Te Tāhuhu o te Mātauranga
Ministry of Education

Privacy Impact Assessment

for the

Digital Identity for Online Learning Project

Plain Language Summary

Contents

Background **3**
What is the problem? 3
How are we fixing it? 3
Terms used 3

About Digital Identity for Online Learning **4**
How does Digital Identity for Online Learning (DI4OL) work? 4
Who will use DI4OL? 4
How do students get to use DI4OL? 4
What happens when a student is about to leave school? 4

Privacy **5**
Why is privacy important? 5
What is personal information? 5
The Privacy Act 2020 5

The Privacy Impact Assessment **6**
DI4OL and privacy 6
What is a Privacy Impact Assessment? 6
What is Assessed in the DI4OL's PIA? 6
How DI4OL will work 7
What happens behind the scenes? 8
Privacy Principles 9
United Nations Convention on the Rights of the Child 9
Data Protection and User Policy (DPUP) 9
Risks 10

How does DI4OL manage the privacy risks? **11**
The pilot 11
Managing the moderate level risk 11
Managing the low-level risks 11

Background

The Ministry wants to make sure everyone's:

- privacy is protected
- digital information is safe.

Digital systems need to be able to confirm that a person is who they say they are. This is especially important when the system is being used for educational assessments and results.

What is the problem?

When students are doing their National Certificate of Educational Achievement (NCEA), they need to be able to login to the New Zealand Qualifications Authority (NZQA) to sit online exams, submit work, and to see their results (Record of Achievement).

Students currently have to:

- use different logins for their school systems and for NZQA
- use their separate login for NZQA when they leave school, to access their results.

This can add to student stress, especially if students forget their NZQA login before an online exam or a submission deadline. It can lead to lots of urgent work for schools and NZQA to do.

How are we fixing it?

The Ministry of Education has set up Digital Identity for Online Learning (DI4OL) to make these tasks easier.

When schools opt in to DI4OL, students will use their school login to access NZQA exams and results.

DI4OL will only use a small part of the information that schools already share with the Ministry. DI4OL protects students' personal information by:

- not storing passwords or other verification such as facial recognition
- only linking with trusted education applications.

Terms used

To keep the language simple in this document, the terms 'school' and 'student' include kura and ākonga. A te reo Māori version of this document will be available in the Privacy section of the DI4OL webpage DI4OL Privacy in the future.

About Digital Identity for Online Learning

How does Digital Identity for Online Learning (DI4OL) work?

DI4OL acts as a go-between. It redirects student's NZQA login requests to their school Microsoft or Google account login. Once the student has entered their login details correctly, DI4OL lets the NZQA system know that the student's identity has been confirmed, and NZQA lets the student into the site.

The student's school account is acting as an identity provider. An identity provider is a service that confirms you are who you say you are online.

DI4OL uses the student's National Student Number (NSN) to make sure that the student is given the correct access to NZQA. Students are given an NSN when they start in education (usually early childhood or school).

Who will use DI4OL?

Schools can opt in to using DI4OL for NCEA-level students from early 2024.

In the future, students may be able to login to other learning applications such as Mathletics. If you go to the Ministry of Education website and search for DI4OL, you will be able to see what apps and sites can use DI4OL login.

How do students get to use DI4OL?

Students doing NCEA assessments will use DI4OL to login to NZQA if their school has opted in to DI4OL. Students may also use DI4OL to check their results if they have previously attended a school that has opted into DI4OL.

What happens when a student is about to leave school?

Before leaving school, students will be able to create a link to one of these personal accounts:

- Apple
- Google
- Microsoft
- RealMe.

This allows them to use their personal account's login to see their results when they have left school.

Privacy

Why is privacy important?

When we say ‘privacy’, we mean keeping people’s personal information safe.

In New Zealand, the main way we make sure personal information is kept safe is through the Privacy Act 2020.

Privacy is also part of some international agreements, such as the United Nations Convention on the Rights of the Child (UNCRC). (This link has a child-friendly version as well as the full text.)

What is personal information?

Personal information is any information about a person that allows someone to identify them. Personal information doesn’t have to include their name. It could be something like their phone number, home address, or gamertags.

