Summary of the PIA for the Identity Service and SMS Extender Service

Auckland Head Office
Suite 306, Geyser Building
100 Parnell Road
Auckland 1052
PO Box 37 118
Parnell, Auckland 1151

Wellington Office
Level 9, Bayleys Building
36 Brandon Street
Wellington 6011
PO Box 11 487
Wellington 6142

P 0800 LEARNING
P +64 9 972 1679
W www.n4l.co.nz
E info@n4l.co.nz

Table of Contents

1 Introduction

1.1 Background

N4L has introduced two new services (the **SMS Extender** and the **Identity Service**) which store identity information for individual users and enable users to access services provided by N4L and other 3rd parties using the Identity Service.

N4L completed a detailed Privacy Impact Assessment (**PIA**) which considered the privacy implications of the proposed Identity Service and SMS Extender services. This document provides an overview of that PIA. Further information on the PIA is available from N4L.

1.2 N4L's approach to privacy

N4L is committed to providing safe and secure education solutions. Since N4L's inception, privacy has been a core consideration for all N4L services. N4L's privacy policy is available on its website at www.n4l.co.nz/legals/, and any privacy related enquiries are handled by N4L's privacy officer.

It is very important to N4L to ensure that privacy of students, teachers and other users is appropriately protected, and any identified privacy risks are identified and appropriately mitigated. N4L has a number of internal assurance processes in place to ensure that personal information held by N4L is not misused.

The management of privacy for the SMS Extender and Identity Service is particularly important given N4L will be collecting and using the personal information of minors. Ultimately, N4L's goal is to build a system that is attractive to the New Zealand education system at large. Potentially, once fully implemented, the SMS Extender and Identity Services may be taken up by the majority of New Zealand school age students and their teachers. Given the potential for significant holdings of personal information, N4L is very aware of the importance of robust privacy practices.

N4L took a "privacy by design" approach to developing the SMS Extender and Identity Services. Privacy was considered throughout the development process. N4L actively engaged privacy professionals and consulted with the Government Chief Privacy Officer and the Office of the Privacy Commissioner on the privacy aspects of the SMS Extender and Identity Service, and is proud of the solution that has been implemented. N4L also consulted with the Ministry of Education.

1.3 Terminology used in this document

Some terminology used in this document:

- **SMS Extender** means the infrastructure connecting a school's SMS to the IAM Platform.
- **IAM** means Identity and Access Management.
- **IAM Platform** means the infrastructure providing the core functionality of the Identity Service.
- **Identity Service** means the identity service described in this PIA.
- **NSN** means a national student number as defined in the Education Act.
- **PIA** means N4L's detailed Privacy Impact Assessment on the SMS Extender and Identity Service.
- **Pond** means N4L's online community application available at www.pond.co.nz.
- **SMS** means Student Management System.
- **SMS Data** means data obtained from a school's SMS in order to provide the Identity Service.
- **SMS Provider** means an organisation that provides an SMS to a school.

2 The Services

2.1 Service Overview

The PIA covers the SMS Extender and Identity Service products. Further information on these services is available on N4L's website.

2.2 Personal Information Collected

The personal information being collected by the SMS Extender and the Identity Service is described in Attachment 1.

Through a user's use of the Identity Service, N4L will gain additional personal information. This may include information such as:

- answers to security questions which a user chooses if a password reset is necessary.
- information on the content and applications that a user has accessed.
- statistical information on a user's session (e.g. the length of time they were logged in for, type of device etc).

N4L will only use this information for purposes directly related to the provision of the Identity Service. N4L will not data mine, profile or perform other analysis of a user's information which is unrelated to the provision of the Identity Service. This is a key benefit of the service over some other commercial SSO or IAM services where it is difficult to be confident that inappropriate data mining, profiling or analysis unrelated to education is not occurring.

2.3 Personal Information Used and Disclosed

The personal information of students and educators (i.e. school teachers and staff members) that is disclosed by the Identity Service is summarised in the Attachment.

