



# Safer Technologies for Schools Assessment: Supplier Guide

*(previously known as the ST4S Vendor Guide)*

Guide for suppliers participating in the Safer Technologies for Schools Assessment process (ST4S) covering Australian and New Zealand controls.

Release:	2023.1
Date of this version:	9 May 2024
Author:	ST4S Team
Document Version Number:	V1.1 Final
Location:	Latest official version available <a href="http://www.st4s.edu.au">www.st4s.edu.au</a>

## **Important information including disclaimer:**

This guide is provided:

- for information purposes only and does not constitute advice;
- on the basis that suppliers are responsible for assessing the relevance and accuracy of its content.

Education Services Australia Limited through its business unit the National Schools Interoperability Program (NSIP) has compiled this guide in good faith and has endeavoured to ensure that all material is accurate and does not breach any entity's rights at the time of its inclusion. However, the material may contain unintentional errors and is provided 'as is'.

Participation in the Safer Technologies for Schools (ST4S) process is voluntary. An entity which chooses to participate in the ST4S process acknowledges and agrees that:

- the ST4S process and results depend entirely on the answers provided by an entity and the point of time at which such answers are provided;
- the ST4S assessment of an entity may result in a recommendation to participating education authorities that such entity's product not be used until security/privacy issues are remedied; and
- NSIP is conducting the ST4S assessments on behalf of participating jurisdictions for the purpose of ensuring consistency in security/privacy assessments and to protect data including the personal information of students.

To the extent lawful, NSIP:

- excludes all warranties in respect of the guide and the ST4S assessment process;
- is not liable for any loss or damage (direct or indirect) resulting from the use of the guide or participation in or the results of, the ST4S assessment process; and
- will not be liable for any incidental, special or consequential damages of any nature arising from the use of or inability to use the guide or participation in the ST4S assessment process.

Links provided to other websites are provided for the user's convenience and do not constitute endorsement of those sites. ESA is not responsible for material contained in any website that is linked to from this guide.

If you use the links provided in this guide to access a third party's website, you acknowledge and agree that the terms of use, including licence terms, set out on the third party's website apply to the use which may be made of the materials on that third party's website. If this guide contains links to your website and you have any objection to such link, or if you have any questions regarding use of material available on or through this website, please contact us.

Unless otherwise indicated, the copyright in this Supplier Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Supplier Guide without the prior written permission of Education Service Australia Ltd.

## Contents

Version Control & Latest Version.....	5
1. Introduction .....	5
1.1 Purpose .....	5
1.2 Terminology .....	5
1.3 Background .....	6
1.4 Benefits of a coordinated approach .....	6
1.5 High level assessment process & prioritisation .....	7
2. Assessment process .....	7
2.1 Readiness Check.....	7
2.2 Full Assessment process .....	8
2.2.1 Assessment stages .....	9
2.2.2 Release of findings to suppliers .....	9
2.2.3 Findings outcomes .....	10
2.2.4 What do findings outcomes mean? .....	10
2.2.5 Challenging findings .....	11
2.2.6 Re-assessment .....	11
2.2.7 Changing the school level report .....	11
2.2.8 Discontinuing an assessment.....	11
3. Sharing and use of full assessment reports, findings and outcomes.....	12
3.1 Distributing reports, findings and outcomes .....	12
3.2 Sharing information .....	12
3.3 Sharing of findings with Suppliers.....	12
3.4 Supplier use of the findings internally .....	12
3.5 Guidance regarding supplier use of assessment outcomes.....	13
Requirements for non-compliant, non-participating suppliers or discontinued assessments:.....	14
Disclaimer in relation to Supplier Guide: .....	14
4. Support.....	14
5. Instructions for responding to the questionnaire and throughout the assessment process .....	15
5.1 Important information and disclaimer in relation to the questionnaire. ....	15
5.2 Completion of the questionnaire .....	15
5.3 Accuracy of responses to the questionnaire.....	16
5.4 Timeline.....	16
5.5 Other requirements .....	16
5.6 Supplier conduct .....	16
6. Assessment criteria .....	17

6.1 Criteria – Company & product detail .....	17
6.2 Criteria – Security.....	18
6.2.1 Security – Product function.....	18
6.2.2 Security – Hosting and Location.....	23
6.2.3 Security – Technical .....	24
6.2.4 Security – Logging .....	30
6.2.5 Security – Access .....	31
6.2.6 Security – HR .....	35
6.2.7 Security – Processes and Testing .....	37
6.2.8 Security – Plans and Quality.....	39
6.2.9 Security – Incidents .....	41
6.2.10 Security – Data Deletion and Retention.....	42
6.2.11 Security – Compliance Controls .....	42
6.2.12 Security – Governance .....	43
6.3 Criteria – Privacy .....	44
6.3.1 Privacy .....	44
6.3.2 Privacy – General .....	45
6.3.3 Privacy – Functionality .....	54
6.4 Criteria – Interoperability.....	71
6.4.1 Interoperability – Data Standards.....	71
6.4.2 Interoperability – Technical Integration .....	72
6.5 Criteria – Safety.....	74
6.6 Criteria – Desktop and Mobile Applications, Browser Extensions.....	75
6.7 Criteria – Informational.....	77
6.8 Evidence .....	77
6.6 Minimum criteria .....	79
6.7 Updates to the ST4S Criteria, Response Options & Minimum Standards .....	79
6.7.1 Key Changes to the ST4S Criteria (from 2022.1):.....	79
Appendix A – Tier Self-Assessment.....	81
Appendix B – Standards, Frameworks and References .....	86
Appendix C – Storage and Processing of Information .....	86

## Version Control & Latest Version

**Note: The latest copy of the ST4S Supplier Guide is available from [www.st4s.edu.au](http://www.st4s.edu.au)**

Version Control			
Version	Date:	Author/Organization:	Comments
<b>V1.0</b>	07/12/2023	ST4S Team / Education Services Australia	First release of 2023.1 framework
<b>V1.1</b>	16/02/2024	ST4S Team / Education Services Australia	Corrected control GO2 response option label, INT7 as a minimum control listed in s6.6 and updated New Zealand contact email.
<b>V1.2</b>	09/05/2024	ST4S Team / Education Services Australia	Corrections to Minimum Criteria s6.1 and additions to the Appendix item C.

