQA use case. Where there is no clear purpose for sharing the NSN, it will not be shared. Where a digital service provider is not a specified user or their agent, again the DI4OL identity broker	**Compliant.**	**P-05,** **P-06**

IPP	Privacy Principle	Assessment against Privacy Principles	Compliance	Link to Risk
		will not share the NSN attribute. This design decision is codified as part of the data standards and will be implemented through technical controls in the DI4OL identity broker. The DI4OL identity broker will operate with minimal human interaction required by Ministry IT administrators, thereby minimising the visibility of NSN and other PI stored in the identity broker being visible to Ministry staff who may not otherwise regularly use other Ministry systems that contain richer information about Learners. E.g., ENROL. Within the Ministry the risk of someone accessing the DI4OL identity broker to gather information about a Learner is considered low. Multiple other systems exist within the Ministry (see Collection of Personal Information on page 22) which hold more detail about a Learner. Per analysis under IPP1 and specific to the NSN itself, given that IdP technology providers and digital service providers are acting as agents for education providers, the NSN remains under the education providers accountability and authority to use as a specified user. Where education providers are connecting to digital service provider applications via the DI4OL identity broker, the NSN will not be shared by default. Where education providers are connecting directly to digital service provider applications without the DI4OL identity broker, the NSN is unlikely to be shared as it is configured as a custom attribute which the digital service provider would need to know about to even request. The Ministry currently has no visibility of whether digital service providers are collecting NSN's as part of the services they provide today. Although this is highly unlikely. Adoption of the DI4OL identity broker will enable visibility of whether this is happening and constrain digital service providers receiving the NSN in future. Outside of IdP considerations, where Microsoft, Google, SMS vendors, and others are acting as Agents for education providers in the provision of services, the use of the NSN by education providers within digital service provider IT systems is authorised and the responsibility of the education provider to manage see National Student Number (NSN): for schools – Education in New Zealand		
IPP 11	Personal information should only be disclosed for the purpose for which it was collected, unless an exception applies	Analysis of this IPP is noted as Compliant, given the expected Gazetting process to authorise use of the NSN for 'online learning'. Given the legislative context, the same risk for use of the NSN also applies to disclosure. IF a Gazette notice is not approved, then the NSN cannot be used by any entity for 'online learning' purposes. As noted above for IPP10, the identity broker will exchange information between the IdP and the application the Learner is accessing. While information contained within the identity broker is minimised, and the information exchanged is minimised, this does not prevent the application service provider from disclosing information it receives or collects. Contractual commitments to confidentiality, privacy, and adherence to the Privacy Act would be the main controls in this instance. See Addendum 1 September 2022 updates at the end of this PIA for an update on this evolving consideration.	**Compliant**	**P-05,** **P-06**

IPP	Privacy Principle	Assessment against Privacy Principles	Compliance	Link to Risk
IPP 12	Personal information may only be disclosed to a person or organisation outside of New Zealand if the person/ organisation is subject to comparable privacy safeguards to New Zealand	Under the Privacy Act 2020 s11, as confirmed by the Office of the Privacy Commissioner[12], where organisations are storing information offshore with a third-party IT supplier, the supplier is acting as the organisation's agent, so the storage of information is not considered an 'offshore disclosure'. Additionally where Microsoft, Google, SMS vendors, and others are acting as Agents for education providers in the provision of services this is the responsibility of the education providers to manage, see National Student Number (NSN): for schools – Education in New Zealand. In a DI4OL context the identity broker is hosted within Microsoft's Australian data centres, with data stored there. However, the Azure B2C service which performs processing for the identity broker is a non-regional service offered by Microsoft that cannot be geographically restricted to just being delivered within Australia[13]. What this means in practice is where an international student has returned to their home country and is accessing the NZQA Record of Achievement portal to find their NCEA results, after authentication with the IdP the processing or transit of the authentication confirmation may take place within the home country before the DI4OL identity broker service performs any validation within the identity broker data store residing in Australia. Outside of this scenario, for performance or availability purposes Microsoft may undertake similar routing or processing actions. Either scenario is entirely outside of the Ministry's ability to manage. The Azure B2C service is one of several non-regional services that has been reviewed by both Australian and New Zealand Government agencies and confirmed as being suitable to store or process information up to a Sensitive classification. Thus, in a DI4OL context this non-regional delivery does not present a greater risk. See Australian Government IRAP Certification of Azure, GCDO Certification of Azure, various NZ Govt. Agency C&A of Azure. School IdPs with Microsoft or Google have a similar 'non-geographic' delivery model. Commentary above relating to Azure B2C applies to Azure Active Directory, which is the Microsoft IdP. The Ministry's licensing agreement with Microsoft includes a provision to store school's persistent data within Australia once schools novate to the Ministry licensing agreement. Google only offers regional ring fencing for a limited sub-set of data storage at rest, i.e. not for services, with the only options being the EU and USA. Google's identity platform and access management service are globally delivered with no regional ring fencing possible. Finally, Australia is considered a privacy friendly country with privacy safeguards that currently exceed equivalent NZ safeguards. No material Privacy risk was identified in relation to the storage of DI4OL information with Microsoft, whether that is in Australia or elsewhere.	**Compliant.**	**N/A**

[12] https://privacy.org.nz/tools/knowledge-base/view/219?t=338829_455184
[13] Region availability and data residency - Azure AD B2C | Microsoft Docs

IPP	Privacy Principle	Assessment against Privacy Principles	Compliance	Link to Risk
	Identifiers			
IPP 13	Don't assign a unique identifier unless this is necessary to carry out your functions, make sure they're right and that they're protected, and don't use another agency's unique identifier instead of creating your own	The Ministry is using an existing assigned unique identifier, in this instance the National Student Number (NSN), which is necessary to ensure that a trustworthy record of achievement can be correctly associated with the individual who undertook the assessment and obtained the qualifications. If a unique identifier is required to facilitate access via the DI4OL identity broker to a third-party application, e.g. in cases where a digital service provider is Privacy focussed and does not require a real name for account creation, a unique pseudonymous identifier will be assigned and used by default to ensure that third parties are not provided with the NSN in lieu of the Learner's real name. Assignment of a unique pseudonymous identifier is privacy preserving in this case as there is no capability for even authorised/specified users of the NSN to resolve this back to an identifiable person and helps manage the risk of data aggregation by digital service providers. The creation and assignment of the NSN is authorised under the ETA. As noted previously for IPP10, the NSN will only be shared by the DI4OL identity broker where the application is operated by a specified organisation and used for specified purposes. Where the application is operated by a non-specified organisation on behalf of a specified organisation the NSN may, or may not, be shared depending upon the purpose and need. At this time the only identified purpose and business need is the NZQA use cases. Any future request to share the NSN will be considered on a case-by-case basis where there is sufficient business need articulated by education providers for each individual third-party application. By using open standards Open ID Connect (OIDC) the DI4OL identity broker will have the ability to share a pseudonymous identifier with digital service provider applications instead of the NSN. This pseudonymous identifier is configured by default to be 'pairwise' (i.e., unique to each third-party application), however it can also be configured if desired to be a 'sector identifier' (i.e., an identifier unique to the user and shared to each digital service provider). Therefore, alternatives to sharing the NSN will be available which protect the individual Learners privacy and manage the risk of data aggregation, even if an education provider makes a compelling case to use the NSN. Existing provisions within the ETA clearly identify specified users and specified purposes, with an infringement provision defined. This places strict restrictions on the use of the NSN, as well as a condition for extending the scope of any specified users or specified purposes requiring a Gazette notice. In addition to this IPP13 of the Privacy Act performs a similar controlling function, per the principle description in the left-hand column.	**Compliant**	**P-07**

Commentary on the UN Convention on the Rights of the Child (UNCRC)

Per the *Sixth Periodic Report by the Government of New Zealand* in reply to question 10, the Education and Training Act 2020 includes "*Explicit requirements for the best interests or needs of children to be taken into account at the individual level".* In the context of the DI4OL service, this can be articulated as commentary to Article 3 below;

- ○ **3 best interests of the child** – the objective of DI4OL service is in the best interests of the child, in reducing stress when undertaking exams to obtain qualifications. It is commonly accepted that qualifications have an impact on a child's sense of worth, potential in life, career paths etc. The DI4OL service supports children in achieving their potential and removing a potential impediment. As noted in the PIA, some aspects of the DI4OL service are in a child's best interests by enhancing privacy (e.g. data minimisation, pseudonymous identifiers) particularly when information is shared by a school with a third party through the DI4OL service.

Also of relevance from the *Sixth Periodic Report* in reply to 14(d), referring to the new Privacy Act 2020 "*Principle 4 of the Privacy Act 2020 requires that agencies take particular care when they are collecting information from children and young people and that they do so in a way that is fair and reasonable. This includes recognition that children's personal information merits specific protection because children may be less aware of the risks, consequences and safeguards of providing personal information."* In the context of the DI4OL service, we have included commentary under IPP4 on page 31.

Taking a very broad view of the 54 articles, the following considerations to the articles are pertinent for the DI4OL service.

- Four General Principles
  - ○ **Non-discrimination (Article 2)**
  - ○ **Best interest of the child (Article 3)**
  - ○ **Right to life survival and development (Article 6)** – explicitly not pertinent to DI4OL
  - ○ **Right to be heard (Article 12)**
- Articles pertinent to DI4OL
  - ○ **2 non-discrimination** – The DI4OL service undertakes no activity nor automated decision making based on the minimal information about a child that the DI4OL service holds. While information is held about a child's name, which could infer ethnicity or gender, and identifying a child's school, which could infer socioeconomic status based on school decile or equity index rank, no such inferences are made.
  - ○ In the future if the DI4OL service is made available to primary schools, automated restrictions may be implemented based on a child's age (inferred by class year in the case of composite schools), to ensure that content restrictions based on age are honoured. Schools should be honouring any age-based restrictions already, with the DI4OL service being able to provide a check and balance to existing school processes. Per Articles 3 and 17(e), in this case age-based discrimination is in the best interests of the child to protect them from inappropriate content.
  - ○ **3 best interests of the child** – As noted above, the objective of the DI4OL service is in the best interests of the child, in reducing stress when undertaking exams to obtain qualifications. And in ensuring continued access to their Record of Learning. It is commonly accepted that qualifications have an impact on a child's sense of worth, potential in life, career paths etc. DI4OL supports children in achieving their potential and being able to demonstrate their achievements to potential employers or Tertiary education providers.
  - ○ **12 right to be heard** – though the main context of this right is in legal proceedings, the right also relates to holding views. Which may include consent, or declining consent, to information being shared. In a DI4OL context, consent to use the DI4OL service needs to be obtained from the child by their schools. Where consent is not given then it would be for the school to work with the child, and their parents as appropriate, to understand the concerns to address

them. The Ministry will support schools in this awareness and education aspect by providing information to schools that can be used as part of any discussion about consenting to use the DI4OL service.

- **16 right to privacy** – Noting commentary about article 12 in relation to consent, the DI4OL service makes no interference upon a child's Privacy. As noted in the PIA, some aspects of the DI4OL service are privacy enhancing (e.g. data minimisation, pseudonymous identifiers) particularly when information is shared by a school with a third party through the DI4OL service.
- **28 right to education** – broadly speaking various digital technologies are making mainstream education more accessible to children with learning support needs, or to children who are unable to participate directly in traditional in-school education for short or extended durations. While the DI4OL service does not directly contribute to this, the Ministry's delivery of DI4OL as a free service to schools is in alignment with State Parties obligations to provide free education. Similarly while the DI4OL service does not directly contribute to access to higher education, reducing stress during exam time and ensuring accessibility to their record of achievement supports a child's achievement and potential entry to higher education.
- **36 other forms of exploitation** – this article is very broad. As noted elsewhere in this PIA, through the overall Privacy by Design process consideration has been given to the potential risks and issues in collecting even a minimal set of information about Learners. The inclusion of the NSN as an authoritative government issued unique identifier. The risks of data analytics, particularly those targeting children. The DI4OL identity broker will implement a high level of information security and privacy controls, and may identify instances where schools may be sharing information with digital services providers that is not strictly necessary, or digital service providers may be collecting information that is again not strictly necessary.

Assessment Part 3 – Risk Assessment

The Ministry has an established Risk Assessment Methodology that must be used to assess privacy risks. The outcome of the risk assessment process is documented in Table 4 below. Controls applicable to every Privacy risk are identified after Table 4 in Table 5 on page 52 to avoid duplication within Table 4. More detailed information about the Risk Assessment Methodology can be found in Appendix 2. Control Catalogue references are drawn from the Ministry's information security controls catalogue.