SMS Extender

As illustrated by the Attachment, the disclosure of personal information in the SMS Extender is very limited. This is consistent with N4L holding this information on the school's behalf (or in limited circumstances on the behalf of another authorised user) and only for the purpose of enabling effective and efficient information transfer to the Identity Service.

Identity Service

As illustrated by the Attachment, the personal information disclosed by the Identity Service varies depending on which users are accessing the information and which third 3rd party providers have been authorised by the school or another authorised user to receive identity information.

2.4 Security Measures

Given the potential exchange and storage of large quantities of personal information, both the SMS Extender and Identity Service include robust security measures. These measures help ensure the systems are available and that integrity and confidentiality are safeguarded. There are system wide and user protections to ensure that personal information is not inappropriately lost, accessed, used, modified or otherwise misused.

Security measures include:

- Multi-tiered application structures with firewalls separating network zones.
- Load balancers that are configured to only allow particular traffic to pass.
- All web traffic to both the SMS Extender and Identity Service being encrypted.

The IAM Platform that supports the Identity Service has been designed to recognise that a number of users may validly need to be able to view and amend a student's profile (e.g. their teacher, dean, principal and the school's administrator). Different users have differing ability to change and view user information. To ensure the accuracy of certain information, certain changes to personal profiles, and the addition of new users, must be made in the SMS, which then syncs through to the Identity Service.

As highly secure passwords may be difficult for younger students to remember, the Identity Service will allow various levels of password security.

2.5 Unique identifiers

In order for the system to operate, N4L must provision an N4L ID. This unique ID is a back end number which is not visible to users, but will be used within N4L's systems to identify a user within the system.

N4L will not provide its N4L ID to any 3rd party application provider. Instead, each 3rd party application provider will receive from N4L a provider specific unique identifier for each user. The provision of a new unique identifier helps to ensure that users cannot be uniquely identified with certainty between application providers and provides further privacy protection for users.

To enable easy provisioning and a low error rate it was important to automate in a secure manner the creation of the N4L identifier. To do this, N4L created an algorithm to generate the N4L identifier based on the information included in the standard Ministry of Education approved IDE and SMS-LMS formats. Some of this information is used in its entirety and some in a hashed form. The inputs included in the algorithm ensure the resulting N4L ID it is repeatable and unique.

The algorithm does not allow for any input to be reverse engineered from the resulting N4L identifier (e.g. from the N4L identifier you could not figure out a person's date of birth, NSN or other personal information). To do this, the algorithm uses processes similar to the algorithms that are commonly accepted in the banking industry around protecting credit card numbers (the PCI Principles).

There are statutory protections regarding the use of the NSN and restrictions around the authorised users of NSNs. Schools are authorised to use the NSN for a number of purposes, including ensuring education providers and students receive appropriate resourcing (such as digital learning tools). Other educational agencies (such as NZQA and the Ministry) are also authorised users of the NSN.

N4L is not an authorised user of the NSN. Accordingly, where a school wishes to use the Identity Service they will approve N4L's use of the NSN on that school's behalf, for the purpose of generating the N4L unique identifier (as described above) and for the purpose of providing information to the Identity Service. N4L will provide this service on the school's behalf and has no other right to access information in the SMS Extender. In effect, the SMS Extender can effectively be thought of as an extension to the SMS service. (In a similar way, SMS providers are not authorised users, but hold each student's NSN in the SMS which they manage on the school's behalf.)

For most students the NSN will only persist in the SMS Extender for a short length of time. However, where an authorised user of the NSN develops an application which uses N4L's Identity Service (i.e. the authorised user is a consuming service of the Identity Service), then an authorised user can authorise N4L as their processing agent for authorised students to capture the NSNs for those students in the SMS Extender, and transfer it to the Identity Service and then on to the application. This authorisation only allows N4L to use the NSN in the SMS Extender and in the Identity Service for the purpose of providing the NSN to the authorised user's application. In such cases, as an agent of the relevant authorised user, the SMS Extender and Identity Service may hold and disclose the NSN as specifically authorised by the relevant authorised user. N4L will only agree to pass on the NSN as an attribute to an authorised user of the NSN where the authorised user confirms that the proposed use of the NSN accords with the NSN provisions in the Education Act.