## 1. Introduction

### 1.1 Purpose

This supplier guide provides guidance and information regarding:

- the assessment process;
- the initial categorisation of services/products based on assessment tiers (see Appendix A);
- the questions that make up the questionnaire;
- the minimum and indicative responses to the questions and links to relevant industry standards;
- the clarification process; and
- the assessment results and how they will be shared with participating member organisations.

### 1.2 Terminology

Term	Definition
<b>AIS</b>	Australian Independent Schools, including their bodies and representatives across States/Territories within Australia.
<b>Education authority</b>	Government or non-government ST4S member organisations responsible for ICT guidance to schools and other compulsory sector education providers in a given jurisdiction e.g. Government education departments, independent schools, catholic dioceses, New Zealand Ministry of Education
<b>ESA</b>	Education Services Australia Limited ( <a href="http://www.esa.edu.au">www.esa.edu.au</a> )
<b>NERA</b>	National Education Risk Assessment (name changed to ST4S Assessment)
<b>ST4S</b>	Safer Technologies for Schools ( <a href="http://www.st4s.edu.au">www.st4s.edu.au</a> )
<b>ST4S WG</b>	Safer Technologies for Schools Working Group
<b>NEDAG</b>	National Education Digital Advisory Group (formerly known as the NSIP Steering Group)
<b>NSIP</b>	National Schools Interoperability Program ( <a href="http://www.nsip.edu.au">www.nsip.edu.au</a> ), a business unit of ESA

### 1.3 Background

- Schools, Kura (in New Zealand) and school system authorities have obligations stemming from Federal/National and State legislation to protect the privacy and security of official information and personal information held on behalf of students, parents and staff. As the role of ICT in schools has expanded and the range of online products and services has increased, the need for a rigorous and systematic approach to managing information risk and facilitating system integration has also increased.
- The need for information risk mitigation also aligns with efforts to improve online safety for students. In 2018 the Council of Australian Governments (COAG) endorsed the National Principles for Child Safe Organisations, based on the Royal Commission's Child Safe Standards. In New Zealand, the Child and Youth Wellbeing Strategy (2019) seeks to improve the safety and wellbeing of all children, including in the online context (<https://www.childyouthwellbeing.govt.nz/>)
- As schools adopt new digital products and services, the need to streamline the on-boarding and integration of applications increases. Integration using agreed standards and APIs rather than bespoke manual data exchange (no effective integration) is key to learner centric data management and minimising administrative overheads as well as optimising privacy and security.
- At the request of the National Schools Interoperability Program Steering Group, the NSIP Team worked with agency and sector representatives to develop a standardised set of online education services risk and interoperability assessment criteria. Subject matter experts from agencies and the non-government school sectors meeting as the ST4S Working Group have developed a common evaluation process and assessment criteria covering the key domains of trust namely: security, privacy, interoperability and online safety.
- As suppliers develop and market new digital products and services to schools, they need to be aware of user safety considerations and the role that their services play in shaping online environments. The Australian eSafety Commissioner's [Safety by Design](#) is designed to provide online and digital interactive services with a universal and consistent set of realistic, actionable and achievable measures to better protect and safeguard citizens online. Suppliers are encouraged to become familiar with the Safety by Design principles. Tools and resources to support suppliers to embed user safety into the design of their products or services will be made available on the [eSafety website](#) throughout 2020.
- Safer Technologies for Schools (ST4S) commenced in 2020 in Australia following a pilot (known as the National Education Risk Assessment in 2019).
- The New Zealand Ministry of Education | Te Tāhuhu o Te Mātauranga Aotearoa, joined ST4S in 2021.

### 1.4 Benefits of a coordinated approach

- Most schools and school system authorities have established local risk assessment teams or are planning to do so.
- The anticipated benefits of a coordinated assessment approach are as follows:
  - Agreed standards and practices for the management, exchange and use of personal information in schools are clearly communicated to all school communities and product suppliers.
  - School selection of online services is guided by reliable information about privacy, security and interoperability.
  - Reduced cost, effort and time for education authorities in assessing and on-boarding online services for schools.
  - Increased transparency and trust regarding the data exchanged with service providers.
  - Reduced cost and time for suppliers to demonstrate compliance with national security, privacy and interoperability standards.
  - An incentive for suppliers to comply with security, privacy and interoperability standards.

## 1.5 High level assessment process & prioritisation

The ST4S Assessment process consists of 3 steps:

1. Suppliers complete a self-directed ST4S Readiness Check (refer [www.st4s.edu.au/readiness-check](http://www.st4s.edu.au/readiness-check)) to determine eligibility.
2. Eligible services are prioritised by the ST4S WG.
3. Prioritised services undergo a full ST4S assessment in collaboration with the ST4S Assessment team.

Importantly, the ST4S WG, in consultation with the NEDAG, is responsible for determining the assessment priority of supplier products and services. Each assessment period a limited number of services can undergo a full ST4S assessment. Results from the Readiness Check do not guarantee a priority invitation to complete, or compliance under, the full ST4S assessment.

## 2. Assessment process

A typical ST4S assessment consists of 3 steps:

1. The software supplier, at the request of schools or through their own initiative, completes an ST4S Readiness Check. If the Readiness Check outcome indicates that the product or service is 'eligible' for a Full Assessment, the supplier can optionally submit their product or service for prioritisation.
2. Products and services submitted for full assessment are verified by the ST4S Team and then prioritised by the ST4S WG. This group meets monthly and is made up of security and privacy professionals from the education sector across Australia and New Zealand. Products and services are prioritised based on members' needs and consultation with their schools.
3. Once prioritised, suppliers are invited to participate in a 'full' ST4S assessment of their product or service.

An overview of the assessment process is further described in this guide.

### 2.1 Readiness Check

The Safer Technologies 4 Schools (ST4S) Readiness Check is a self-assessment tool for suppliers. It allows suppliers to check how their product compares against the agreed privacy and security assessment framework for primary and secondary education (the ST4S assessment framework).