The Privacy Act 2020

The Privacy Act 2020 tells people and groups how they are allowed to collect, store, use and share your personal information.

It makes sure that:

- you know when your information is being collected
- your information is used and shared appropriately
- your information is kept safe and secure
- you can get access to your information.

The Privacy Act has thirteen principles, as well as guides for specific areas. You can get more information about the Privacy Act 2020 in these places:

- Office of the Privacy Commissioner
- Netsafe’s OWLS (child-friendly explanation).

The Privacy Impact Assessment

DI4OL and privacy

The project to set up DI4OL has focused on making sure learners' personal information and login details will be kept secure.

To do this, the Ministry needed to find the answers to questions like:

- Can information be shared between NZQA and the other parties securely?
- Will shared information be kept to the minimum required for the system?
- Will learners' information be stored so it can only be accessed by people and functions who need it?
- Will each learner be able to see all their own information and no-one else's?

These questions and others have been looked at in the Privacy Impact Assessment.

What is a Privacy Impact Assessment?

A Privacy Impact Assessment (PIA) works out privacy risks and ways to reduce them.

The PIA for DI4OL also looked at risks related to using a student's National Student Number (NSN).

What is Assessed in the DI4OL's PIA?

The DI4OL PIA assesses the privacy impacts under the following topics:

- how DI4OL will work
- how the Privacy Act and UNCRC principles are met
- how the Government's Data Protection and Use Policy (DPUP) is met
- what the privacy risks are and how are they will be managed.

Each of these is explained more in the next sections.

How DI4OL will work

What processes are not affected

These things will be the same when DI4OL is used:

- how a student enrols at a school (including what information is collected)
- how information is used by a school
- how information is shared with the Ministry.

What information is collected

When enrolling at a school, the student (or their parent/whānau) is asked to share personal information that the school needs. This includes the student's name and date of birth.

If the school gives students a school email address, the school will add students' details to the Microsoft or Google system the school uses.

The details added are the student's name, preferred name, and school email address. If the school is enrolled in DI4OL, the student's date of birth, and National Student Number are also included.

What will it be like to login to NZQA with DI4OL?

The only difference for the student is that they use their school login, rather than a separate one for NZQA.

When a student tries to login to NZQA, they will:

1. Choose the option to login with their school account.
2. Fill in their school login details.
3. Access the NZQA site for online assessments or their results.

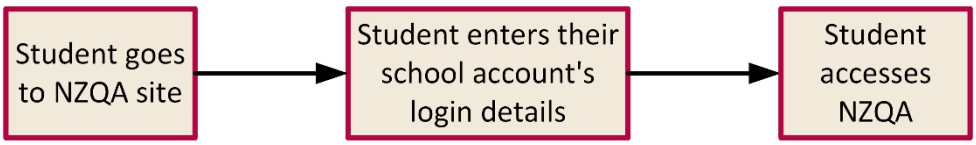

Figure 1: Student login experience

What happens behind the scenes?

This section gives an overview of the technical process behind student login. Detailed information is given in the PIA in the *Logical view and data flow* section.

