THE VOICE OF EDTECH IN NEW ZEALAND, SUPPORTING THE GROWTH OF THE SECTOR.

THE AOTEAROA EDTECH DATA PRIVACY PLEDGE

EdTech NEW ZEALAND

WWW.EDTECHNZ.ORG.NZ

INTRODUCTION

The Aotearoa EdTech Data Privacy Pledge is a framework developed by EdTechNZ which provides standards on data privacy and security safeguards for EdTechNZ's EdTech members to meet. This offers an ideal starting point in preparation to complete the Safer Technologies 4 Schools (ST4S) assessment and certification.

The Privacy Pledge is a self-assessment process. If you determine that your business meets and supports the Privacy Pledge standards, upon signing the Pledge on our website, your company name and logo can be added to the Privacy Pledge page on EdTechNZ's website. This will demonstrate to teachers, parents, students, your team and your peers in the sector more broadly that you are committed to safeguarding the data you hold.

You will also have access to online resources and templates to support you in preparing your ST4S application, when you are at a stage where it makes sense to do so.

PRIVACY PLEDGE AIMS

The Privacy Pledge aims to establish a standard level of protection that New Zealand EdTech companies should adhere to. These standards apply regardless of how your IT service is delivered, the frequency of use, or the underlying technology. They are for all NZ EdTechs offering products and services within the Primary and Secondary sectors, whether domestically or overseas.

The Privacy Pledge framework also identifies and encourages all New Zealand EdTechs to consider the principles of Māori data sovereignty in relation to the collection, ownership and application of Māori data.

The Privacy Pledge is accompanied by a comprehensive set of guides that have been developed by experts in the New Zealand EdTech Community, Hail, to support others in their development of security practices and adherence to this Privacy Pledge. We will invite you to renew your commitment to the Pledge annually.

CONTENTS

DEFINITION OF TERMS 04

RISK PROFILE 04

PRIVACY POLICY AND SECURITY STANDARDS (SELF-ASSESSMENT) 06

STANDARDS – PRIVACY 06

STANDARDS – DISCLOSURE 06

STANDARDS – SECURITY POLICY 07

CONFIDENTIALITY STANDARDS 07

ACCESS CONTROL 07

ASSET MANAGEMENT 08

INCIDENT MANAGEMENT 08

DATA INTEGRITY AND DISPOSAL 09

SYSTEMS SECURITY 09

AWARENESS 09

SUPPORTING RESOURCES 10

DEFINITION OF TERMS

Information:	Information refers to any data that is collected, processed, stored, or shared, whether in physical or digital form. This includes personal data, such as names, addresses, phone numbers, and identification details, sensitive information like financial records, medical histories, disciplinary or academic records, and, in the context of Aotearoa New Zealand, Māori data, which pertains to information about or from Māori people, language, culture, resources, or environments. Protecting information means ensuring it is handled responsibly, safeguarded from unauthorised access, and used in compliance with privacy laws, ethical standards, and principles of Māori data sovereignty to maintain trust and security.
2 Factor or Multi Factor Authentication (2FA)	2FA adds an extra layer of security by requiring users to verify their identity using two different methods: something they know (like a password) and something they have (such as a code sent to their phone or generated by an authenticator app). This ensures that even if a password is compromised, unauthorized access is prevented without verification of the second factor.
De-identified and re-identify	De-identified refers to information that has been stripped of personal identifiers, such as names, addresses, or other details that could link the data to a specific individual. The purpose of de-identifying data is to protect privacy while still allowing the data to be used for analysis or research without revealing personal information. Re-identify means to reverse the process of de-identification, linking the de-identified data back to an individual by matching it with other data or applying techniques that restore the original identifying details. Re-identification is typically not allowed unless proper consent is obtained, as it can compromise privacy and security.
Security Framework	A security framework is a structured set of guidelines, best practices, and standards that organizations use to manage and reduce risks to their information and systems. It provides a comprehensive approach to identifying, protecting, detecting, responding to, and recovering from security threats.

RISK PROFILE

We understand that the risk of information being disclosed or compromised depends on what service you provide. While it is recognised there are exceptions, this Privacy Pledge groups the risk of information disclosure into two profiles: **HIGH RISK** and **LOW RISK**.

Each profile has differing standards for the provider (you) to meet.

HIGH RISK PROFILE	LOW RISK PROFILE
Your EdTech service captures and retains Personal Information (PI). That is information that identifies an individual, such as a student, staff member or parent/guardian at the school. For example: • Student or staff login accounts at the school. • Names and details of students • Parents email addresses • Academic Results These are examples and not an exclusive list.	Your Edtech service does not capture or retain any Personal Information (PI). The information you use, retain and share to provide your service does not identify any individual student, parent/guardian or staff member. For example: • Online service where access does not require capture of PI. • Services that a school can use that doesn't identify students, staff or parents/guardians. These are examples and not an inclusive list.