Table 4 Privacy risk assessment

Risk ID	Risk Description	Likelihood	Impact	Rating	Control Recommendations and Privacy Response	Likelihood	Impact	Rating	Rationale
P-01	Excessive items of PI are collected for no clear purpose, or without the knowledge of the individual. Potential breach of Privacy Act Principle IPP1	Possible	Medium	Moderate	**CPL-01** Due Diligence - Ministry expectations for Assurance reporting to be articulated and a framework established to enable reporting. Including RACI matrix to clarify shared responsibility obligations. **GOV-01** Compliance requirements - Ministry information security and Privacy requirements and recommendations to be articulated to other parties, to be embedded in contracts if possible (**TPM-08** SLAs and Contracts). **HRS-03** Advice and guidance is provided to School Board, Teachers, staff, as to their responsibilities for Privacy and Security of school information and systems. **IAC-15** User Account Lifecycle Management – Identity idle accounts, disable them, and define re-authorisation process. **IAO-05** Digital service providers will be reviewed against criteria (specifics of which are TBD), before being permitted to connect to the DI4OL identity broker. **IAO-05** An assurance plan applicable to schools (incl. school IdPs), and for digital service providers will be developed. **IRO-09** A full change and communications plan is being developed to ensure that all stakeholders are informed about the DI4OL identity broker. Awareness raising communications will also be conducted with peak bodies.	Possible	Minor	Low	PI consumed by DI4OL is already part of enrolment PI collection. Purpose, as supported by existing *NSN Notice 2019* and planned Gazette update is clear. Connection approval criteria, along with ongoing assurance will be developed to maintain trust in the DI4OL ecosystem. Pilot will be used to confirm schools Privacy respecting practices, and the transparency of communications provided by the Ministry and schools with parents and Learners.

P-01					**PRI-01 & PRI-02** Schools have existing Privacy policies, these may need updating in line with the new 'online learning' purpose. The pilot school's enrolment forms and Privacy policies will be reviewed to assess whether further guidance from the Ministry to schools may be needed as a result of the planned Gazette notice and before DI4OL goes into production rollout. **PRI-01.5** Existing controls on the specified users and specified purposes for using the NSN within the Education and Training Act are a major factor here. Offences relating to use of the NSN are specified in the ETA §661. **PRI-01.6** Data collection and use minimisation is a key 'privacy by design' principle for the DI4OL identity broker. **PRI-05** Retention requirements – agree an approach to retaining PI in a 'lifelong learning' context. **PRI-06** Personal information permission – the Learner has access to review and update information stored about them in the DI4OL identity broker linking portal.				The Ministry is responsible to ensure the NSN is not disclosed counter to ETA. This is implemented through Policy, Procedural, and technical controls within the DI4OL identity broker.
P-08	Schools may not be transparent with Learners or their parents on the detail of the purpose for collecting information, or the detail of what information is shared with the Ministry for specific purposes. Resulting in a Privacy complaint being raised. Potential breach of Privacy Act Principle IPP3	Possible	Minor	Low	**HRS-03** Advice and guidance is provided to School Board, Teachers, staff, as to their responsibilities for Privacy and Security of school information and systems. **IRO-09** A full change and communications plan is being developed to ensure that all stakeholders are informed about the DI4OL identity broker. Awareness raising communications will also be conducted with peak bodies. **PRI-01 & PRI-02** Schools have existing Privacy policies, these may need updating in line with the new 'online learning' purpose. The pilot school's enrolment forms and Privacy policies will be reviewed to assess whether further guidance from the Ministry to schools may be needed as a result of the planned Gazette notice and before DI4OL goes into production rollout. **PRI-01.6** Data collection and use minimisation is a key 'privacy by design' principle for the DI4OL identity broker. **PRI-04** Collection of PI from older children is for identified purposes	Unlikely	Minor	Very Low	This risk is an iteration of P-01 in terms of knowledge of the individual and being more about transparency by the school. HRS-03 is also tangentially applicable in terms of raising awareness with Learners and Parents who may then ask questions of schools.

P-09	Schools may not be transparent with Learners or their parents on the detail of the purpose for collecting information, or the detail of what information is shared with the Ministry for specific purposes. An individual feels that their Privacy rights have been infringed. Potential breach of Privacy Act Principle IPP3	Almost Certain	Minor	Moderate	**HRS-03** Advice and guidance is provided to School Board, Teachers, staff, as to their responsibilities for Privacy and Security of school information and systems. **IRO-09** A full change and communications plan is being developed to ensure that all stakeholders are informed about the DI4OL identity broker. Awareness raising communications will also be conducted with peak bodies. **PRI-01 & PRI-02** Schools have existing Privacy policies, these may need updating in line with the new 'online learning' purpose. The pilot school's enrolment forms and Privacy policies will be reviewed to assess whether further guidance from the Ministry to schools may be needed as a result of the planned Gazette notice and before DI4OL goes into production rollout. **PRI-01.6** Data collection and use minimisation is a key 'privacy by design' principle for the DI4OL identity broker. **PRI-04** Collection of PI from older children is for identified purposes	Likely	Minor	Low	This risk is an iteration of P-08 in terms of effect for an individual and caused by a lack of transparency or detail by the school when seeking consent from an individual. HRS-03 is also tangentially applicable in terms of raising awareness with Learners and Parents who may then ask questions of schools.

Risk ID	Risk Description	Likelihood	Impact	Rating	Control Recommendations and Privacy Response	Likelihood	Impact	Rating	Rationale
P-02	The DI4OL solution does not implement effective or sufficient safeguards to ensure the security of PI stored within the DI4OL identity broker. PI is disclosed, the Privacy of multiple individuals is breached though without serious harm. Potential breach of Privacy Act Principles IPP5	Rare	Medium	Low	**CHG-02** Configuration management – integral with change control will be technical configurations implemented to prevent sharing of PI or the NSN except where configured, tested and approved. **CRY-03** Transport Layer Security – all data is encrypted in transit between the DI4OL identity broker and external connections, and within the DI4OL identity broker service itself. **CRY-05.1** Storage data security – all information and data is encrypted at rest and in storage. **DCH-03.1** Sharing a pseudonymous identifier unique to each application, thus not sharing the NSN, prevents the NSN from being used as an authoritative unique identifier across applications, vendors, or longitudinally over time. **GOV-03** Information security reviews – NZQA will undertake an independent review of DI4OL C&A artefacts to ensure that they meet NZQA's requirements and expectations. It is anticipated that part of this NZQA review will include a review by an independent security consulting organisation. Both organisations will be considering the reliance of assurance that can be placed on the Ministry's work. In addition, the DI4OL project will engage an independent auditor to perform Technical Quality Assurance (TQA) and IQA. **IAC-06** Multi Factor Authentication (MFA) – All Ministry administrative users will be required to use MFA. **IAC-08** Role Based Access Control – Ministry access to the DI4OL identity broker will be limited to privileged administrators only. Other than Learners, there will be no standard user access. **IAC-15** User Account Lifecycle Management – Identity idle accounts, disable them, and define re-authorisation process. **IAO-05** An operational assurance plan for the DI4OL service, referencing external assurance frameworks will be developed.	Rare	Medium	Low	Residual risk considers the DI4OL solution itself. Impact is driven by potential extent of unintended disclosure by Ministry and need for reporting of potential privacy breach to OPC. Ministry's ESL is built on Azure B2C, information security review of ESL will inform controls applicable to DI4OL identity broker instance of B2C.

					MON-02 Logging and Auditing – the DI4OL identity broker will implement full logging of all system and user events. These logs will be fed in to monitoring and alerting tools. **MON-02.3** System monitoring and alerting – the identity broker will be monitored, and alerts generated using existing Ministry tools. **MON-02.3** Security Incident and Event Management (SIEM) – in addition to creation of anomaly reporting criteria within the Ministry SIEM solution, operational and business reporting will be defined. This reporting will include reports on idle accounts. **OPS-03** Service Management RACI & SoPs to be established. **PRI-05** Retention requirements – agree an approach to retaining PI in a 'lifelong learning' context.				
P-03	There is an existing business risk that Schools have ineffective or insufficient safeguards implemented to ensure the security of PI stored within School IT systems, third party IT systems that Schools use and configure. Significant quantities of PI, or sensitive PI, could be disclosed, including photos of children, the Privacy of multiple individuals is breached potentially causing serious harm to some. Potential breach of Privacy Act Principles IPP5	Possible	Medium	Moderate	**CPL-01** Due Diligence - Ministry expectations for Assurance reporting to be articulated and a framework established to enable reporting. Including RACI matrix to clarify shared responsibility obligations. **CPL-01** Due Diligence – The Ministry will perform Assurance reviews of Google and Microsoft as school IdP vendors to ensure they meet Ministry expectations. **GOV-01** Compliance requirements - Ministry information security and Privacy requirements and recommendations to be articulated to other parties, to be embedded in contracts if possible (**TPM-08** SLAs and Contracts). **HRS-03** Advice and guidance is provided to School Board, Teachers, staff, as to their responsibilities for Privacy and Security of school information and systems. **IAC-06** Multi Factor Authentication (MFA) – The Ministry will recommend that all school administrative users with access to manage their IdP should be required to use MFA. **IAC-15** User Account Lifecycle Management – the Strengthening Cyber Security and Digital Support for Kura & Schools programme is undertaking discovery work with Google and Microsoft to establish IdP configuration and management	Possible	Medium	Moderate	Impact is driven by potential extent of unintended disclosure and need for reporting of potential privacy breach to OPC. Despite controls, impact of the event is still Medium, likelihood remains as Possible given there are ~2,500 schools. Consolidating access to multiple services through one account (the school account) would potentially increase the extent of impact should the school account credentials be compromised. However the material impact (severity) is not increased by DI4OL since the risk of breaching school IT systems already exists. Providing broad privacy and security guidance to education providers to increase awareness of obligations and improve practices was identified in the RIS

					recommendations for schools. In a DI4OL context this will include data integrity and quality checks (**PRI-10**). **IRO-09** A full change and communications plan is being developed to ensure that all stakeholders are informed about the DI4OL identity broker. Awareness raising communications will also be conducted with peak bodies. **SAT-02** security awareness training – Ministry Strengthening Cyber Security and Digital Support for Kura & Schools programme has a specific workstream for awareness raising within the education sector. **SAT-02** There is extensive engagement in the education sector from NZ organisations such as Netsafe, NZ Police, OPC, CERT NZ on basic cyber security and privacy awareness applicable to children. This is in addition to similar engagement from international organisations such as Apple, Facebook, Google, Microsoft etc.				as a key control. The Ministry's Strengthening Cyber Security and Digital Support for Kura & Schools programme of work has this as a core objective, and it is outside of the DI4OL project's scope to broadly address school cyber security. DI4OL reduces some risk due to reducing manual administration and risk of human error.
Further rationale for P-03: The Ministry has no visibility of the configuration of school IdPs and associated business practices, nor any operational visibility of logging and monitoring tools for school IdPs. This constrains what the Ministry can do through centralised tools to help schools or further specific advice that can be provided. Additional work is being performed under the Te Rito program, focussed on SMS' and associated information security and privacy practices of SMS vendors.									
P-04	There is an existing risk that individual may have ineffective or insufficient safeguards implemented on their Personal credentials, to ensure the security of their Personal IdP, or any information they store in the account. Potential breach of Privacy Act Principles IPP5, with the personal IdP providers being held accountable.	Possible	Minor	Low	**CPL-01** Due Diligence – The Ministry will perform Assurance reviews of the identified personal IdP vendors to ensure they meet Ministry expectations. **HRS-03** Individuals are provided guidance by IdP vendors in ensuring the security of their Personal IdP and account information. **MON-02.3** Security Incident and Event Management (SIEM) – in addition to creation of anomaly reporting criteria within the Ministry SIEM solution, operational and business reporting will be defined. **SAT-02** There is extensive public engagement from NZ organisations such as Netsafe, CERT NZ, NCSC, NZ Police on basic cyber security. There is a 'Cyber Safe' week. This is in addition to similar engagement from international organisations such as Apple, Facebook, Google, Microsoft etc.	Possible	Minor	Low	This risk is for individuals to manage themselves, and in their choice of personal IdP. It is unlikely that any additional communications from schools or the Ministry, above and beyond what is already communicated, will make a material difference. Schools have additional controls that can be implemented for school accounts that are not necessarily available on equivalent consumer (Personal) IdPs.