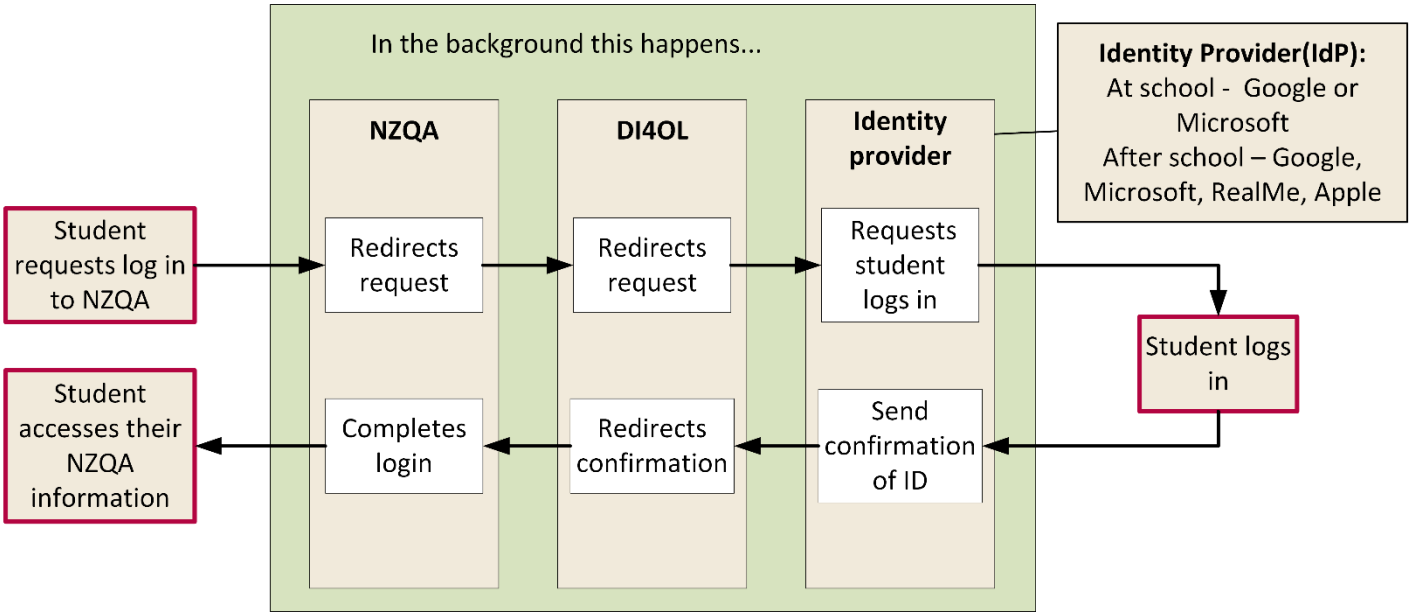

Figure 2: Process around student login

As shown in Figure 2, the process for the student login is:

The student:

1. Goes to the NZQA login screen.
2. Chooses the option to login with their school account.

NZQA:

3. Forwards the login request to DI4OL.

DI4OL:

4. Forwards the login request to the identity provider (Microsoft or Google).

The identify provider:

5. Prompts the student to enter their login details.
6. Confirms the login details are correct.
7. Sends DI4OL the confirmation of the student's identity.

DI4OL:

8. Forwards the confirmation of the student's identity to NZQA.

NZQA:

9. Allows the student access.

Privacy Principles

The privacy principles that most apply to DI4OL are:

- Principle 1 - Purpose for collection
- Principle 3 - What to tell the individual about collection
- Principle 5 - Storage and security of information
- Principle 10 - Use of personal information
- Principle 11 - Disclosing personal information.

United Nations Convention on the Rights of the Child

The United Nations Convention on the Rights of the Child is divided into articles. The PIA considered how well the DI4OL contributes to the best interest of the child, by:

- protecting the child, including their privacy (articles 3, 16)
- ensuring children can reach their potential (articles 28, 29)
- protecting a child's information so it is not used to disadvantage the child (article 36).

Data Protection and User Policy (DPUP)

The Government's Data Protection and User Policy (DPUP) is based on five principles that aim to build trust. The principles also encourage data practices that focus on the wellbeing of people and communities.

The PIA assessment checks the DI4OL project will meet the DPUP principles.

You can learn more about DPUP at Learn about DPUP.

Risks

Deciding the risk level helps work out how much effort needs to be put into making sure a harmful event doesn't happen.

The risk level of a possible event is based on:

- how likely it is that it will happen
- how much harm it may cause.

A risk can be reduced by making it less likely to happen, or by reducing the harm the risk may cause.