EdTech Providers as examples:

- Student Management and Learning Systems
- Teacher admin aids that capture student details.
- Enrolment services where information is recorded about students

Hail stores student/staff and parent email addresses.

LearnCoach captures student login details, school details and personal information.

EdTech Providers as examples:

Online web content or other resource that doesn't capture PI or uses anonymous access that can't identify an individual.
Portals that use generic logins.

Carerwise provides career education information to assist career advisors in High Schools.

Before you start: Consider which risk profile fits your business. If unsure, use the **HIGH RISK** profile.

Download a Word doc copy of the self-assessment here.

Upload it to your team's document management system (Google Drive, SharePoint, etc.) to collaborate and check off items as you go.

Download self-assessment word document

Use our helpful Security Portal templates and resources to assist with the completion of the self-assessment.

Security Portal

DOWNLOAD DOC ABOVE OR CONTINUE
TO START SELF ASSESSMENT FROM NEXT PAGE

PRIVACY POLICY AND SECURITY STANDARDS (SELF-ASSESSMENT)

Standards	HIGH	LOW
Privacy		
You have reviewed and complied with the Privacy Act 2020 and all other applicable regulations and laws related to protecting information. This includes appointing a Privacy Officer in your organisation. Reference: https://www.privacy.org.nz/	Yes	Yes
You and your team understand the importance and requirements of the Privacy Act including participating in awareness training that may include online education material. Reference: Online education: https://www.privacy.org.nz/tools/online-privacy-training-free/	Yes	Yes
You have developed and implemented a Privacy Policy. Reference: https://www.privacy.org.nz/tools/privacy-statement-generator/	Yes	Yes
You have published your Privacy Policy and all users of your service can access this policy. Note: This typically means posting your policy on your website.	Yes	Yes
You review your Privacy Policy annually, and when you make changes to it, you notify your users of the changes. You should also clearly show when your policy was last reviewed.	Yes	Yes
You and your team recognise the significance of Māori data sovereignty and commit to upholding its principles, including engaging in awareness training.	Yes	Yes
Disclosure		
You agree with the following disclosure statement: **Statement on Disclosure.** You will not disclose, or sell student, staff or parent/guardian information or use information for these purposes: • Marketing purposes to inform, influence, or enable advertising; • Developing a profile of a student, staff member,parent/guardian or group for any purpose other than providing the services you provide to that customer/school; • Sharing with other third-parties (unless necessary for providing the service and the party is subject to your confidentiality, privacy and security policies, such as a contractor); • AI services where the AI system uses information to learn (which necessitates retaining a copy of the information). <u>Note:</u> This does not prohibit you from using student data (i) for adaptive learning or customised student learning (including generating personalised learning recommendations); or (ii) to make product recommendations to teachers or other school staff; or (iii) to notify account holders about new education product updates, features, or services, provided that in the case of (ii) and (iii) the recipient of the recommendation or update has consented to receiving such communications.	Yes	N/A

Security Policy		
You have developed and implemented a Security Policy that outlines how your business will protect information, the personal responsibility of staff using your IT services as well as access controls.	Yes	Yes

Confidentiality Standards	HIGH	LOW
You include a confidentiality obligation in your employee agreements (or in a separate confidentiality or non-disclosure agreement that employees are required to sign).	Yes	Yes
If third-parties (such as developers or other business partners who you engage as independent contractors) have access to your services, and the information you collect and retain, then you require that they sign a confidentiality agreement with you that covers: • Terms of permitted use and confidentiality obligations; • Duration and review period; • Ownership of the information (i.e. the third party does not own it); • Obligation to return the information/not retain it.	Yes	Yes, If applicable
Student, staff and parent/guardian data is encrypted when accessed and transmitted in your service, including access via API or data transfer. This also includes storage devices that are used for backups or transfer of information.	Yes	Yes, If applicable

Access Control	HIGH	LOW
You limit who has access to your service, including using: • Unique identifiers for user accounts (students, parents/guardians, and school accounts, as examples); and • Secure authorisation process.	Yes	Yes, If applicable
You have enabled 2FA: • as an option for accounts that have a higher level of access to information, for example administration accounts; and • as a requirement for IT system level accounts.	Yes	
You restrict the number of attempted logins before access to your system is prohibited.	Yes	
You enforce password management practices that includes: • A minimum password length for all users (ideally passphrases – *see below*); or • Complex password settings requiring a password length of a minimum of 14 characters with a mix of uppercase and lowercase letters, numbers, and special characters like !, @, #. Note: If your service can enable long passphrases, it is recommended that you require the minimum length of 14 characters. Additionally, if your system allows, require new passwords to be different from previous ones to prevent reuse.	Yes	