P-05	Personal information is used or disclosed by the DI4OL identity broker outside of the specified legal purpose for which it was collected. Specifically, the NSN is used by non-specified users or for non-specified purposes. Limited or non-identifying PI of many individuals is disclosed, the Privacy of many individuals is breached though without serious harm. Potential breach of Privacy Act Principles IPP10, 11. Potential breach of Education and Training Act Schedule 24.	Rare	Medium	Low	**CHG-01** Change control – Change control, approvals processes, pre-deployment testing as per normal Ministry processes will be implemented to minimise inadvertent misconfiguration. **CHG-02** Configuration management – integral with change control will be technical configurations (aka authentication policy scope) implemented to prevent sharing of PI or the NSN except where configured, tested and approved. **IAC-08** Role Based Access Control – Ministry access to the DI4OL identity broker will be limited to privileged administrators only. Other than Learners, there will be no standard user access. **IAO-05** An operational assurance plan for the DI4OL service, referencing external assurance frameworks will be developed. **IAO-05** Digital service providers will be reviewed against criteria (specifics of which are TBD), before being permitted to connect to the DI4OL identity broker. Effort will focus on digital education providers prioritised by extent and frequency of use across the education sector by Learners and Schools, volume of PI involved, other factors may be included. **MON-02.3** System monitoring and alerting – the identity broker will be monitored, and alerts generated to existing Ministry tools. **MON-02.3** Security Incident and Event Management (SIEM) – in addition to creation of anomaly reporting criteria within the Ministry SIEM solution, operational and business reporting will be defined. **OPS-03** Service Management RACI & SoPs to be established. **PRI-01.5** The Ministry is responsible to ensure the NSN is not disclosed counter to ETA. This is implemented through Policy, Procedural, and technical controls within the DI4OL identity broker. **PRI-05** Retention requirements – agree an approach to retaining PI in a 'lifelong learning' context.	Rare	Medium	Low	Impact is driven by potential volume of disclosure by Ministry and need for reporting of potential privacy breach to OPC.

P-06	Personal information is used or disclosed by education providers, or their authorised IdP or digital service providers, outside of the specified legal purpose for which it was collected. Specifically, the NSN is used by non-specified users or for non-specified purposes. Limited PI of several individuals is disclosed, the Privacy of several individuals is breached though without serious harm. Potential breach of Privacy Act Principles IPP10, 11. Potential breach of Education and Training Act Schedule 24.	Unlikely	Medium	Low	**CHG-02** Configuration management – integral with change control will be technical configurations (aka authentication policy scope) implemented to prevent sharing of PI or the NSN except where configured, tested and approved. Plus 'pair wise' identifiers to prevent NSN being used as an index for aggregation. **CPL-01** Due Diligence - Ministry expectations for Assurance reporting to be articulated and a framework established to enable reporting. Including RACI matrix to clarify shared responsibility obligations. **GOV-01** Compliance requirements - Ministry information security and Privacy requirements and recommendations to be articulated to other parties, to be embedded in contracts if possible (**TPM-08** SLAs and Contracts). **HRS-03** Advice and guidance is provided to School Board, Teachers, staff, as to their responsibilities for Privacy and Security of school information and systems. **IRO-09** A full change and communications plan is being developed to ensure that all stakeholders are informed about the DI4OL identity broker. Awareness raising communications will also be conducted with peak bodies. **OPS-03** Service Management RACI & SoPs to be established. **PRI-01.5** Existing controls on the specified users and specified purposes for using the NSN within the Education and Training Act are a major factor here. Offences relating to use of the NSN are specified in the ETA §661. The need to Gazette the intended use of the NSN for 'online learning' purposes provides a control point consistent with IPP13 and the ETA in limiting both specified users and specified purposes. Applicability of any Conditions or Restrictions in new Gazette notice. **PRI-05** Retention requirements – agree an approach to retaining PI in a 'lifelong learning' context.	Rare	Medium	Low	This was highlighted in the RIS as the primary risk. Although in the 2015 NSN PIA (R6) was one of a number that were rated as low. Technical configuration control – custom attribute of NSN is difficult for IT administrator to find. Isn't part of default authentication policy scope. Gazette notice or guidance to schools should include clear articulation of the difference between a third-party provider acting as an agent for an education provider, and when acting for the third-party providers own interests with the prohibition in using the NSN.

					SAT-02 security awareness training – Ministry Strengthening Cyber Security and Digital Support for Kura & Schools programme has a specific workstream for awareness raising within the education sector.				
P-07	An individual is able to be identified from a number of aggregated or anonymised data sets, or through the NSN unique identifier. Potential breach of Privacy Act Principles IPP10, 11, 13. Potential breach of Education and Training Act Schedule 24.	Unlikely	Medium	Low	**CHG-02** Configuration management – integral with change control will be technical configurations (aka authentication policy scope) implemented to prevent sharing of PI or the NSN except where configured, tested and approved. Plus 'pair wise' identifiers to prevent NSN being used as an index for aggregation. **DCH-03.1** By sharing a pseudonymous identifier unique to each application, thus not sharing the NSN, prevents the NSN from being used as an authoritative unique identifier across applications, vendors, or longitudinally over time (**CHG-02**). **GOV-01** Compliance requirements - Ministry information security and Privacy requirements and recommendations to be articulated to other parties, to be embedded in contracts if possible (**TPM-08** SLAs and Contracts). **OPS-03** Service Management RACI & SoPs to be established. **PRI-01.5** The need to Gazette the intended use of the NSN for 'online learning' purposes provides a control point consistent with IPP13 and the ETA in limiting both specified users and specified purposes. Privacy Act IPP13 then functions as a backup control with the same effect.	Rare	Medium	Low	Use of the DI4OL identity broker is a control, as it will highlight any instances where schools and digital service providers may exchange the NSN today (as noted in IPP10 analysis), particularly if there may not be a clear purpose. Technical controls within the DI4OL identity broker will only permit NSN exchange where the Ministry implements an appropriate configuration. Recommendations can be provided to schools about which digital service providers may be more reputable than others, for example using the Safer Technology for Schools (ST4S) assessment. However, schools are under no obligation to follow Ministry recommendations. Further rationale below.

Further rationale for P-07:

The default today is that schools share the associated Learner school email address with digital service providers to enable login. This practice is unlikely to change. Although names are not necessarily unique, digital service providers may aggregate with publicly available information to identify Learners. While such activity is undesirable, there is nothing in practice the Ministry can do to prevent this.

Gazette notice or guidance to schools should include clear articulation of the difference between a third-party provider acting as an agent for an education provider, and when acting for the third-party providers own interests with the prohibition in using the NSN.

Given the size of education sector cohorts (~190k in ECE, ~850k+ in schools, ~530k in Tertiary) it would be non-trivial to identify in real life a specific individual from multiple datasets where the NSN was the only PI. This provides a degree of anonymity 'in the crowd'. Individuals are potentially able to be identified as unique, though not necessarily identify who they are, via 'fingerprinting' technology used by websites. This is a risk of using the internet, with a variety of controls available in browsers, operating systems, use of shared devices.

Access to NSI, which would resolve a pseudonymous NSN to an identifiable individual is controlled and not publicly available. Although ECEs, Schools, Tertiary institutions all have access to the NSI to perform searches for enrolment purposes, this access is limited to a few staff identified as administrators for each school. The same applies for access to ENROL, with only a few staff having access that would permit searching for an NSN. In either case, searching for an NSN not related to a Learner at their school, or seeking enrolment with their school, would by unauthorised use of authorised access.

Controls applicable to every Privacy risk are shown in Table 5 below.

Table 5 Controls applicable to every Privacy risk

PRI-01.5 Legal obligations, identified in ETA Sch 24 NSN relating to specified users and specified purposes for using the NSN are a key control. Offences relating to use of the NSN are specified in the ETA s661.	**PRI-01** Policies for information security and **PRI-02** Privacy Policy – Existing Ministry and NZQA information security and privacy policies, practices, processes, education and awareness training, applicable for all staff involved in the design, operation, and management of the end-to-end service.	**PRM-01** (Per IPP5) Within the Ministry's overall digital strategy are several initiatives to help schools with their cyber security including Te Mana Tūhono, Strengthening Cyber Security and Digital Support for Kura & Schools programme, Network for Learning (N4L), Safer Technology for Schools (ST4S).
PRI-01.6 Privacy by design inc. data minimisation, evidence checked rather than evidence retained.	**GOV-02 & PRI-07** DI4OL reduces system wide risk by implementing a consistent standards-based approach to disclosing PI to digital service providers.	**VPM-07** Security testing – Perform security testing, remediate findings to an acceptable risk level.
GOV-01 Identify compliance requirements – inc. Certification and Accreditation (C&A) of the DI4OL identity broker solution and end to end service.	**IRO-04** Incident response plan – Ministry incident response plans cater for information security and privacy incidents, including escalation, communications, notification to effected parties.	**GOV-03** Information security reviews – The DI4OL project will engage an independent auditor to perform Technical Quality Assurance (TQA) and project IQA.
GOV-03 Information security reviews - Perform a risk assessment, particularly in concert with major changes of scope, solution capability etc.	**GOV-03** Information security reviews – NZQA will undertake an independent review of DI4OL C&A artefacts to ensure that they meet NZQA's requirements and expectations. It is anticipated that part of this NZQA review will include a review by an independent security consulting organisation. Both organisations will be considering the reliance of assurance that can be placed on the Ministry's work.	**IAO-05 & PRI-14** Operational Assurance Plan. In concert with the assurance requirements identified of school and personal IdPs, digital service providers, the Ministry will agree a formal assurance plan covering the end-to-end DI4OL identity broker service. Explicitly it Is the intention to assess the DI4OL service against the ST4S criteria to ensure alignment with that framework.

We will also assess the DI4OL service against the ICO age appropriate design code to ensure best practice.
We will review the applicability of the US focussed Common Sense Privacy evaluation framework for aspects that may be applicable to an NZ based DI4OL service.

To enable traceability back to the *2015 NSN PIA*, a brief summary of the risks identified in that previous work and how they are reflected in the current risk assessment is provided in Appendix 5 2015 NSN PIA Risks, Privacy Responses, and Recommended Controls on page 62.

Assessment Part 4 – Data Protection and Use Policy (DPUP)

Overview of the DPUP

The DPUP describes values and behaviours that, when applied across the sector, will build trust and help to ensure that data practices are focused on the wellbeing of people and communities. These values and behaviours are represented as five Principles that have people and their wellbeing at the centre.

The focus is on relationships, rather than rules — a way of working that respects people, their information and their stories.

The Policy provides good practice guidance on how to uphold these Principles in four key areas (the Guidelines). These Guidelines help organisations to understand and apply the Privacy Act in relation to these activities. However, this Policy goes beyond solely privacy matters to also think about ethical considerations when making decisions. Good practice requires that if, and when, agencies contemplate using people's information, it's done with the involvement, understanding, and support of the people impacted by those proposals.

Assessment against Guidelines

DPUP Guidelines	Manner of compliance
Purpose Matters The vital importance of purpose to collecting and using people's personal information. Be clear about the purposes of collecting personal information, only collect what's needed, and consider how collection and use could affect people's wellbeing.	As articulated through this PIA, the purpose and objective for re-using information that is already collected by education providers is clear. The overall benefits are for Learners and Teachers wellbeing, by reducing stress at important assessment and results times. Privacy by design, including data minimisation is a key principle. Further privacy by design will minimise the ability for digital service providers to link aggregated information about Learners. In practice it is not possible to fully prevent this.
Transparency and Choice Enable people to understand what's happening with their information and what choices they have. When collecting information from people, help them understand why it's being collected, how that might help them or people in similar circumstances, and what rights they have to access and request changes. Provide them with choices whenever possible.	Use of the DI4OL identity broker remains opt-in for education providers, though not for individual Learners while at school. Post school, Learners will have the choice to continue using the DI4OL identity broker or not. Education providers will need to ensure they have consent, or knowledge, by the Learner or their parent(s) addressed by 'learning/education' purposes in their Privacy policy/statements. Learners will have choice in terms of which Personal IdP they can connect with to maintain access to their Record of Achievement, DI4OL is agnostic on which approved IdP is used. Again, this remains a benefit for Learners for lifelong learning and as they enter the workforce. Whether Learners continue to engage using the DI4OL identity broker post-secondary or tertiary education will be entirely at their discretion. The DI4OL project has conducted engagement with schools and learners to gain their initial feedback on suitability of the DI4OL identity broker solution and how they may wish to interact with it.