The SMS Extender will also generate (using a similarly secure process) a unique N4L identifier for teachers and non-teaching staff and other users. Key information provided in the data feed from the SMS (such as the full name, date of birth, teacher registration number and gender) will be used to create the N4L identifier. These details may be involved in their full form, or in a truncated / hashed form. Because of the lower number of users, this process is considered sufficiently repeatable and unique.

3 Privacy analysis

3.1 Privacy risk ratings

The risk analysis in the PIA rates privacy risks as follows according to the following scale:

✓✓	✓	?	X
Privacy enhancing - goes beyond requirements in the Privacy Act	Meets requirements of the Privacy Act	May not meet the requirements in the Privacy Act	Does not meet the requirements in the Privacy Act

3.2 Privacy analysis

The table below summarises the privacy analysis in the PIA.

As SMS Data in the SMS Extender and Identity Service is held by N4L as an *agent* of the school (or other authorised user), the school (or other authorised user) will have primary responsibility for ensuring the Privacy Act obligations are met in respect of the personal information in the SMS Extender or Identity Service. But N4L will contractually agree to assist the school (or other authorised user) to meet those obligations. In its agreement with schools and authorised users for the SMS Extender and Identity Service, N4L will agree:

- not to do, or omit to do, anything that could cause a school or other authorised user to breach its privacy obligations;
- to immediately notify the school or other authorised user upon becoming aware of any such breach; and
- within five Business Days following a request, provide the school or other authorised user with a written description of the technical and organisational methods employed by N4L for protecting the SMS Data in the SMS Extender from unauthorised use, loss, alteration or disclosure.

Privacy Principle	Application to SMS Extender	Application to Identity Service
Collection of the personal information including Principle 1 – Purpose of collection Principle 2 – Source of personal information Principle 3 – Collection of information from subject Principle 4 - Manner of collection of personal information	✓✓	✓
Storage and security of personal information (principle 5)	✓✓	✓✓
Access to and correction of personal information including Principle 6 - Access to personal information Principle 7 - Correction of personal information	✓✓	Access ✓✓ Correction ✓
Accuracy of personal information Principle 8 - Accuracy etc of personal information to be checked	✓	✓✓

Privacy Principle	Application to SMS Extender	Application to Identity Service
before use		
Retention of personal information Principle 9 - Obligation not to keep personal information for longer than necessary	✓✓	✓
Use and disclosure of personal information by N4L including: Principle 10 - Limits on use of personal information Principle 11 - Limits on disclosure of personal information	✓	✓
Unique identifiers (principle 12)	✓	✓

4 Privacy enhancing initiatives

N4L's Privacy Officer is responsible for reviewing privacy at N4L. Any privacy complaints, issues or suggested improvements to the SMS Extender or Identity Service will be discussed with the Privacy Officer.

The Privacy Officer must report on any privacy breaches or near misses and these will be escalated within N4L to ensure they are appropriately actioned (e.g. presented to the Audit and Risk Committee of N4L's Board).

N4L establishes focus groups to consider any proposed changes to its services. These would be established for any material change to the SMS Extender or Identity Service, and would consist of ICT and education specialists. Privacy considerations would be specifically considered prior to launch.

N4L staff will receive training on the SMS Extender and Identity Service, including privacy aspects.

The PIA will also be reviewed after the SMS Extender and Identity Service have been fully operational for one year, in order to:

- ensure the systems been appropriately built and operated.
- consider any unexpected issues that have occurred.