The ST4S Readiness Check is suitable for products and services that are used within a primary/secondary education setting and which process or handle personal or sensitive information and operate in an online environment (whether partially or entirely).

The ST4S Readiness Check consists of two steps:

- A short survey that presents critically important criteria. Upon completing the survey suppliers will be provided with some feedback about their service's readiness to complete a full ST4S assessment.
- An optional step to submit the service to be considered for a full ST4S assessment.

Once suppliers have completed the Readiness Check, the readiness status of the service will be displayed.

**If the service is not ready to submit for full assessment**, suppliers can return later to update responses once the recommended changes have been incorporated.

**If the service is ready**, suppliers can submit their results to the ST4S WG for consideration and prioritisation for a full ST4S assessment.

### Questions in the Readiness Check:

The following questions (as identified by reference numbers in this guide) are presented to suppliers in the Readiness Check:

Framework section	Control questions in Readiness Check
<i>Company and product details</i>	C0, C1, C2, C3, C4, C5
<i>Product information</i>	P1, P2, P3, P4, P5, P6, P9, P10, P11, P12, P13
<i>Hosting and location</i>	H5
<i>Security – Technical</i>	S1, S2, S3, S4, S5, S7, S8, S9, S10, S11, S13
<i>Access</i>	A1, A2, A5, A6, A7, A10, A11, A13, A16A, A16B
<i>HR</i>	HR1, HR2, HR3
<i>Processes and testing</i>	T1, T2, T3, T6, T7
<i>Plans and quality</i>	Q5, Q7
<i>Data deletion and retention</i>	D3
<i>Compliance controls</i>	CC2
<i>Privacy – Requests</i>	PR1, PR1A, PR2, PR10, PR12, PR13, PR14, PR17
<i>Privacy - Functionality</i>	PF4, PF6*, PF7*, PF8*, PF9*, PF10*, PF13*, PF36, PF51*
<i>Governance</i>	G01, G02
<i>Integrations</i>	INT5, INT7
<i>Safety Criteria and Safety Principles</i>	SC3, SC5

Please note that functionality questions marked with \* are presented based on the response to PF4.

Learn more about the ST4S Readiness Check here: [www.st4s.edu.au/readiness-check](http://www.st4s.edu.au/readiness-check)

## 2.2 Full Assessment process

Suppliers that complete the Readiness Check and are prioritised for full assessment may be invited by the ST4S Assessment Team to proceed and undertake a full assessment. This may occur days, weeks or months following the original Readiness Check submission. If a product is not nominated for an assessment and/or a new version of the ST4S framework is published, the ST4S Team may invalidate a Readiness Check submission and a new Readiness Check may be required.

Suppliers that are invited to the full assessment process will be provided with a link to the ST4S Full Assessment questionnaire and be asked the full set of ST4S control queries as represented in this guide. Suppliers are also required to provide supporting evidence and additional information throughout the assessment process.

Suppliers may also in some circumstances be invited directly to the ST4S Full Assessment. This may occur in scenarios such as where an ST4S WG member has requested a Supplier undertake the assessment process.



### 2.2.1 Assessment stages

#### **Stage 1: Submission**

Suppliers must first lodge the Full Assessment using the online questionnaire provided by the specified due date. Extensions may be requested by contacting the ST4S Team in writing and are subject to review. Please note, the Full Assessment questionnaire is in addition to the Readiness Check.

#### **Stage 2: Precheck and Evidence Review**

An initial review of the service is conducted which includes reviewing the submissions against the minimum criteria, reviewing the website, technical checks and reviewing provided documentation and evidence.

#### **Stage 3: Assessment and Report Creation**

The ST4S Team will continue with its detailed review of the service and begin drafting the ST4S school report for the service. As part of this process, suppliers are provided with an opportunity to clarify responses and additional information may be sought from the ST4S Team to complete the review process.

Suppliers may also seek to undertake additional remediation, should they wish to reduce any additional risks and improve the outcome of their assessment. Additional time to remediate is subject to review by the ST4S Team and may extend the time to complete an assessment.

#### **Stage 4: Finalisation**

Provided the service achieves a compliant outcome, the ST4S Team will provide a copy of the draft report to the supplier to review and approve to be finalised. Handling feedback of the report is described in 2.2.5 of this guide. If a service does not achieve a compliant outcome, the ST4S Team may produce another outcome (e.g. a non-compliant outcome) or choose to discontinue an assessment. Further information on outcomes is further described in this guide. If you choose not to accept a report, or we are unable to finalise a report we may discontinue the assessment.

#### **Progress Updates:**

Throughout the assessment process, the ST4S Team records an overall assessment status to the ST4S WG, NEDAG and other education authorities as described in this guide. This status may detail the service is 'pending submission', 'awaiting remediation' or another status determined by the ST4S Team. The ST4S Team does not currently communicate status updates to schools. Communication of updates, findings, outcomes etc are a local matter and are decided by the education authority, ST4S WG member and/or NEDAG as relevant.

#### **Assessment Approach:**

Where suppliers have missed a question or not provided sufficient detail, the assessment team may follow up with the submitting supplier to ensure a fair and accurate response is gathered and assessed. Where a response cannot be obtained from a supplier or the ST4S Assessment Team is satisfied there is a differing level of compliance (or non-compliance) an alternative finding may be made by the ST4S Team in order to facilitate the completion of the assessment.

### 2.2.2 Release of findings to suppliers

Suppliers will receive a draft of the school level report which is generated based on the responses provided to the supplier questionnaire. Suppliers may also receive a spreadsheet containing questions on which the assessment team is seeking further clarification. Suppliers are asked to respond to the clarifications within the timelines as directed. Supplier responses to the clarifications and a commitment to rectify any risks resulting in a 'non-compliant' outcome may alter the school report.