DPUP Guidelines	Manner of compliance
	This feedback has provided insights on their perceptions of potential benefits, as well as UX and other design considerations. Further engagement will take place during the pilot phase, which is intended to include a range of diverse schools and kura to ensure different perspective, expectations and understandings are considered prior to the planned production deployment. A formal communications plan will have multiple channels to ensure effected parties (Learners, Teachers, Schools more broadly) are informed in plain English and Te Reo Māori. We don't have a capability (yet) to support subsets of attributes, enabling Learners to choose to share only some of their PI. In an education context we have minimised data use and will further minimise data exchange with digital service provider applications to protect privacy. Ministry Privacy statements relating to the NSN, NSI, will be updated as a result of this change.
Access to Information Make it easy for people to see and request correction of their information. Help people to understand what personal information is held about them, to access it, to request correction of it and, where possible, to correct it themselves.	All Learners will have a login to the DI4OL identity broker linking portal, allowing self-service updates to the limited personal information that may change (e.g., official or preferred name, linked credentials, linked Tertiary accounts where they exist). Irrespective of this, Learners at secondary or tertiary education will retain the ability to update PI with their educational institutions directly.
Sharing Value Work together for better insights and outcomes. Work together and be inclusive to ensure that information used to create insights is relevant and usefully describes real experiences. Share insights that deliver value and improved wellbeing.	Overall, the better outcome is that Learners experience less stress at important assessment times, thereby ensuring that they are focussed on the assessment itself. The Ministry is working closely with NZQA to resolve education sector problems that Learners have to deal with, such as access to their Record of Achievement through lifelong learning. As re-use of data collected by schools is minimised, there are minimal specific insights or analytics that are anticipated. Business and operational reporting for the DI4OL identity broker may provide insights relating to DI4OL identity broker uptake, Schools IdP configuration, or third-party applications used, these will be at an organisational rather than individual level. There will be some individual posthumous value add where DI4OL identity broker accounts can be disabled based on information sharing relating to deceased persons. Thus, ensuring that a digital service provider does not compromise PI posthumously.

Assessment Part 5 – GCSB Information Classification

See ***Error! Reference source not found.*** for Policy guidelines. Per the DI4OL Information Classification memo, the DI4OL identity broker inherits the existing SENSITIVE classification of information within the ESL. This is driven by credentials stored in the ESL provide access to other systems within the Ministry that contain SENSITIVE information. Noting that for DI4OL objectively the information relating to Learners is UNCLASSIFIED, being owned by Learners and publicly available apart from the NSN.

GCSB Information rating	Information Security Requirements	Manner of Compliance
Information is classified as **SENSITIVE**	**Principles and Clearance Levels** - Information classified as RESTRICTED or SENSITIVE should be held, processed, transmitted and destroyed with discretion to make compromise highly unlikely. - Only Staff authorised by the department to access RESTRICTED or SENSITIVE levels are authorised to handle the information. This includes all staff involved with transmission, storage, and disposal.	Technical controls consistent with the NZISM requirements for SENSITIVE information are implemented to protect information in transit and at rest. The DI4OL identity broker has minimal need for manual intervention or management, thereby minimising the number of Ministry or 3rd party vendor support staff who have access. For education providers, teachers, office administrators and third-party IT providers may have access to the same information with fewer, or less effective, controls than the Ministry.
	Electronic Transmission - All RESTRICTED or SENSITIVE information transmitted across public networks within New Zealand or across any networks overseas must be encrypted using a system approved by GCSB.	Per NZISM, a minimum of TLS v1.2 will be used. Appropriate levels of cryptographic strength and algorithms/ciphers will be used.
	Electronic Storage - Electronic files (including databases) should be protected against illicit internal use or intrusion by external parties through two or more of the following mechanisms: - user challenge and authentication (username/password or digital ID/Certificate) - logging use at level of individual - firewalls and intrusion-detection systems and procedures - server authentication - OS-specific/application-specific security measures.	The DI4OL identity broker will store minimal & necessary information to enable its function. Privileged access control measures will be in place, including MFA.

GCSB Information rating	Information Security Requirements	Manner of Compliance
	Electronic Disposal - Electronic files should be disposed of in a way that makes reconstruction highly unlikely.	Information will be securely disposed of in accordance with the Ministry's Data Retention and Disposal Policy.
	Manual Transmission - **Within a single physical location**—As determined by the Chief Executive or Head of the organisation. - **Transfer between establishments within or outside New Zealand—** - May be carried by ordinary postal service or commercial courier firms, provided the envelope/package is closed and the word RESTRICTED, or SENSITIVE is not visible. - The outer envelope should be addressed to an individual by name and title. RESTRICTED/SENSITIVE mail for/from Overseas posts should be carried by diplomatic airfreight via MFAT. - The outer envelope must clearly show a return address in case delivery is unsuccessful. In some cases, due to the nature of the contents, identifying the originating department may be inappropriate and a return PO Box alone should be used.	There will be no manual transmission of information from the DI4OL identity broker.
	Manual Storage - In an office environment, RESTRICTED and SENSITIVE material should be held in a lockable storage area or cabinet. - In a storage facility, all material should be protected through controlled access to the storage areas, and through a secure physical environment	There will be no manual storage of information as part of operational functions for the DI4OL identity broker. Any design documents, operational manuals, Standard Operating Procedures etc. related to the DI4OL identity broker that need hard copies, will be stored appropriately within Ministry offices.
	Manual Disposal - RESTRICTED and SENSITIVE documents are to be disposed of or destroyed in a way that makes reconstruction highly unlikely.	Where hard copies of documents were required and can now be disposed of, existing Ministry secure disposal processes will apply.

Appendix 1 Information Privacy Principles

The Privacy Act 2020 sets out 13 information privacy Principles ("IPPs").

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

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

a) Principle 1 – purpose of collection of personal information

b) Principle 2 – source of Principle of information

c) Principle 3 – collection of information from subject

d) Principle 4 – manner of collection of personal information

e) Principle 5 – storage and security of personal information

f) Principle 6 – access to personal information

g) Principle 7 – correction of personal information

h) Principle 8 – accuracy of personal information to be checked before use

i) Principle 9 – agency not to keep personal information for longer than necessary

j) Principle 10 – limits on use of personal information

k) Principle 11 – limits on disclosure of personal information

l) Principle 12 – disclosure of personal information outside of New Zealand

m) Principle 13 – - unique identifiers.

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

Appendix 2 Ministry Risk Assessment Methodology

Risk assessment guidelines

Risks to privacy can arise in many circumstances. Collecting excessive information, using intrusive means of collection, or obtaining sensitive details in unexpected circumstances all represent risks to the individual. Unexpected or unwelcome uses or disclosure of that information, or its retention for an unduly long period, put individual privacy at risk.

The privacy impact report should identify the avoidable risks and suggest cost-effective measures to reduce them to an appropriate level. The identified risks should be assessed with no controls in place. This will provide the inherent risk rating and enable the effectiveness of the proposed controls to be assessed.

The risks of the project need to be summarised and assessed.

Impact (consequences) assessment

The qualitative scale used to assign an impact rating is presented in Risk Table 1 and Table 2 below. All impacts need to be seen in a business context and be informed by the business. Rating the impact of a risk should include a consideration of any possible knock-on effects of the consequences of the identified risks, including cascade and cumulative effects.

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

Likelihood (probability) assessment

The qualitative scale used to assign a likelihood rating is presented in Risk Table 3 below. Where information is available about the frequency of an incident in the past it should be used to determine the likelihood of the risk eventuating. However, where such information does not exist it does not necessarily mean that the likelihood of the risk eventuating is low. It may merely indicate that there are no controls in place to detect it or that the agency has not previously been exposed to the particular risk.

Risk matrix

Risk Table 4 presents a 5x4 matrix for assigning a risk rating to a risk. It is used by mapping the likelihood and impact ratings. The rating being the point where the likelihood and impact ratings intersect.

Table 1 – Impact Assessment

Security Anchor		Time	Cost	Public Confidence and Reputation	Stakeholder interest	Deliverables Quality	Business Objectives
Opportunity	Substantial	1+ years early	>$5m saving	Held as a reference point for others National media coverage	Government policy change	Steep change in deliverables and quality	Exceeds business objectives
	Major	Months early	$2m-5m saving	Business unit receives industry acknowledgement	Ministerial support	Major deliverables and quality improvements	Major contribution towards objectives
	Medium	Weeks early	$550k-$2m saving	Reputation of Business Unit enhanced	Governance board regulation	Moderate deliverables and quality Enhancement	Moderate contribution towards objectives
	Minor	Days early	<$500k saving	Public appreciation Local media coverage	Letter of support	Some deliverable and quality enhancement	Minor contribution towards objectives

Table 2 – Impact Assessment

Security Anchor		Time	Cost	Public Confidence and Reputation	Stakeholder interest	Deliverables Quality	Business Objectives
Threat	Substantial	1+ years late	>$5m saving	Significant public concern National media coverage	Commission of inquiry	Deliverables and quality do not meet requirements	Objectives unable to be achieved
	Major	Months late	$2m-5m	Loss of credibility to business unit Sustained regional media coverage	Ministerial inquiry	Deliverables and quality will be compromised	Major impact on the achievement of objectives
	Medium	Weeks late	$550k-$2m	Limited damage to reputation Local / regional media coverage	Ministerial question / 3rd party investigations	Deliverables and quality can be met with workaround required	Moderate impact on the achievement of objectives
	Minor	Days late	<$500k	Local public concern Local media coverage	Minor complaint / Official Information request	Deliverables and quality can be met with minor workaround	Minimal impact on the achievement of objectives

Table 3 – Likelihood Assessment

Description	Probability rating	Definitions
Almost certain	Greater than 90%	Event is expected to occur in the life of the project / programme / next 12 months
Likely	Greater than 60% but less than 90%	Event has a strong likelihood of occurring in the life of the project / programme / next 12 months
Possible	Greater than 30% but less than 60%	Event may occur in the life of the project / programme / next 12 months
Unlikely	Greater than 5% but less than 30%	Event should not occur in the life of the project / programme / next 12 months
Rare	Less than or equal to 5%	Event highly unlikely to occur in the life of the project / programme / next 12 months