5 Conclusions

Identity services are becoming increasingly necessary in a complicated digital world. It is currently too complicated for many schools to manage their student's user permissions and access arrangements and to provision new applications for their students. In many schools the current systems are ad hoc and manual. The SMS Extender and Identity Service proposed by N4L are a significant step forward in addressing these current issues.

If the SMS Extender and Identity Service are taken up by a majority of schools, they would hold the personal information of over a hundred thousand students and thousands of teachers. Given this scale, it is appropriate that privacy has been robustly considered in their design. There are inherent privacy risks in a system of this nature given the scale of the system, the amount of personal information and the sensitivity of personal information about minors. Online safety and security are core to N4L's business model - so N4L's significant business drivers have also helped to produce a system which appropriately enhances privacy.

N4L have adopted a robust SMS Extender and Identity Service (including the IAM Platform) which is designed to mitigate the inherent privacy risks and have adopted a number of privacy enhancing approaches. However, the design of the system has been a balancing act - as to eliminate some of the risks (e.g. the likelihood of manual data errors and security issues with manual processes) the only reasonably practicable option has been to automate significant aspects of the provisioning of the system (this results in a risk information will also be captured from students who wish to opt out and information may be collected on all groups a student is in, even where only a basic authentication service is being provisioned). On balance, the resilience, accuracy and security benefits of automation mean this is the only reasonably practicable option for this Identity Service. To ensure the privacy principles are met, user information and group information will be deactivated and/or not used by N4L for such students, such that no harm will eventuate from this data being collected by N4L.

Attachment: Summary of the personal information in the SMS Extender and Identity Service and how the information is used and disclosed

Student Personal Information	Disclosed To		Disclosed To						Disclosed To			
	Data in SMS Extender	N4L Developers	Data in IAM Platform	N4L Admin	Provider Admin**	Super User (IT Admin / Principal)	Standard User (Teacher)	Non admin (Student)	Authentication Only OAuth or SAML	Consuming Applications Integration Level 1 OAuth or SAML	Integration Level 2 OAuth	Integration Level 3 OAuth
First Name	x	view	x	view	view	view	view	view		x	x	x
Last Name	x	view	x	view	view	view	view	view		x	x	x
Preferred Name	x	view	x	edit	edit	edit	edit	edit		x	x	x
Gender	x	view	x	view	view	view	view	view		x	x	x
Role (teacher/student)	x	view	x	view	view	view	view	view		x	x	x
Email Address	x	view	x	edit 1*	edit 1*	edit 1*	edit 1*	edit 1*		x	x	x
N4L ID (Application-Specific)			x	view	view	view	view			x	x	x
Organisation (school)	x	view	x	view	view	view	view	view			x	x
Year Level	x	view	x								x	x
Groups/Classes/Departments	x	view	x	view	view	view	view	view		x	x	x
First Attendance	x	view	x	view	view	view	view	view				x
Date of Birth	x	view	x	view	view	view	view	view				x
Tutor	x	view	x									
Last Attendance	x	view	x	view	view	view	view	view				
Username	x	view	x	view	view	view	view	view				
NSN***	x	view	x									
SMS Person ID	x	view		view		view	view					
N4L ID	x	view	x									
IAM Role			x	edit		edit	view	view				
IAM Initial Password			x	view	view	view	view					
IAM Password strength			x	edit		edit	edit					
IAM Enrolled Applications			x	edit	edit	edit	edit	view				
IAM Application Profiles			x	edit		edit						
IAM Security Questions			x	view	view	view	view	view				
IAM Account Enabled/Disabled			x	view	view	view	view					
IAM Account Disabled Reason			x	view	view	view	view					
IAM Account Creation Date			x	view	view	view	view	view				
School Population			x	view		view	view					

* Only personal email address is editable.

** Provider Admin role is limited to the Provider's own organisation.

*** Only for students where N4L has been specifically authorised as a processing agent of an authorised user, and only in accordance with that authorisation.