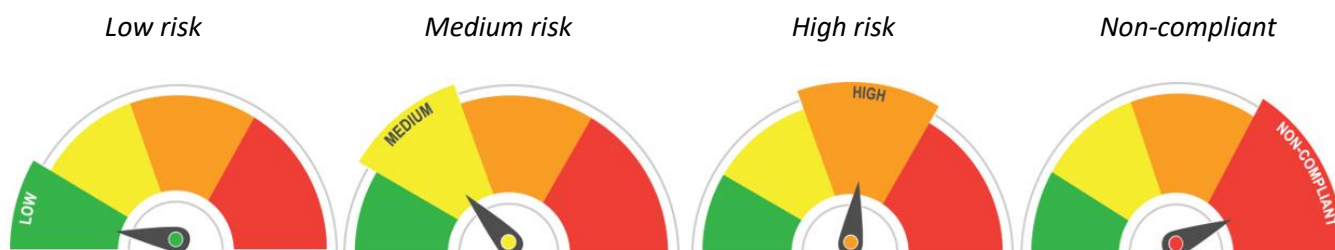
Following the successful conclusion of clarifications, suppliers should expect to receive a final school level report. A copy of the final school level report will be provided to the supplier's nominated contact. The exception to this

release timeline is where a supplier has received a non-compliant outcome, the assessment was discontinued or another outcome was determined which did not result in a report being produced.

### 2.2.3 Findings outcomes

The possible assessment outcomes depend on the 'tier' of the product or service. Tiering is dependent largely on the data processed or stored and functionality offered. To learn more about tiers, refer to Appendix A.

For Tier 1 and 2 services, the assessment of a product or service results in one of the following outcomes:



The overall assessment outcome is the highest risk level remaining after all available treatments have been applied. A 'Non-compliant' assessment outcome is assigned when a mandatory minimum standard is not met. The assessment outcome appears on the front page of the school level report.

For Tier 3 services, the assessment of a supplier's product or service results in one of the following outcomes:



Other assessment outcomes include: discontinued, non-participating, or another outcome as determined by the ST4S Team. These outcomes may or may not result in the creation of a report by the ST4S Team.

### 2.2.4 What do findings outcomes mean?

In typical school settings, there is always some risk in using a product/service. Some products/services may receive a Medium or High rating simply because of the types of functionality that they offer (for example remote access, the use of webcams, ability to chat with members of the public). The overall assessment outcome highlights to schools that in using the product/service there are treatments that need to be applied (e.g., configuration, reviewing of logs). Assigning a Medium, High, or Use with Caution outcome to a product/service is intended to draw school users' attention to the fact that treatments need to be reviewed and implemented when using the particular product/service. Typically, besides removing the particular functionality in question, there is little or nothing a supplier can do to reduce the overall assessment outcome to Low.

The most common risk achieved is a 'Medium' risk rating. This reflects the importance to schools in ensuring parental/student consent is sought prior to personal information being disclosed or shared with the service.

Products/services which have fundamental compliance gaps or have failed to meet the minimum criteria may be determined as being 'Non-Compliant', the ST4S Team may discontinue the assessment or determine another outcome.

Each education authority, ST4S WG member and/or NEDAG may determine what advice or other information they provide to schools. Suppliers should be aware that education jurisdictions, other ST4S members and/or NEDAG may

at their discretion choose to accept or reject an outcome, apply additional requirements and/or conduct their own assessment activities. Common examples include where local regulations require an education authority to conduct a privacy impact assessment (PIA), policies require additional information to be communicated to schools or a ST4S WG member may choose to only accept a certain risk level or services with data hosting that is within their jurisdiction.

Suppliers are encouraged to contact the education jurisdiction or other education authority for further information on their requirements and policies.

#### 2.2.5 Challenging findings

As part of the development of the final school level reports, suppliers will have been provided a draft copy of the school level report and clarification questions. The final school level report should not be a surprise to the supplier as the outcomes are dictated by the guidance and criteria in this guide. If a supplier considers a school level report is not accurate, that supplier may lodge a request to have their report re-reviewed. In order to request a re-review, suppliers need to provide relevant details to the ST4S Team in writing. Any challenge to a finding or outcome is first reviewed by the ST4S Team. Decisions by the ST4S Team are final. If necessary, challenges may be presented to the ST4S WG and/or NEDAG for review.

It's important to note that the ST4S framework references major standards, frameworks and criteria is set by government agencies and other members of the ST4S WG including Catholic and independent school bodies.

#### 2.2.6 Re-assessment

Subject to resourcing and prioritisation, suppliers may be invited to be re-assessed based on a number of factors, including time since original assessment, updates to the ST4S standards, updates to the supplier product/service and/or occurrence of a breach or security incident.

Suppliers may also lodge a request for a reassessment by completing the ST4S Readiness Check on the website.

#### 2.2.7 Changing the school level report

The final ST4S report can only be altered by the ST4S Team. Any request to change a school report must be made in writing to the ST4S Team.

Updates are not always a simple change to the report and outcome. For example, where a product/service is acquired by a new company, there are changes to hosting locations, features/functionality or the types of data collected, the ST4S Team may determine that a reassessment is necessary.

#### 2.2.8 Discontinuing an assessment

The ST4S Team may at any time discontinue an assessment and do so at their sole discretion. Where an assessment is discontinued, the ST4S Team will no longer conduct any assessment activities and formally close the assessment, noting the reason for discontinuing the assessment to the ST4S WG and/or NEDAG.

Assessments may be discontinued for a variety of reasons. Some examples may include:

- The service being assessed is not suitable for an assessment or the ST4S Team postpones an assessment to a newer framework.
- The service is not ready for an assessment. For example: multiple non-compliant items are responded to in the Full Assessment which would have returned a "Not Ready" outcome in the Readiness Check.
- A supplier is unable to provide evidence to a satisfactory standard
- As part of the review, the ST4S Team will send out clarifications to the supplier to seek more information or to recommend product or process changes to remove non-compliant risks. If no response is received or no action is taken on the required changes and the assessment period has gone over 6 months from the time the first pass clarifications were sent, the ST4S Team may discontinue the full assessment.
- The ST4S Team receives a request from a ST4S WG and/or NEDAG to discontinue an assessment.

If an assessment is discontinued:

- The Supplier must note their product was discontinued along with the reason when approached by a school, education authority, ST4S WG member and/or NEDAG, and
- A minimum waiting period of 3 months may apply to the supplier before it is eligible for consideration for a new assessment.

Further information on communication requirements regarding discontinued outcomes is described in this guide.