Table 4 - Risk Matrix

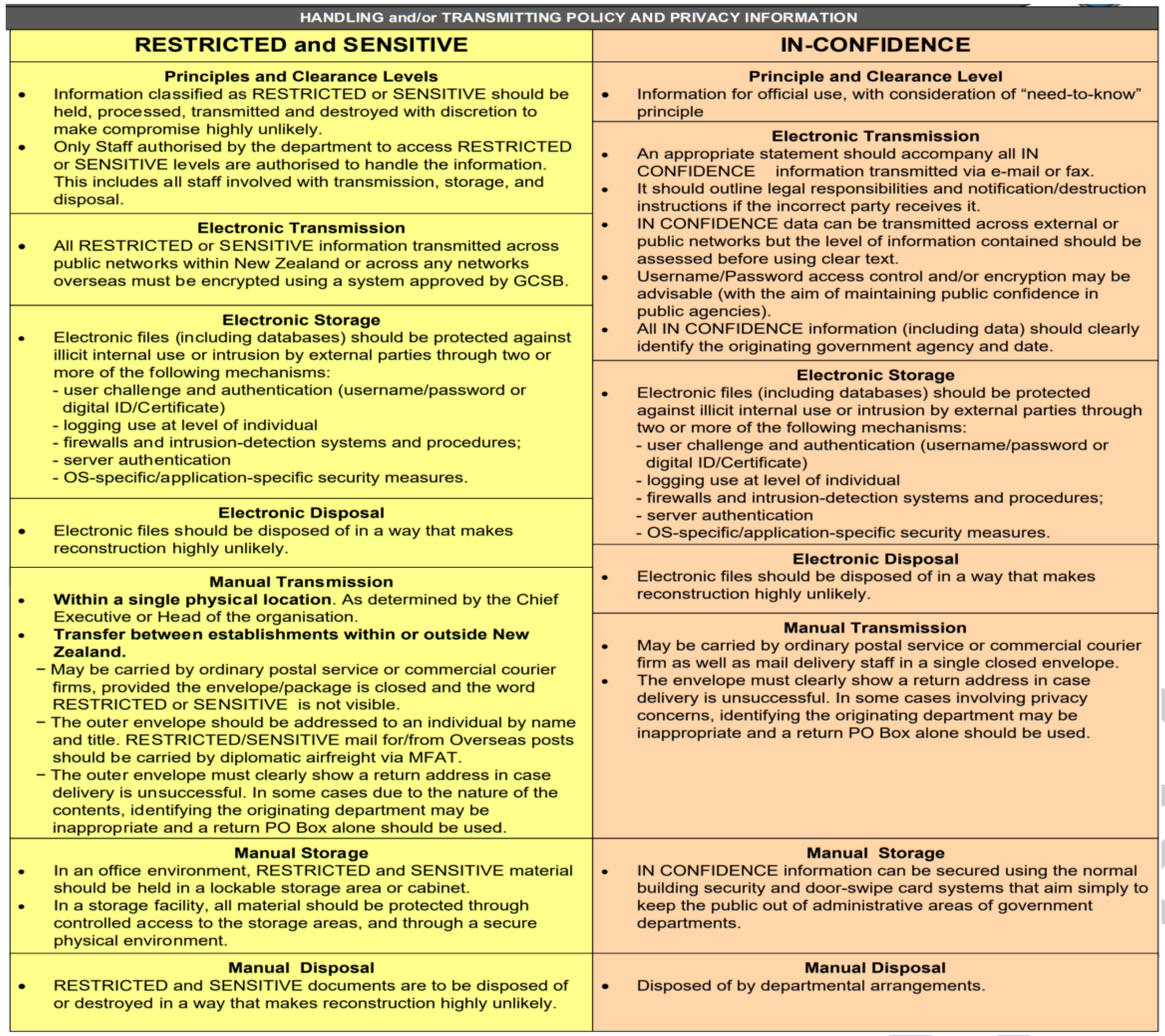
LIKELIHOOD

	Minor	Medium	Major	Substantial
Almost Certain	Moderate	High	Extreme	Extreme
Likely	Low	High	High	Extreme
Possible	Low	Moderate	High	High
Unlikely	Very Low	Low	Moderate	High
Rare	Very Low	Low	Moderate	Moderate

IMPACT

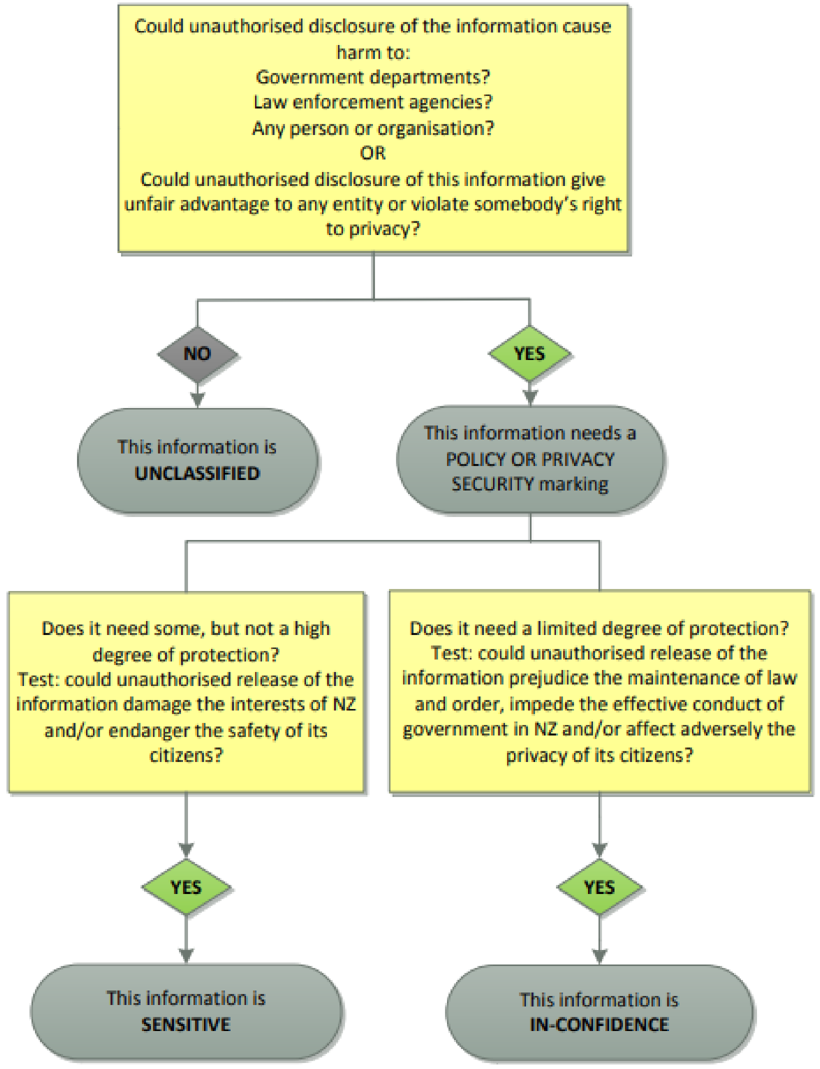
Appendix 3 Security Classification Guidelines

Use this information to complete Part 5 – GCSB Information Classification



HANDLING and/or TRANSMITTING POLICY AND PRIVACY INFORMATION

RESTRICTED and SENSITIVE	IN-CONFIDENCE
Principles and Clearance Levels • Information classified as RESTRICTED or SENSITIVE should be held, processed, transmitted and destroyed with discretion to make compromise highly unlikely. • Only Staff authorised by the department to access RESTRICTED or SENSITIVE levels are authorised to handle the information. This includes all staff involved with transmission, storage, and disposal.	**Principle and Clearance Level** • Information for official use, with consideration of "need-to-know" principle
Electronic Transmission • All RESTRICTED or SENSITIVE information transmitted across public networks within New Zealand or across any networks overseas must be encrypted using a system approved by GCSB.	**Electronic Transmission** • An appropriate statement should accompany all IN CONFIDENCE information transmitted via e-mail or fax. • It should outline legal responsibilities and notification/destruction instructions if the incorrect party receives it. • IN CONFIDENCE data can be transmitted across external or public networks but the level of information contained should be assessed before using clear text. • Username/Password access control and/or encryption may be advisable (with the aim of maintaining public confidence in public agencies). • All IN CONFIDENCE information (including data) should clearly identify the originating government agency and date.
Electronic Storage • Electronic files (including databases) should be protected against illicit internal use or intrusion by external parties through two or more of the following mechanisms: - user challenge and authentication (username/password or digital ID/Certificate) - logging use at level of individual - firewalls and intrusion-detection systems and procedures; - server authentication - OS-specific/application-specific security measures.	**Electronic Storage** • Electronic files (including databases) should be protected against illicit internal use or intrusion by external parties through two or more of the following mechanisms: - user challenge and authentication (username/password or digital ID/Certificate) - logging use at level of individual - firewalls and intrusion-detection systems and procedures; - server authentication - OS-specific/application-specific security measures.
Electronic Disposal • Electronic files should be disposed of in a way that makes reconstruction highly unlikely.	**Electronic Disposal** • Electronic files should be disposed of in a way that makes reconstruction highly unlikely.
Manual Transmission • **Within a single physical location**. As determined by the Chief Executive or Head of the organisation. • **Transfer between establishments within or outside New Zealand.** – May be carried by ordinary postal service or commercial courier firms, provided the envelope/package is closed and the word RESTRICTED or SENSITIVE is not visible. – The outer envelope should be addressed to an individual by name and title. RESTRICTED/SENSITIVE mail for/from Overseas posts should be carried by diplomatic airfreight via MFAT. – The outer envelope must clearly show a return address in case delivery is unsuccessful. In some cases due to the nature of the contents, identifying the originating department may be inappropriate and a return PO Box alone should be used.	**Manual Transmission** • May be carried by ordinary postal service or commercial courier firm as well as mail delivery staff in a single closed envelope. • The envelope must clearly show a return address in case delivery is unsuccessful. In some cases involving privacy concerns, identifying the originating department may be inappropriate and a return PO Box alone should be used.
Manual Storage • In an office environment, RESTRICTED and SENSITIVE material should be held in a lockable storage area or cabinet. • In a storage facility, all material should be protected through controlled access to the storage areas, and through a secure physical environment.	**Manual Storage** • IN CONFIDENCE information can be secured using the normal building security and door-swipe card systems that aim simply to keep the public out of administrative areas of government departments.
Manual Disposal • RESTRICTED and SENSITIVE documents are to be disposed of or destroyed in a way that makes reconstruction highly unlikely.	**Manual Disposal** • Disposed of by departmental arrangements.



Could unauthorised disclosure of the information cause harm to:
Government departments?
Law enforcement agencies?
Any person or organisation?
OR
Could unauthorised disclosure of this information give unfair advantage to any entity or violate somebody's right to privacy?

This information is UNCLASSIFIED

This information needs a POLICY OR PRIVACY SECURITY marking

Does it need some, but not a high degree of protection?
Test: could unauthorised release of the information damage the interests of NZ and/or endanger the safety of its citizens?

Does it need a limited degree of protection?
Test: could unauthorised release of the information prejudice the maintenance of law and order, impede the effective conduct of government in NZ and/or affect adversely the privacy of its citizens?