Here is an image showing how likelihood and harm interact to give different levels of risk:

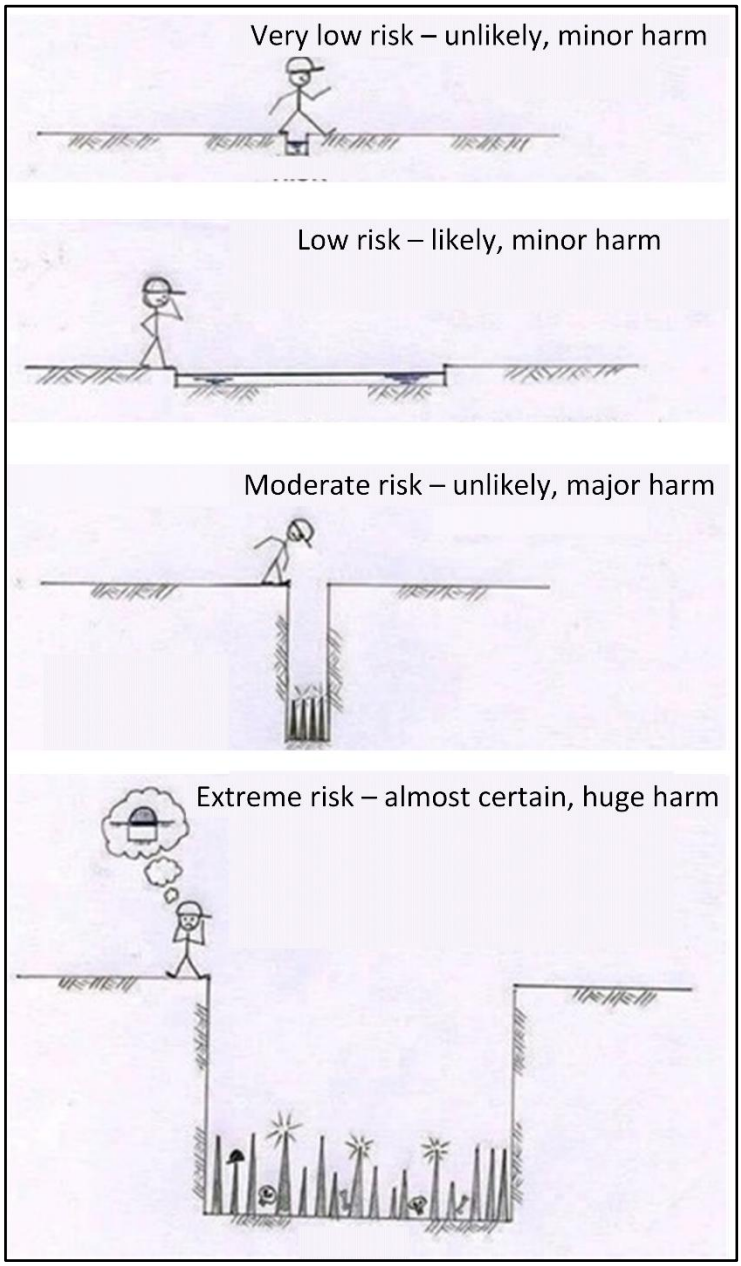

Figure 3: Examples of risk levels

Source: Crashoverride on Twitter 2018.

How does DI4OL manage the privacy risks?

The PIA worked out that there was one moderate-level risk and eight low-level privacy risks in DI4OL.

The pilot

The first step in managing the risks was to run a pilot to check:

- that DI4OL works and keeps information secure
- how easy DI4OL is to use
- that the advice and guidance MoE provides is useful
- whether privacy policies and processes in schools will need amending because of DI4OL.

Managing the moderate level risk

The moderate-level risk comes from DI4OL linking to systems which may have poor security.

We are managing this risk in DI4OL, by:

- having strong security systems
- encrypting data
- strictly limiting who has access to change DI4OL
- only collecting information that is needed
- making sure students can review and update their information
- clearly stating who is responsible for what
- having processes to make sure that everyone continues to do the right thing
- having outside experts review DI4OL processes.

Managing the low-level risks

The low-level privacy risks already occur in some schools and service providers. The Ministry of Education will manage these risks by providing advice and guidance.

Some schools, or service providers may:

- collect, use, or share personal information in ways that aren't appropriate
- not explain privacy and personal information in a way that is understood by students, whanau, and parents.

When schools opt in to DI4OL, they:

- might not tell students and parents/whānau all the information about the change.
- students may reuse or share passwords or choose poor passwords.