## 3. Sharing and use of full assessment reports, findings and outcomes

### 3.1 Distributing reports, findings and outcomes

The ST4S Team provides assessment findings (including raw results and school level reports) to the NEDAG (typically the Chief Information Officer at each education authority) and the ST4S WG (Chief Information Officer and/or nominated security and privacy representatives). The ST4S Team may distribute findings and outcomes to schools directly, however this is currently limited to Australian Independent Schools (AIS) and is subject to change. The process and timelines by which each education authority distributes findings is a local matter and is not managed by the ST4S Team. In some education authorities, findings will be distributed to schools within days of release from the ST4S Team, in others, schools need to make requests directly to their local education authority.

### 3.2 Sharing information

One of the goals of ST4S is for an international assessment framework across Australia and New Zealand, with collaboration from education authorities and other members of the ST4S WG and NEDAG. A standardised assessment process reduces the requirement for suppliers in providing multiple cybersecurity, privacy, and safety questionnaires.

When responding to the questionnaire and participating in the ST4S assessment process, suppliers should be aware that information provided throughout the assessment, status updates, assessment results, evidence, reports and any other information (e.g. including your contact details) may be shared with the ST4S WG, NEDAG and other parties (e.g. Trusted Parties) as nominated by the ST4S WG and/or NEDAG. This may include central department or sectoral staff and their schools and/or regional offices.

In addition, subject to approval by the NEDAG and/or the ST4S WG, results may be distributed to other parties without prior notice or consultation with the relevant supplier.

### 3.3 Sharing of findings with Suppliers

Suppliers will be provided with a copy of their school level report. These guidelines are intended to provide a sufficient level of detail so that suppliers can effectively perform a self-assessment against the assessment criteria. However, where there are critical risks the ST4S assessment team may contact suppliers directly to communicate any issues identified.

The ST4S assessment team will not provide suppliers with the findings of other suppliers who have submitted responses.

Suppliers must not provide results, findings, and outcomes themselves to schools. Instead, suppliers should refer schools to their education jurisdiction, education authority or other contact as specified in this guide.

### 3.4 Supplier use of the findings internally

One of the goals of the ST4S process is to encourage suppliers to improve, privacy, security, online safety and interoperability approaches in the design, build, testing, deployment, maintenance, configuration and end-user training regarding their product/service. Suppliers can continue to improve their products/services over time and are encouraged to continue to reference the ST4S standards (as documented in this guide) as it is updated over time.

### 3.5 Guidance regarding supplier use of assessment outcomes

Suppliers receive copies of the final assessment reports with the following caveats and conditions:

1. ST4S reports will be marked as “Not for commercial purposes”
2. Suppliers must not provide the ST4S assessment report or any copies or extracts of it to anyone outside the supplier organisation (for example, schools or school communities).
3. Suppliers may notify existing and prospective customers that they have participated in the ST4S process and meet the minimum required ST4S standards (against a specific version of the ST4S assessment standards) for the specific version of their product/service.
4. Suppliers must acknowledge and communicate with customers that an ST4S assessment outcome does not necessarily mean that the supplier is compliant with local State/Territory/Country or Non-Government sector requirements.
5. Suppliers must direct enquiries from schools regarding the provision of detailed reports to the relevant education authority (Government schools to the relevant State/Territory Department or Ministry of Education, Australian Catholic schools to their local State or Diocese office and Australian Independent schools to their State/Territory association) as listed on the final report.
6. Suppliers must not edit or modify their final or draft school-level reports in any way.
7. Suppliers must not claim that a ST4S assessment applies to other products, services, or modules offered by the supplier, or different versions of the product, service or module.
8. Suppliers must not publish, advertise or promote their specific assessment outcome (low/medium/high), or use or extract any part or portion of their ST4S report. Communications to existing and prospective customers must be limited to the particular service version that has been assessed and the result, and must indicate that this version aligns to a particular ST4S assessment standard version (compliance assessments are not enduring for all time).
9. Suppliers must not claim or imply that ST4S is an endorsement, recommendation, or approval of the product/service or a guarantee that the service is fit for purpose.
10. Suppliers must not publish in whole or in part the ST4S assessment results for another supplier’s service.
11. Suppliers must notify the ST4S Assessment Team if they come into possession of some or all of another supplier’s ST4S report or results.
12. If a supplier does not comply with the above usage conditions, the ST4S Assessment Team may rescind/withdraw/modify that supplier’s assessment outcome.
13. In its sole discretion, the ST4S Assessment Team may rescind/withdraw/modify any assessment outcome at any time.

*These guidelines will be updated from time to time. Please refer to the ST4S website ([www.st4s.edu.au](http://www.st4s.edu.au)) for the latest usage conditions*

Suppliers should direct Australian government school queries to the relevant educational jurisdiction listed below:

- Government Schools:
  - NSW [information.security@det.nsw.edu.au](mailto:information.security@det.nsw.edu.au)
  - QLD [riskreviews@qed.qld.gov.au](mailto:riskreviews@qed.qld.gov.au)
  - SA [education.ictcybersecurity@sa.gov.au](mailto:education.ictcybersecurity@sa.gov.au)
  - TAS [security@education.tas.gov.au](mailto:security@education.tas.gov.au)
  - NT [cloudsystems.doe@ntschoools.net](mailto:cloudsystems.doe@ntschoools.net)
  - WA [privacy@education.wa.edu.au](mailto:privacy@education.wa.edu.au)
  - VIC [cyber.security@education.vic.gov.au](mailto:cyber.security@education.vic.gov.au)
  - ACT [DSST@act.gov.au](mailto:DSST@act.gov.au)

Suppliers should direct Australian non-government school queries to the relevant authority listed below:

- Catholic and Independent Schools
  - Catholic Education – Contact the relevant local jurisdiction i.e. diocese, CEnet or commission.
  - Independent schools – Contact the local AIS operating in your State/Territory or at [st4s@isa.edu.au](mailto:st4s@isa.edu.au).