This information is SENSITIVE

This information is IN-CONFIDENCE

Appendix 4 Full DI4OL data flow diagram

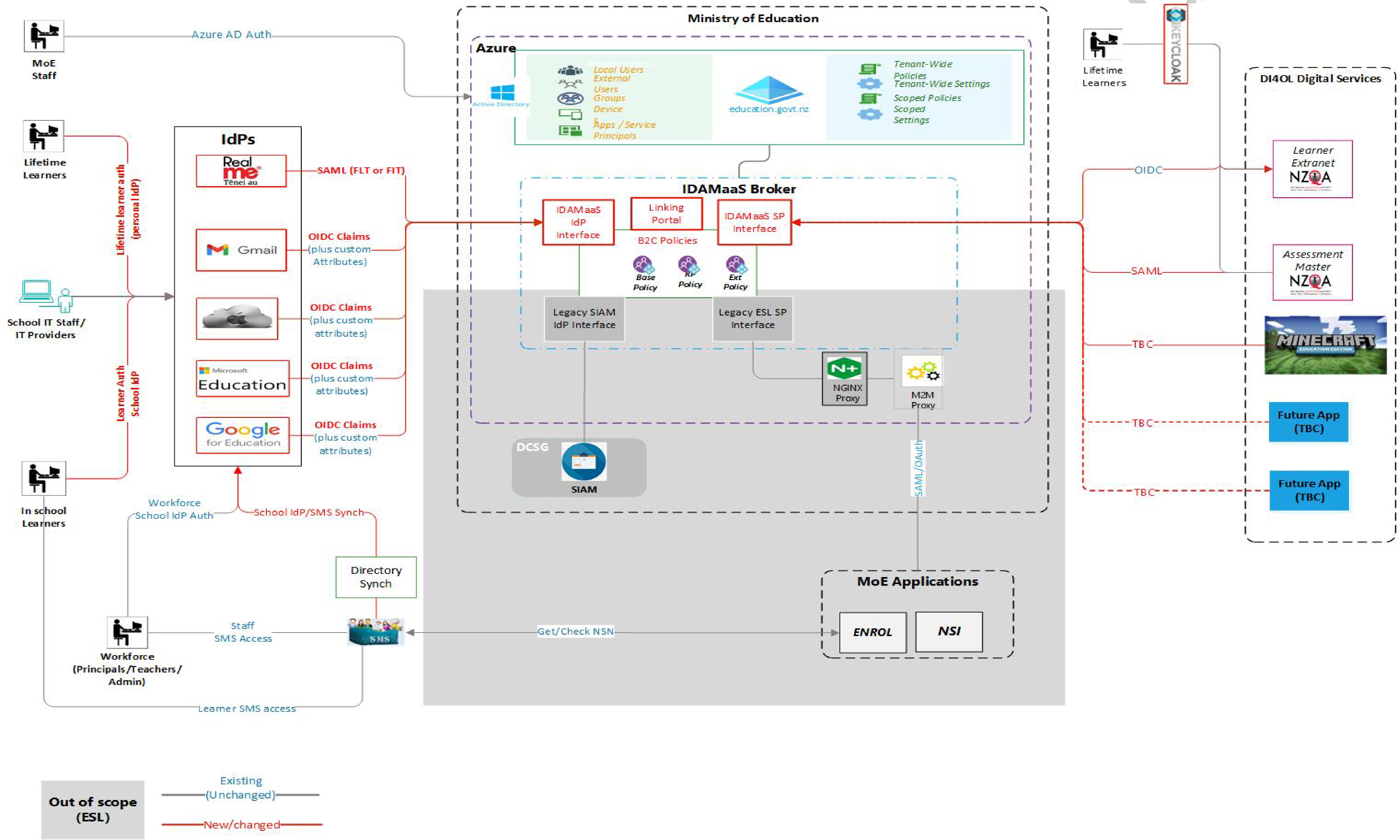
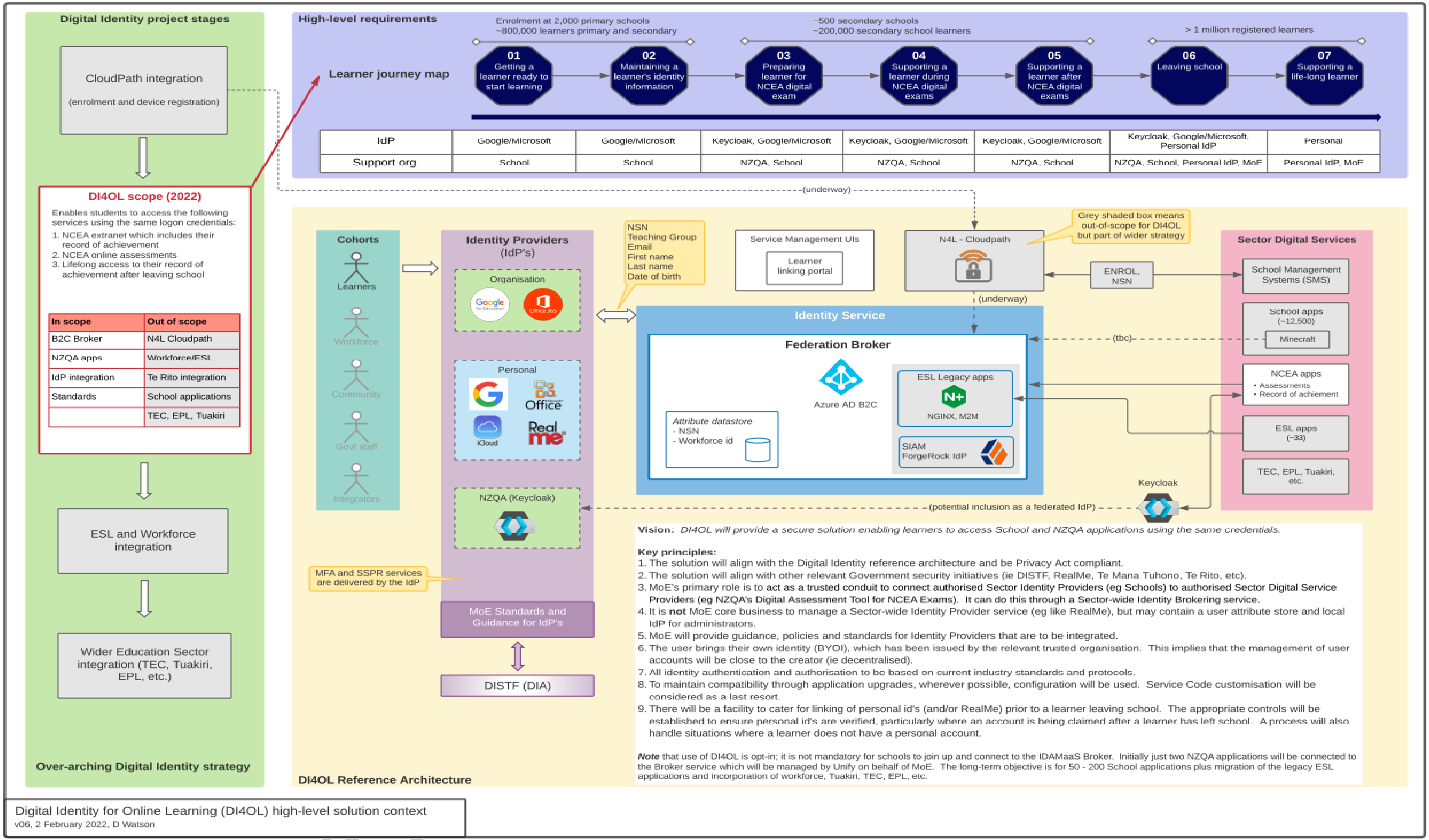


Figure 7 DI4OL full data flow diagram

The greyed-out box in the middle represents the ESL service, which is not part of the DI4OL identity broker. It is included to illustrate possible future integrations.

Figure 1 is repeated below from page 16 to provide a larger diagram to view.



Digital Identity project stages
CloudPath integration
(enrolment and device registration)

DI4OL scope (2022)

Enables students to access the following services using the same logon credentials:

1. NCEA extranet which includes their record of achievement
2. NCEA online assessments
3. Lifelong access to their record of achievement after leaving school

In scope	Out of scope
B2C Broker	N4L Cloudpath
NZQA apps	Workforce/ESL
IdP integration	Te Rito integration
Standards	School applications
	TEC, EPL, Tuakiri

ESL and Workforce integration
Wider Education Sector integration (TEC, Tuakiri, EPL, etc.)
Over-arching Digital Identity strategy
High-level requirements
Learner journey map
Enrolment at 2,000 primary schools
~800,000 learners primary and secondary
~500 secondary schools
~200,000 secondary school learners
> 1 million registered learners
01 Getting a learner ready to start learning
02 Maintaining a learner's identity information
03 Preparing learner for NCEA digital exam
04 Supporting a learner during NCEA digital exams
05 Supporting a learner after NCEA digital exams
06 Leaving school
07 Supporting a life-long learner

IdP	Google/Microsoft	Google/Microsoft	Keycloak, Google/Microsoft	Keycloak, Google/Microsoft	Keycloak, Google/Microsoft	Keycloak, Google/Microsoft, Personal IdP	Personal
Support org.	School	School	NZQA, School	NZQA, School	NZQA, School	NZQA, School, Personal IdP, MoE	Personal IdP, MoE

Vision: *DI4OL will provide a secure solution enabling learners to access School and NZQA applications using the same credentials.*

Key principles:

1. The solution will align with the Digital Identity reference architecture and be Privacy Act compliant.
2. The solution will align with other relevant Government security initiatives (ie DISTF, RealMe, Te Mana Tuhono, Te Rito, etc).
3. MoE's primary role is to act as a trusted conduit to connect authorised Sector Identity Providers (eg Schools) to authorised Sector Digital Service Providers (eg NZQA's Digital Assessment Tool for NCEA Exams). It can do this through a Sector-wide Identity Brokering service.
4. It is **not** MoE core business to manage a Sector-wide Identity Provider service (eg like RealMe), but may contain a user attribute store and local IdP for administrators.
5. MoE will provide guidance, policies and standards for Identity Providers that are to be integrated.
6. The user brings their own identity (BYOI), which has been issued by the relevant trusted organisation. This implies that the management of user accounts will be close to the creator (ie decentralised).
7. All identity authentication and authorisation to be based on current industry standards and protocols.
8. To maintain compatibility through application upgrades, wherever possible, configuration will be used. Service Code customisation will be considered as a last resort.
9. There will be a facility to cater for linking of personal id's (and/or RealMe) prior to a learner leaving school. The appropriate controls will be established to ensure personal id's are verified, particularly where an account is being claimed after a learner has left school. A process will also handle situations where a learner does not have a personal account.

Note that use of DI4OL is opt-in; it is not mandatory for schools to join up and connect to the IDAMaaS Broker. Initially just two NZQA applications will be connected to the Broker service which will be managed by Unify on behalf of MoE. The long-term objective is for 50 - 200 School applications plus migration of the legacy ESL applications and incorporation of workforce, Tuakiri, TEC, EPL, etc.

Digital Identity for Online Learning (DI4OL) high-level solution context
v06, 2 February 2022, D Watson

Figure 8 DI4OL Business Context view (A3 size)

Appendix 5 2015 NSN PIA Risks, Privacy Responses, and Recommended Controls

To enable traceability back to the *2015 NSN PIA*, a summary of the risks identified in that previous work and how they are reflected in the current risk assessment is provided in Table 6 below. Risks R1-R7 were specific to the proposal to use the NSN as part of digital identity. Risks R8-R26 related to the establishment of an education digital identity solution whether or not the NSN was included. In the past seven years the legislative context for digital identity has changed and will change further with the anticipated DISTF. Similarly, the Ministry's planned approach to delivering digital identity has changed. Therefore, not all the previously identified risks remain relevant, nor do all the previously recommended controls remain applicable to the current DI4OL identity broker. Although arrived at separately, it is noteworthy that the key risks articulated in the Executive Summary of the *2015 NSN PIA* are the key risks identified in this current PIA.

Table 6 2015 PIA risk assessment cross reference to 2022 PIA risk assessment

2015 Risk Id	2015 cross ref to IPP	2015 Risk Summary	2015 anticipated residual risk[14]	2022 PIA Risk x-ref	2022 Commentary
R1	5	Education providers IT provider discloses NSN or other PI.	Moderate	P-03, 06	Identified risk, use of the DI4OL identity broker as part of the data flow can mitigate some of this risk. Identified in 2015 NSN PIA as a key risk.
R2	10	Education providers IT provider uses NSN or other PI for unspecified / unapproved purposes.	Moderate	P-01, 06	As noted previously the ETA places restrictions on use of the NSN, and the Privacy Act guides use of PI more broadly. Identified in 2015 NSN PIA as a key risk.
R3	5	Aggregation of all identity credentials in one place is risky.	Moderate	n/a	This risk exists for each individual education providers instance of an IdP, irrespective of any aggregation taking place, see R7. The DI4OL identity broker will not store authentication credentials, mitigating the DI4OL risk.
R4	9	Excessive retention of PI for 'lifelong learning' purposes may not meet individual expectations for PI disposal.	Low	P-02	Derivative of R8.
R5	10	Future function creep, or de facto national identity number.	Moderate	P-01, 07	Scope creep is identified as potential risk under P-01. As noted previously the ETA places restrictions on use of the NSN, and the Privacy Act places restrictions on the use of unique identifiers. Identified in 2015 NSN PIA as a key risk.
R6	10	Education providers use NSN and other PI for other (unapproved) purposes.	Low	P-06, 07	Derivative of R2. As noted previously the ETA places restrictions on use of the NSN, and the Privacy Act guides use of PI more broadly.

[14] The Ministry's risk management taxonomy has been updated since 2015, level of risk has been translated to current 2022 terminology. See Appendix 2 Ministry Risk Assessment Methodology

2015 Risk Id	2015 cross ref to IPP	2015 Risk Summary	2015 anticipated residual risk[14]	2022 PIA Risk x-ref	2022 Commentary
					Identified in the RIS as the primary risk. Identified in 2015 NSN PIA as a key risk.
R7	5	Decentralisation of identity information in multiple IdP instances is risky.	Moderate	P-02, 03, 06	This is an existing business risk for each individual education providers instance of an IdP. Identified in 2015 NSN PIA as a key risk.
R8	3	Purpose for collecting and using PI is not made clear.	Low	P-01, 08	Identified risk for the additional 'online learning' context.
R9	3	PI is exchanged with a third party without having sought prior express consent.	Very Low	P-01, 06, 08	Related to R1, R6.
R10	5	Third party providers do not implement sufficient information security protections, Ministry requirements are not articulated, assurance from providers is not obtained.	Moderate	P-02, 04, 06	Identified as a broad risk relating to IPP5. R10 is an umbrella risk that could cover R1, R2, R5, R9, R13, R14, R16, R19, R20, R21, R23.
R11	5	Learner credentials are shared with, or known by, teachers, parents. This leads to credential compromise.	Moderate	P-03, 04	As noted under P-04 in Table 4, there are multiple sources of advice seeking to mitigate this issue.
R12	5	Trivial passwords are used, or passwords are re-used across multiple personal accounts.	Low	P-03, 04	As noted under P-04 in Table 4, there are multiple sources of advice seeking to mitigate this issue.
R13	5	Accounts may be compromised via a fraudulent password reset due to poor identity verification processes when resetting passwords.	Moderate	P-02, 03, 04	Related to R10
R14	5	Idle accounts may be brute forced without the account owner or IdP provider noticing.	Low	P-02, 03, 04	Related to R10
R15	6	PI is inadvertently disclosed to individuals subject to Protection or Restraining Orders.	Moderate	P-03	Identified in 2015 NSN PIA as a key risk. This risk was about information held by schools, remaining an existing business risk for schools and the Ministry. In a DI4OL context, minimal necessary information is retained about an individual. The only information stored that may potentially not be known by another person would be the individuals personal email address.