You maintain and store system audit logs and records as needed to monitor, analyse, investigate, and report any unlawful or unauthorised system activity, for a minimum of 90 days. For financial transactions, if this is a service you provide, it is recommended that records are retained for a minimum of 12 months.	Yes	

Asset Management	HIGH	LOW
You maintain an assets registry for all the assets in your business, including: • Recording all the assets you have in your business (e.g., laptops, phones, servers) in a secure location; • Recording who owns or is responsible for each item as well serial numbers, makes/models; and • Labeling each asset (if practicable).	Yes	
Hardware Assets: • When practicable, you secure all assets with a pin or another form of authentication to restrict access to the hardware. • You maintain an assets lifecycle practice to upgrade hardware at a regular interval.	Yes	Yes, If applicable

Incident Management	HIGH	LOW
You have developed an incident management plan to be followed in the event of an unauthorised release, disclosure or access to information. Your incident management plan includes: • Incident Identification: Clear criteria to recognise when an incident plan is to be activated. • Roles and Responsibilities: Define who does what in a response. • Reporting: Procedures for reporting incidents within required timeframes. • Response Procedures: Steps to contain, resolve, and mitigate incidents. • Communication: Guidelines for internal and external communication. • Documentation: Record all actions and decisions made. • Recovery: Procedures to restore systems and operations.	Yes	
In the event of an incident occurring, including unauthorised release or disclosure of information, you agree to promptly assess whether you must inform the Privacy Commission and the impacted parties, and, if required, make the notifications within the recommended time period. Generally, if a breach notification is required, it should be made to the Privacy Commission no later than 72 hours after you are aware of the notifiable breach. Assessment of whether a notification is required should include consulting the guidance provided by the Privacy Commissioner (see below link) and/or obtaining advice from qualified privacy counsel. Reference: https://www.privacy.org.nz/responsibilities/privacy-breaches/ https://www.cert.govt.nz/report/ Note: Impacted parties may include the school(s) impacted as well as individuals, dependent upon the incident and whether PI was disclosed as a result of the incident.	Yes	

Data Integrity and Disposal	HIGH	LOW
You do not alter (including de-identifying or re-identifying) information, unless agreed by the school/customer or it is explicitly detailed in the terms of use of your service. Note: De-identifying information is encouraged where possible, but your terms should state that you will do so. Examples of common uses of de-identified information may include: assisting with academic research, analysis of service behaviors or statistical returns. These cases should be defined in your terms of use.	Yes	Yes, If applicable
You clearly define how you retain and dispose of information in your terms of use or agreement for each information type, including, when applicable: • PI; • Transactional information; • Logs; and • Financial information.	Yes	

Systems Security	HIGH	LOW
Your service operates on software that is well-maintained and kept up to date. Software that has reached end-of-life and no longer receiving security updates or support is not used. Note: Maintaining service levels requires regular updates and prompt action in response to high-priority or security alerts.	Yes	Yes
Your service provision has been optimised to include only the essential services required for your software to operate. All unnecessary programs, functions, ports, protocols, and services have been disabled.	Yes	Yes
Your service has been configured to deny network communications by default and allow communications by exception. Note: This level of protection may be provided by a Firewall.	Yes	Yes
Your service is protected from malicious code (i.e. Antivirus and Antimalware) at designated locations or end-points within organisational systems.	Yes	Yes

Awareness	HIGH	LOW
You monitor for system security alerts and advisories and when necessary prioritise appropriate action in response.	Yes	Yes
You regularly review the security controls in your organisation to assess that your service provision, security framework and alignment to this Privacy Pledge is maintained. Note: It is recommended that a designated person serves as a security lead and completes a monthly review, and that your incident management plan is reviewed regularly with all relevant personnel.	Yes	

SUPPORTING RESOURCES

To assist with the completion of this self-assessment and to raise awareness of security and privacy practices, please visit the Security Portal.

The Portal contains:

- Templates for you to use to help implement the security controls recommended. Templates can be downloaded and amended as necessary for your business.
- Further reading on the points raised in this assessment.

It is a 'self-managed' portal, and it serves to assist you.

If you have templates to share or guides that you feel will help members, please send these to support@hail.to

Security Portal

Last updated: 25 Feb 2025

Disclaimer: This Privacy Pledge is not a legally binding agreement. Your signature to the Privacy Pledge does not create any legal obligation on, or give rise to any liability to, you or your employees. The development and publication of the Privacy Pledge as a self-assessment tool for use by New Zealand's EdTech providers does not create any legal obligation on, or give rise to any legal liability to, EdTechNZ or the New Zealand Tech Alliance, or their respective board, staff or council members. The Privacy Pledge is a voluntary, self-assessment tool only and does not represent an endorsement of any signatory's services.