Suppliers should direct New Zealand school enquiries to: [digital.services@education.govt.nz](mailto:digital.services@education.govt.nz)

#### Requirements for non-compliant, non-participating suppliers or discontinued assessments:

1. If approached by current or potential customers regarding the ST4S process, suppliers must state that their outcome was non-compliant, non-participating, discontinued or another status determined by the ST4S Team as relevant, note the reason and direct schools to the relevant education authority as listed above.
2. If you have published documents, articles or other information in relation to your participation (or prior participation) within the ST4S program you must retract that information where it's reasonably practical to do so.

#### Disclaimer in relation to Supplier Guide:

1. This Supplier Guide is provided for your information only and you are responsible for ensuring that its contents are current, complete and accurate before using it.
2. Whilst ESA has endeavoured to ensure that the Supplier Guide is accurate and up-to-date, the Supplier Guide is provided to you on an 'as is' basis and you use it at your own risk.
3. To the extent lawful, NSIP:
  - excludes all warranties in respect of the Supplier Guide; and
  - is not liable for any loss or damage however caused resulting from the use or inability to use the Supplier Guide or caused to any property as a result of the use of the Supplier Guide.

## 4. Support

The ST4S Team provides support to suppliers throughout the assessment process. New suppliers are encouraged to contact the ST4S Team prior to finalising their ST4S Readiness Check submission to discuss any compliance gaps.

Queries relating to ST4S can be raised via the contact form on our website or you may contact the ST4S Team by responding to our assessment email address. Information on the standards, references and other supporting materials can be found in the appendix of this guide.

The ST4S Team will be publishing supporting materials for Suppliers on the ST4S website to provide additional information on the ST4S criteria, documentation and evidence requirements etc.



## 5. Instructions for responding to the questionnaire and throughout the assessment process

### 5.1 Important information and disclaimer in relation to the questionnaire.

If you do not agree to any of the points below, you must not complete a ST4S assessment questionnaire.

- Responses provided may be used to inform any contractual arrangements entered into by government departments, non-government sectoral authorities or individual schools.
- Please note that the ST4S school-level reports resulting from participation in ST4S do not constitute an endorsement, approval or recommendation regarding the use of the product/service to which they apply, nor do they constitute advice regarding the quality or licensing of, or the decision to purchase or use a particular product or service. ST4S assessment outcomes are provided with no guarantee or warranty.
- For the purpose of a ST4S assessment questionnaire, a reference to “Solution” means the ICT system/s your organisation intends to use to capture, store and process personal, departmental, sectoral or education data (or any form of official data).
- You may be required to provide evidence at a later date to support your responses.
- This questionnaire is:
  - necessary to meet due diligence requirements of education data being stored and used outside of internal networks or in products/services that have the ability to communicate with external networks/systems; and
  - specifically designed to elicit detail of the product, service or solution in order to inform potential end-users of the product, to detail any potential risks and mitigations and to arrive at an overall risk rating.
- Participating stakeholders outside of the ST4S assessment team may seek further detail from suppliers to address local cyber security and information security needs at a future date.
- Engagement in the assessment process and /or completion of the questionnaire does not guarantee or indicate any intention to proceed with purchasing, licensing or procurement activities.
- Participation in any stage of the ST4S assessment process or otherwise in relation to any matter concerning the ST4S assessment process, will be at each supplier’s sole risk, cost and expense. NSIP will not be responsible for any costs or expenses incurred by a supplier in preparing its response to the questionnaire or otherwise taking part in the ST4S assessment process or taking any action related to the ST4S assessment process.
- The ST4S assessment process is not an offer capable of acceptance by any person or entity or as creating any form of contractual, quasi contractual or any other rights based on legal or equitable grounds. Therefore, engagement in the ST4S assessment process and /or completion of the questionnaire does not constitute an agreement, arrangement or understanding between a supplier and NSIP, the assessment service or any stakeholders in ST4S.
- NSIP is not liable to any supplier or any other entity on the basis of any legal or equitable grounds including negligence or otherwise as a consequence of any matter or thing relating or incidental to a supplier’s participation in the ST4S assessment process.
- The questions below directly relate to the requirements contained within the various and relevant privacy acts and the various Government information security classification frameworks. Supplier responses will assist in the assessment, mitigation and monitoring of the risks associated with their product/service.

### 5.2 Completion of the questionnaire

- Suppliers will receive, via email, a link to complete a questionnaire for a specific nominated service/product. A survey access pin will be sent via text message to the nominated contact.
- Suppliers ideally make a submission for both Australian and New Zealand education authorities. Where suppliers only operate in one country they may elect to submit for a single country.

- All questions are mandatory, and suppliers will not be able to navigate between pages without first completing the questions on the page displayed.
- If at any time suppliers are not sure which product, module or component is the subject of the response, please contact the assessment team.
- If the supplier's service offers a 'for school use' and a 'for home use' version, please complete the questionnaire based on the 'for school use' version.
- If suppliers need to provide any attachments which are directly relevant to the question being asked (please do not provide advertising materials or lengthy documents) prefix the file name with the relevant question ID e.g. INT3-API Product XYZ).
- Suppliers will be able to partially complete the questionnaire and return at a later time to complete it.
- Suppliers may choose to print a copy of their responses to the questionnaire prior to submitting.
- Suppliers can contact the assessment team if they have any questions or comments. We are here to help.

### 5.3 Accuracy of responses to the questionnaire

In submitting the questionnaire, suppliers must:

- confirm all information provided in response to the questionnaire is true, correct, accurate, up-to-date, and not misleading in any way;
- acknowledge that:
  - the ST4S assessment team will rely on the information provided in response to the questionnaire to assess the service's compliance and provide guidance to stakeholders;
  - incomplete, inaccurate, out of date or misleading information may result in the relevant service receiving an inaccurate or misleading report; and
  - agree to provide further information or evidence to support the questionnaire responses if requested.

### 5.4 Timeline

Timelines to submit the self-assessment questionnaire are included in the assessment information email sent to suppliers.

The ST4S is a detailed audit and review process. Time to complete an assessment varies depending on the complexity of the service, the types of data being provided, priorities set by the ST4S WG and other factors. Suppliers should allow at least 3 months from submission of the Full Assessment questionnaire.