2015 Risk Id	2015 cross ref to IPP	2015 Risk Summary	2015 anticipated residual risk[14]	2022 PIA Risk x-ref	2022 Commentary
R16	7	Third party providers do not honour requests to correct PI.	Low	n/a	Objectively this would be a breach of the Privacy Act by the third-party provider, beyond any dissatisfaction that the Ministry or an education provider may express.
R17	8	Idle account may contain out of date PI.	Very Low	n/a	Related to R4.
R18	9	PI may be retained for longer than strictly required for authentication transaction purposes.	Low	n/a	The counterpoint to this risk is that if insufficient logging is retained, then incident investigation is more difficult. Retention of logging information by the DI4OL broker will be considered in the security risk assessment. In additional this risk is primarily for education providers, personal IdPs, and the third-party applications relying upon the transactions. Any risk is an existing business risk for those organisations and outside of the individual user's knowledge.
R19	10	Digital service providers share PI with sub-processors who use the PI for unapproved purposes, the sub-processors may be outside of NZ.	Low	P-04, 06, 07	Derivative of R1.
R20	13[15]	A persistent identifier [the NSN] used in authenticating with different third-party application providers is used by those different providers to aggregate information about an individual.	Very Low	P-06, 07	Identified risk, though derivative of R1.
R21	13	A unique identifier [school email address] used in authenticating is used by random third-party providers with malicious intent.	Low	P-03	Derivative of R1. Where individual logins are required, sharing something unique/identifiable is a pre-condition.
R22	3	Parents or Learners decline to provide information required for the specified use/purpose.	Very Low	P-08	Related to R8. As noted elsewhere, information required for DI4OL and online learning purposes is basic and minimal. Transparency by schools with Learners and parents is key to ensure awareness. If parents or Learners decline to provide this information, their enrolment with an education provider could not proceed. If they decline to permit enrolment information to be used for online learning their ability to participate in education would be significantly impeded and would be a matter for the education provider to resolve with the Learner/parents.

[15] 2015 cross references to IPP12 have been corrected to reflect that the former IPP12 is now IPP13.

2015 Risk Id	2015 cross ref to IPP	2015 Risk Summary	2015 anticipated residual risk[14]	2022 PIA Risk x-ref	2022 Commentary
R23	10	PI shared with approved third-party application providers is used for unintended purposes.	Low	P-06	Derivative of R2.
R24	5	Learners deliberately share credentials for the purpose of committing fraud.	Moderate	n/a	In the current context where examinations or assessments are performed in person on a specified date at a specified location, even if they are performed digitally/online, this is an existing business risk managed by NZQA with some existing controls in place. In the future where digital/online assessments may be performed unsupervised or remotely (e.g., at home), or at any time as part of a continual assessment approach, this risk will need reviewing to determine if a digital identity could help mitigate the risk of exam/assessment fraud.
R25	1	The Ministry or education provider populates the identity store with extraneous or unnecessary PI.	Moderate	P-01, 07	Identified risk, mitigated through minimisation of PI used for DI4OL purposes. For education provider purposes, they may require additional attributes to support internal business processes however SMSs should be the main source repository for additional information.
R26	8	Populated PI contains errors through lack of integrity checks.	Low	P-03	Integrity checking will need to be performed by education providers, it is likely Learners will be well placed to identify errors and seek correction.

Various Privacy Responses were documented in §5.1 of the *2015 NSN PIA*, and while these are also reflected in the recommended controls using different descriptions, we consider it useful to keep them separate from the specific controls here to aid traceability. These are summarised in Table 7 below. A cross reference between the 2015 Privacy Responses and Recommended Controls has been added as this was not provided in the original *2015 NSN PIA* itself. Commentary has been added to reflect relevance to the current PIA. Colour coding of the ref providers a quick view of planned implementation status for DI4OL.

Table 7 2015 NSN PIA Privacy Responses

Ref	**Summarised Privacy Response Description**	**Control x-ref**	**DI4OL commentary**
5.1.1	Minimise data collection in the first place, look at the possibilities for derived attributes.	C1	The DI4OL identity broker has minimised data attribute requirements, and these will be reflected in technical specifications for digital service providers.
5.1.2	Opt-out mechanism for individual Learners.	C2, 3, 18, 19	The DI4OL identity broker will be opt-in for education providers, but individual Learners in school will not then have an option to opt-out. Information used by the DI4OL identity broker is already collected by education providers to provide education/instruction. Opting out of education provided via digital

Ref	Summarised Privacy Response Description	Control x-ref	DI4OL commentary
🟧			channels will become progressively more difficult and remain an issue for handling by schools with individual Learners/parents. Benefits and value of education providers opting-in will be clearly articulated and communicated to schools. The use of information collected by education providers and used by DI4OL will be communicated to parents and Learners. Post school (or Tertiary) Learners will have the choice to opt-out of continued use of the DI4OL identity broker, although they would still need some credentials to access their Qualifications or RoA.
🟩 5.1.3	Governance group for reviewing and approving third party application provider connectivity.	C2, 4, 19, 22	This was identified as a key control in the RIS. An assurance framework applicable to digital service providers is to be developed under the DI4OL project. This will need to align and integrate with other Ministry strategic initiatives with digital service providers.
🟩 5.1.4	Identify configuration changes with third party providers where only a ‘check’ is needed, not persistent storage of the attribute or evidence	C1, 2, 3	Part of the configuration and specification for the DI4OL identity broker will consider whether information and evidence collection can be minimised and after ‘checking’ expressed as a ‘checked’ attribute.
🟩 5.1.5	NSN can be Privacy enhancing	C1, 2, 3, 19	Agreed. The DI4OL identity broker will manage which attributes are shared with digital service providers. The DI4OL identity broker will implement OIDC pairwise identifiers to prevent aggregation of information using the NSN as a common unique identifier. The Ministry will consider any scenario’s where the sharing of the NSN is requested by education providers for ‘online learning’ purposes.
🟧 5.1.6	Third party application providers should provide the Ministry with independent security and privacy assurance.	C4, 17	There are 12,000+ digital service providers in the NZ education sector for schools alone. The Ministry has several strategic activities in progress focussing on the most important third-party application provides. Extensibility of these approaches to providers needs consideration and will be developed in parallel with pilot activity.
🟥 5.1.7	Consider practical solutions where young Learners are otherwise expected to remember a password	n/a	Broadly this is outside the scope of the DI4OL project. Although implementing the DI4OL identity broker will reduce the need for any Learners to remember multiple different passwords for the most used educational applications as they will be connected to the DI4OL identity broker. Younger Learners tend not to be assigned personal devices with personal credentials by schools, instead using shared devices and shared credentials. A suitable level of teacher supervision and monitoring is in place. Explicitly biometrics will not be used as an authentication mechanism for direct access to the DI4OL identity broker linking portal. However, if an education provider implements biometrics, such as facial

Ref	Summarised Privacy Response Description	Control x-ref	DI4OL commentary
🟥			recognition or fingerprint readers, to unlock personally assigned devices for students that is a matter for the education provider to consider. Similar applies for any BYOD, DI4OL will have no knowledge of, or control over, whether a student uses biometrics to authenticate to their personal devices.
🟩 5.1.8	Consider alternative authentication options to the traditional username/password combination. Also consider use of MFA where there is greater authentication assurance required.	n/a	Usability considerations and modern trust methods are being considered for authentication. MFA is implemented for all privileged access to the DI4OL identity broker and will be required for all school IdP administrators.
🟩 5.1.9	Account idle/unused checks	C16	In the DI4OL identity broker solution the main account used will be school credentials (logon accounts). Thus, it will remain a school responsibility to perform identity management and disable any idle accounts. In the DI4OL identity broker itself Learner accounts may not be used for multiple years. An appropriate cut-off time, considering DISTF draft rules will be considered. In addition, monitoring of 'idle' DI4OL identity broker accounts for potentially suspicious activity will be developed. Given that the DI4OL identity broker is there to facilitate lifelong learning, and that 65,000 Learners exit secondary education each year, over time most existing accounts will be 'idle' as they are not used every day by post-school or post-tertiary Learners.
🟥 5.1.10	'Keep private' flag from ENROL	C2, 3, 15,	In the DI4OL identity context only the individual Learner will have access to their account within the identity broker, accepting some Ministry privileged administrative users. There is no function nor capability for other people (school staff or teachers, random Ministry staff) to access any identity information. Irrespective of this, the only identity information stored within the DI4OL identity broker would be a school or personal email address. While this does provide a contact mechanism, it does not disclose a location.
🟩 5.1.11	Account renewal	C5, 15, 16	As school accounts will be used as part of the DI4OL identity broker solution, it is implicit that these accounts are renewed daily while at school. And remain the responsibility of schools to manage. After a Learner leaving school the need for a finite lifetime on personal IdP accounts linked within the DI4OL identity broker has been considered. Five years is a proposed setting. This aligns to the DISTF Standards and Rules relating to a finite age of the Level of Assurance for Binding and Authentication.
🟩 5.1.12	Scope of [then proposed] NSN changes	C3, 4, 19	The Gazetting process will consider specified users and specified purposes across the entire education sector; ECE, Primary, Secondary, Tertiary, and lifelong learning.

Ref	Summarised Privacy Response Description	Control x-ref	DI4OL commentary
5.1.13	Education sector communications plan	C3, 18	A communications plan for the piloting with schools is being developed, with a dedicated Change and Engagement Manager assigned to the team.
5.1.14	Create a unique pseudonymous identifier for each Learner per third party application provider	C2,	Per 5.1.5 linking is required across some Government operated applications (NZQA). In the future any digital service providers, particularly where record of achievement or NCEA credits are an important consideration, may also require linking. Per IPP13 and risk P-07, although the DI4OL identity broker will not be functioning as a single centralised identity store, it is configured to provide 'pair wise' identifiers to digital service provider applications. This creates a pseudonymous identifier for each Learner that is unique to each application. That said, education providers will still be sharing at least the Learner's email address, so the practical utility of a pseudonymous identifier in lieu of the NSN is limited.
5.1.15	Legislative basis for using PI, and entity responsibilities for operational management.	C19	The legislative basis for use of the NSN is under the ETA 2020 Schedule 24, with further guidance elaborated on the Ministry's webpage for the NSN. More broadly the ETA 2020 provides the legislative basis for education providers collecting information for enrolment purposes, and where necessary sharing that with the Ministry. A RACI matrix is being developed using DISTF controls as a framework for operational responsibility.
5.1.16	Assurance programme for schools.	C2, 4, 5, 6, 7, 8, 17	An assurance framework applicable to schools, and more broadly other education providers, will be developed in alignment with the workstream. Whether the Ministry considers it suitable to mandate this assurance framework through regulation, or take a less directive approach, is outside the scope of the DI4OL project and solution itself.
5.1.17	Future scope changes must review perform further Privacy reviews	C5, 7, 22	The operational assurance framework that will be developed for the DI4OL identity broker, along with this PIA and C&A artefacts will clearly articulate scope and expected reviews given foreseeable changes.

Various recommended controls were articulated in the 2015 NSN PIA, the table describing these and mapping to the privacy risks is copied below in Table 8. Commentary has been added to reflect relevance to the current PIA. Colour coding of the Control ID providers a quick view of planned implementation status for DI4OL.