### 5.5 Other requirements

Throughout the assessment process, the ST4S Team may request a supplier to provide additional support to assist in reviewing the service. This may include requesting a demo or trial account for the service, requesting access to support materials (e.g. user guides and manuals) or a service's terms and conditions and privacy policy if these are not publicly available etc.

### 5.6 Supplier conduct

Suppliers are expected to demonstrate care and skill when engaging in the ST4S assessment process, be transparent, adhere to the conditions in this guide and not engage in misconduct. Examples of misconduct include plagiarism, attempting to solicit an outcome, engaging in misleading and deceptive conduct. Suppliers that engage in misconduct may have their assessment discontinued, determined non-compliant or the ST4S Team may take any other action it deems appropriate. Misconduct may be referred to the ST4S WG and/or NEDAG.



## 6. Assessment criteria

When reviewing the assessment criteria, in the response options column:

- the minimum acceptable response is in bold and may differ depending on the tier of the service.
- the relevant assessment tier is written in brackets as a prefix to the minimum acceptable response, where “T1” means Tier 1, “T2” means Tier 2, and “T1, T2” means both Tier 1 and Tier 2. Where a country code is also provided (e.g., for control H6 – AU T1, AU T2), this indicates that this response is a minimum for that particular country only.
- a hash # (also known as an octothorpe) indicates that the question is of high importance. Failure to meet the minimum acceptable response will result in a “Non-compliant” assessment outcome.
- Further information on the referenced standards, frameworks and other materials can be found in Appendix B.

### 6.1 Criteria – Company & product detail

#	Question	Tier	Notes
<b>C0</b>	For which countries are you submitting an ST4S survey response?	1 & 2	Response options: A. Australia and New Zealand B. Australia only C. New Zealand only
<b>C1</b>	Vendor name	1 & 2	Informational
<b>C2A</b>	Vendor ABN	1 & 2	Informational (AU submissions)
<b>C2B</b>	Vendor NZBN	1 & 2	Informational (NZ submissions)
<b>C3A</b>	Registered Australian address of vendor	1 & 2	Informational (AU submissions)
<b>C3B</b>	Registered New Zealand address of vendor	1 & 2	Informational (NZ submissions)
<b>C4A</b>	Country in which the company is registered for Australian customers	1 & 2	Informational (AU submissions)
<b>C4B</b>	Country in which the company is registered for New Zealand customers	1 & 2	Informational (NZ submissions)
<b>C5A</b>	For Australian customers: Preferred vendor contact name Preferred vendor contact email Preferred vendor contact phone number	1 & 2	Informational (AU submissions)
<b>C5B</b>	For New Zealand customers: Preferred vendor contact name Preferred vendor contact email Preferred vendor contact phone number	1 & 2	Informational (NZ submissions)

## 6.2 Criteria – Security

### 6.2.1 Security – Product function

Q	Question	Tier	Response options	Standard / References
P1	Name of service	All		
P2A	Version of service <i>If no published version number, use date of version.</i>	All		
P2B	Is the service free or paid?	All	A. Free B. Paid	
P2C	For paid services, URL of pricing page	All		
P2D	Are you the product or service's original developer, a re-seller or 'other'?	All	A. Original developer B. Reseller C. Other (please specify)	
P2E	Do you warrant that you have the legal authority to submit this product or service for an ST4S assessment?	All	A. No# B. Yes (T1, T2)	
P2F	Does your organisation outsource any development, maintenance or operation activities to another organisation?	All	A. No B. Yes (please specify)	
P3A	URL of service for Australian customers	All		
P3B	URL of service for New Zealand customers	All		
P4A	URL of Terms of Service/use for Australian customers	All		
P4B	URL of Terms of Service/use for New Zealand customers	All		
P5	Purpose of the service?	All		
P6	In what jurisdiction would disputes, regarding usage of the service, be handled? (e.g., Victoria Australia, New Zealand)	1 & 2		
P7	Does your organisation have a current insurance policy of at least \$1M AUD with claims for data breach/loss?	1	A. <b>Yes - current policy with coverage of at least \$1 million AUD (T1)</b> B. Yes - current policy but coverage is less than \$1 million AUD C. No current policy	

<b>P8</b>	<p>Is this service dependent on another IT service to function according to its intended purpose? (e.g., does this service have YouTube embedded or rely on Facebook logins?)</p> <p><i>For example, does the service utilise any third party/outsourced:</i></p> <ul style="list-style-type: none"> <li>- plug ins</li> <li>- browser extensions</li> <li>- hosting services</li> <li>- video streaming services (e.g., YouTube, Vimeo)</li> <li>- image hosting services</li> <li>- publishing services etc.</li> </ul>	All	<p>A. Yes, please specify</p> <p>B. No</p>	NZISM 12.7
<b>P9</b>	<p>When using the service for its intended purpose, what, if any, of the data types below would reasonably be captured, stored, or processed by the service? Select all that apply.</p> <p><b>Sensitive information</b> is a type of personal information that is given extra protection and must be treated with additional care. If in doubt, select this option. Sensitive information may include:</p> <ul style="list-style-type: none"> <li>- Protection details (i.e., whether the user is under a protection order and/or the details of the order)</li> <li>- Legal custodian arrangements and court orders</li> <li>- Out of home care status</li> <li>- Records of behaviour incidents/discipline, behavioural observations/notes</li> <li>- Consent (e.g., collection and/or recording of consent)</li> <li>- Student absence details (i.e., records of attendance and reason for absence)</li> <li>- Records of contact (e.g., between parents, teacher, school, and/or student) and other agencies</li> <li>- Student/Learning support service information and support arrangements</li> </ul>	All	<ul style="list-style-type: none"> <li>•Protection order details (student)</li> <li>•Legal custodial arrangements (student)</li> <li>•Informal custodial arrangements</li> <li>•Legal status (criminal convictions, protection orders, police checks results etc)</li> <li>•Out of home care status (student)</li> <li>•Records of behaviour incidents (student)</li> <li>•Records of incidents</li> <li>•Behavioural observations/notes (student)</li> <li>•Records of contact or interview (student)</li> <li>•Sensitive social, emotional or mental health and well-being information (staff, student, parent)</li> <li>•Support arrangements (student)</li> <li>•Professional case notes (student)</li> <li>•Reason for absence (student)</li> <li>•Commonwealth Unique Student Identifier (AU) or National Student Number (NZ)</li> <li>•Health and medical details, including mental health diagnoses (staff, student, parent)</li> <li>•Financial information (staff, student, parent, organisation)</li> </ul>	NZ PSR – INFOSEC1