Table 8 2015 NSN PIA recommended controls

ID	Control description	Control to Risk Mapping	DI4OL Commentary
C1	Implement Privacy by Design principles	R9, R23, R25	This was identified in the RIS as a key control. The DI4OL solution has implemented privacy by design principles.
C2	Define privacy policy and information management policy for personal attributes that may be requested by service providers.	R9, R16, R25	The DI4OL solution inherits the existing Ministry Privacy Policy, and restrictions associated with the use of PI and the NSN in the ETA 2020. Technical controls are implemented in the DI4OL identity broker to give effect to these policies.
C3	Define clearly the purposes of the information collection and ensure that these are notified at the point of collection. For existing information, notify existing users of any change in purpose.	R8, R9, R22	As noted in this PIA under IPP1, the Ministry has a core assumption that when education providers are collecting information at enrolment time, that the business process for this takes an appropriate Privacy respecting approach. As part of the communications plan for the implementation of the DI4OL solution, comprehensive communications directly with schools will be undertaken including a FAQ that schools will be able to use with parents, Learners, and other interested stakeholders. Other material will be made available on the Ministry's public websites, and likely through the Education Gazette.
C4	Define contractual obligations for privacy and security with third party service providers including the requirement to assure performance and contractual controls. A regulatory instrument will be required to implement this control for education providers and their third-party service providers.	R1, R2, R3, R7, R9, R10, R16, R18, R19, R20, R21, R23	The recommendation of a regulatory instrument to place obligations (restrictions or conditions) upon education providers and their third-party service provides was identified in the 2015 RIS and PIA. However, the changes to ETA legislation at the time did not identity or implement any obligations. This 2022 PIA aligned to the DI4OL project, may identify recommended obligations (conditions or restrictions). Implementing this recommendation either for education providers or digital service providers that those education providers use are both non-trivial undertakings. An assurance framework applicable to digital service providers is to be developed under the DI4OL project. This will need to align and integrate with other Ministry strategic initiatives with digital service providers. Similarly, there is a strategic workstream Te Mana Tūhono addressing infrastructure security for Schools. An assurance framework applicable to schools, and more broadly other education providers, will be developed in alignment with the workstream. Whether the Ministry considers it suitable to mandate this assurance framework through regulation, or take a less directive approach, is outside the scope of the DI4OL project and solution itself.
C5	Perform information risk assessments.	R3, R10	In parallel with this PIA, an information Security Risk Assessment (SRA) is being performed.

ID	Control description	Control to Risk Mapping	DI4OL Commentary
C6	Perform regular security testing.	R3, R10	Security testing of the DI4OL identity broker will form a key part of the Test Strategy and Test Plan to be developed.
C7	Certify and accredit systems.	R3, R10	Certification and Accreditation of the DI4OL solution is a pre-requisite for the piloting with schools. The C&A will be updated as a result of the pilot and re-submitted for approval prior to production rollout.
C8	Provide security and privacy awareness training for education providers, students and parents.	R11, R12, R21	Providing broad privacy and security guidance to education providers to increase awareness of obligations and improve practices was identified in the RIS as a key control. The Ministry's Strengthening Cyber Security and Digital Support for Kura & Schools programme of work has this as a core objective, and it is outside of the DI4OL project's scope to broadly address school cyber security. Although specific advice and guidance relating to IdPs is envisaged. Professional Learning and Development (PLD) modules exist for teachers on broad security and privacy topics.
C9	Define auditing and logging schemes that identify potential fraudulent behaviour (such as simultaneous logins)	R11, R24	The DI4OL identity broker will implement logging, monitoring, and auditing as part of an overall DI4OL identity broker operational assurance plan. Some activities will be dependent upon education providers to perform commensurate monitoring of suspicious login behaviour. Where personal IdPs are used, it will remain the responsibility of those IT providers (Apple, Google, Microsoft, and DIA for RealMe) to perform appropriate logging and monitoring. An assurance review of the personal IdPs will be performed as part of the overall DI4OL identity broker C&A and operational assurance plan. The Ministry's overall Strengthening Cyber Security and Digital Support for Kura & Schools programme will include guidance on account and credential management to protect schools accounts from being compromised or identify when this has happened.
C10	Maintain audit trails of authentication including location (IP) and time.	R24	The DI4OL identity broker will implement full transaction logging, while technical standards applicable to school's IdPs will include recommendations for schools to ensure they have an appropriate level of logging implemented. Similar standards applicable to personal IdPs will be reviewed with the appropriate vendors to ensure alignment with Ministry requirements.
C11	Define acceptable use policy for identity and credentials.	R11, R12, R13, R24	Acceptable use policies will be for each individual education provider to define in alignment with their policy framework. The Ministry anticipates providing example content that can be used by schools to update their policies where necessary. Acceptable use policies for personal IdPs are already covered in applicable terms of service.

ID	Control description	Control to Risk Mapping	DI4OL Commentary
C12	Strongly verify identity prior to account modification or information requests.	R13, R15	As the DI4OL identity broker is not performing an Authentication, Credentialling, or Identity Provider function, the need for account verification processes relating to DI4OL identity broker is minimal. Similarly, if an individual no longer uses a previously linked personal email account/IdP and now wishes to link their new email/personal IdP, then rebinding processes will be initiated most likely via NZQA.
C13	‘Lock’ accounts after a suitable number of failed logins.	R14	Appropriate controls to be implemented relating to failed account logins will be recommended, it will remain the education providers responsibility to ensure that these are implemented. Ministry requirements relating to personal IdPs will be reviewed with the appropriate vendors as they hold the main customer-provider relationship.
C14	Implement alerting for significant system events such as multiple failed logins	R14	As per C9, C10, C13, the responsibility for monitoring and managing school logins will remain with schools. The DI4OL identity broker will be able to perform commensurate functions in relation to logins to the DI4OL linking portal and transactions brokered. Alerting implemented by IT providers for personal IdPs will be reviewed as part of the assurance review.
C15	Document design parameters and technical specifications for service providers	R16, R18, R19, R21	The DI4OL project team are defining technical specifications and associated configuration requirements to permit third parties (whether IdPs or digital service providers), to connect to the identity broker.
C16	Identify and suspend idle accounts	R4, R5, R17	In the DI4OL identity broker solution the primary accounts used will be school credentials (logon accounts). Thus, it will remain a school responsibility to perform identity management and disable any idle accounts. In the DI4OL identity broker itself Learner accounts may not be used for multiple years. An appropriate cut-off time, considering DISTF draft rules will be considered. In addition, monitoring of ‘idle’ DI4OL identity broker accounts for potentially suspicious activity will be developed. Given that the DI4OL identity broker is there to facilitate lifelong learning, and that 65,000 Learners exit secondary education each year, over time most existing accounts will be ‘idle’ as they will not be used every day.
C17	Require all third-party applications wishing to use the SSIAM to conduct and publish a PIA where shared personal information shared with the online service provider creates potential privacy risks.	R19	The original recommended control to require a PIA from vendors, to manage the risk that sub-processors outside of NZ may use information for unauthorised purposes, is ineffective. A vendor performing a PIA does not prevent sub-processors from misusing information exchanged with them. At best a PIA would identify those commercial contracts with sub-processors need to include comparable Privacy protections. However, this is a requirement under Privacy legislation anyhow and is not a novel finding from a PIA.

ID	Control description	Control to Risk Mapping	DI4OL Commentary
🟥			In the current DI4OL context this recommendation is considered impractical and would become a significant barrier to adoption and uptake of the DI4OL identity broker solution. Any sharing of PI introduces the potential for privacy and information security risk. There are over 12,000 digital service providers that schools use. Assuming digital service providers were to perform a PIA, the Ministry would not have resources to review those PIA's and meaningfully engage with vendors. Hence the intention to establish an assurance framework applicable to third parties, per 2015 NSN PIA recommended controls 5.1.3, 5.1.16, 5.1.17, C4.
C18	Develop and implement a communications plan for the proposed changes and a process of regular reminder communications for education providers and service providers.	R8	A communications plan for the piloting with schools is being developed, with a dedicated Change and Engagement Manager assigned to the team. Change communications direct to schools will be refined as a result of the pilot to inform the production rollout. Communications directed to peak bodies such as NZSTA, PPTA ICT Advisory group, Secondary Principal's Association(s), NZPF, as well as broader communications such as in the Education Gazette, are part of the plan to introduce the concept of the DI4OL identity broker, benefits, outcomes etc. and raise awareness.
C19	Develop policy and clear guidance on the use and disclosure of the NSN for education providers outsourcing IAM functions.	R6, R8	Use of the NSN is covered in the ETA 2020 Schedule 24, associated Gazette notices, with further guidance elaborated on the Ministry's webpage for the NSN. Providing broad privacy and security guidance to education providers to increase awareness of obligations and improve practices was identified in the RIS as a key control. The Ministry's Strengthening Cyber Security and Digital Support for Kura & Schools programme of work has this as a core objective, and it is outside of the DI4OL project's scope to broadly address school cyber security. Although specific advice and guidance relating to IdPs is envisaged.
C20	Design and implement incident response procedures including all steps to identify, respond and recover from a privacy breach or security incident (as per Office of the Privacy Commissioner and NZ Information Security Manual guidelines).	R1	The DI4OL identity broker solution inherits the existing Ministry incident management plans relating to security incidents and potential privacy breaches.
C21	Implement integrity checking and data accuracy mechanisms for the	R26	The DI4OL identity broker will not be migrating identity information from source systems, nor populating a new identity store that duplicates an education provider IdP. As school login accounts are used daily by

ID	Control description	Control to Risk Mapping	DI4OL Commentary
🟩	migration and population of identity data from source systems.		Learners, it is an existing school responsibility to ensure that the information flow between SMS's and IdPs used by a school are accurate and maintain integrity of information. The DI4OL identity broker will implement some data integrity checks focussed on the NSN. Ensuring that one NSN is not claimed by multiple Learners, or that an NSN is not being used in a potentially fraudulent manner. Additional consistency checking of information stored in the DI4OL identity broker, such as an individual's name, may be possible using existing Ministry systems such as ENROL. However, these consistency checks will age as a Learner leaves secondary or tertiary education, and the value implied by having those checks will diminish. E.g., the information stored in the DI4OL identity broker may not be updated by an individual when they change their legal or official name, and the DI4OL identity broker will have no visibility of that original change.
C22	Establish regular reviews and confirmation of the business requirements to retain identity data collected and stored.	R5	To align with DISTF rules, we anticipate that a five-year account 'idle' measure will be used. At any subsequent point where the Learner wishes to access DI4OL connected applications, a rebinding of that individual to their account will be required. Should the account be in continued (at least once every five years) use, rebinding may not necessarily be performed. In the context of lifelong learning, the Ministry's existing requirement to maintain Public Records for as long as they are required applies. Noting that here the Ministry is only managing the account access to the formal public record which is the education achievement. NZQA remain responsible for retention and disposal of the educational public record in alignment with NZQA retention and disposal schedules.

Addendum 1 September 2022 updates

While this PIA has been progressing through the signoff process, a key additional source of information relating to Privacy for UK Schools has been published. This UK Schools report cites work by the Dutch government in the past year with Google, and research lead by the University of Sydney. Recommendations from the UK & Dutch sources are being reviewed and where applicable will be important to updating the PIA for a production deployment in 2023.

With a greater focus by privacy professionals and researchers internationally, and in NZ, on the topic of Children's Privacy this will be a rapidly evolving topic.

References

Additional references

Title	Date	Source and Link
Problems with data governance in UK schools: Google Classroom & Classdojo	31/08/22	5rights & Digital Futures Commission (UK) New report finds digital classrooms flout data protection law to exploit children's data for commercial gain – 5Rights | Digital Futures Commission
Update DPIA report Google Workspace for Education	2/08/21	Dutch Gov SURF/SIVON Original DPIA https://www.surf.nl/files/2021-06/updated-g-suite-for-education-dpia-12-march-2021.pdf Updated DPIA https://www.surf.nl/files/2021-08/update-dpia-report-2-august-2021.pdf Guidance for schools (in Dutch) https://www.surf.nl/en/news/google-workspace-for-education-support-package
Google mitigates 8 high privacy risks for Workspace for Education	9/08/21	Privacy Company (NL) (in English) Google mitigates 8 high privacy risks for Workspace for Education - Blogpost (privacycompany.eu)
Should We be Worried about Google Classroom? The Pedagogy of Platforms in Education	2021/22	Journal of Professional Learning Should We be Worried about Google Classroom? The Pedagogy of Platforms in Education (cpl.asn.au)
DI4OL and the use of Personal Accounts	2022	Ministry internal issues paper personal login

Applicability for DI4OL

In the context of the DI4OL pilot with schools only one recommendation is currently relevant. This is in relation to the use of a personal account when accessing educational services while at school. Although the example cited in the source reports does not directly apply to the DI4OL service, as the only digital service provider accessible via the DI4OL service is from NZQA, the establishment of identity linking through the DI4OL portal creates a potential risk that needs mitigating. Associated risks have been identified in the information security risk assessment (C&A memo), as they have a broader impact for confidentiality than just a privacy risk.

For the pilot the outcome of this will be that Learners will not be permitted to access the NZQA Assessment Master application using a personal credential, only a school credential will be permitted. Naturally Learners will be permitted to access the Record of Achievement using their personal credential.

A Policy paper has been in development to inform the formal decision making process. This will include recommendations on advice and guidance to schools relating to DI4OL, and more broadly to the use of personal credentials in an education environment.