	- Enrolment support records (sensitive case, complex case, adjustments, student plan, developmental map, transportation, Individual Education Plans, Oranga Tamariki 'All about Me' plan)		<ul style="list-style-type: none"> <li>• Identification documentation (staff, student, parent)</li> <li>• Digital signature (staff, student, parent)</li> <li>• Government related Identifiers (e.g., state or federal government assigned identifiers)</li> <li>• Official records</li> <li>• Racial or ethnic origin</li> <li>• Religious beliefs or affiliations</li> <li>• Sexual orientation or practices</li> <li>• Biometric information (e.g., eye/retinal/facial imagery, fingerprints, biometric templates)</li> <li>• Location tracking data (Information about the ongoing geographic positions of individuals or devices derived from GPS or other network sources. Examples include: Current position in time and retained point in time, ongoing positions of individuals, cellular network connection tracking, BLE (Bluetooth Light Energy) beacons communication)</li> <li>• Use of social services (Work &amp; Income, ACC, CYPS, Women's refuge etc)</li> <li>• None of the above (T2)</li> </ul>	
<b>P10</b>	Select the functionality available within the service. Select all that apply.	All	<ul style="list-style-type: none"> <li>• Online meetings, video or audio conferencing, livestreaming (T1)</li> <li>• Consent Management (T1)</li> <li>• Financial management or payment processing systems (T1)</li> <li>• Enrolment management (T1)</li> <li>• Student information, student management system, school administration or student administration system (T1)</li> <li>• Customer relationship management (T1)</li> <li>• Ticketing system - Service Management, Helpdesk (T1)</li> <li>• Learning management system (T1)</li> </ul>	

			<ul style="list-style-type: none"> <li>• Electronic document and records management systems (T1)</li> <li>• File hosting and synchronisation (T1)</li> <li>• Remote access (T1)</li> <li>• Data collection tools (non-curriculum) (T1)</li> <li>• Photo, image, video or audio storage, sharing and backup services (T1)</li> <li>• Two-way communication tools (T1)</li> <li>• Data aggregation, Data broker, Data hub, Data distribution hub (T1)</li> <li>• Software and cloud developer tools (T1)</li> <li>• Mobile device management (MDM) (T1)</li> <li>• Authentication services (T1)</li> <li>• Collaboration and sharing (T2)</li> <li>• One-way communication tools (T2)</li> <li>• Career education, planning and guidance (T2)</li> <li>• Vocational training providers and courses, industry/employment registers, work placements (T2)</li> <li>• Learning activities, assessments and games (T2)</li> <li>• Content creation, presentation tools and publishing (T2)</li> <li>• Educational resources and content libraries (T2)</li> <li>• File download, including executables (T2)</li> <li>• Library Management (T2)</li> <li>• Visitor Management (T2)</li> <li>• Event management, bookings, online ordering or fundraising (T2)</li> <li>• Administrative support services and tools (T2)</li> <li>• None of the above (T2)</li> </ul>	
<b>P11</b>	Does the service contain, display, or promote the following via any means (social media or news feed, direct advertising, pop-ups):	All	A. Yes (please specify) <b>B. No (T1,T2)</b>	

	<ul style="list-style-type: none"> <li>- Products/services: alcohol, controlled or banned substances, gambling, tobacco products, firearms and fire arm clubs, adult products and pornography.</li> <li>- Categories of information which may be deemed offensive by a reasonable member of the school community (e.g., racist, sexist, pornographic content etc.)</li> </ul>			
<b>P12</b>	<p>With regards to any third-party providers that make up the solution, or provide service to you, does your organisation:</p> <ul style="list-style-type: none"> <li>• have an inventory of all third-party service providers;</li> <li>• regularly assess and manage the risks associated with these third-party providers; and</li> <li>• have contractual agreements in place to ensure third-party providers adhere to your information security and privacy policies?</li> </ul>	1	<p>A. No  B. Yes - for some third-party providers  <b>C. Yes - for all third party-providers (T1)</b>  <b>D. NA - solution does not use third party providers (T1)</b></p>	<p>NZ PSR - GOV5  NZISM 12.7  NZPP-5  NZPP-11</p>
<b>P13</b>	For the service being assessed, what is the deployment architecture used for customers?	All	<p>A. Hosted in customer environment  B. Hosted in environment owned or managed by your organisation  C. Both hosted in customer environment and an environment owned or managed by your organisation</p>	
<b>P14</b>	Is the service compliant with the WCAG 2.1 Accessibility guidelines as per <a href="https://www.w3.org/WAI/standards-guidelines/wcag/">https://www.w3.org/WAI/standards-guidelines/wcag/</a>	All	<p>A. No  B. Yes – all components meet WCAG 2.1 AAA  C. Yes – all components meet minimum of WCAG 2.1 AA  <b>D. Yes – all components meet minimum WCAG 2.1 A (T1, T2)</b></p>	NZ Govt Web Standards
<b>P15</b>	Does your organisation seek to absolve indemnity from any legal liabilities with regards to the operation of the service?	1 & 2	<p><b>A. No (T1, T2)</b>  B. Yes, outlined in publicly available terms of service or other public document or public location (please specify and provide link)  C. Yes, outlined in a non-publicly available document or non-publicly available location and not actively provided to customers</p>	

			D. Yes, outlined in a document the vendor proactively provides to all customers prior to contract phase	
--	--	--	---	--

## 6.2.2 Security – Hosting and Location

Q	Question	Tier	Response options	Standard / References
H1	Select the option which best describes where user data or any related data (e.g., metadata, logs, user content) is stored or processed across all components of the service, including live solution, backup, disaster recovery, test environment, and development environments.	1 & 2	<b>A. Entirely in a country nominated by the customer (specify supported countries for Australian and New Zealand customers) (T1, T2)</b> B. Entirely in a single vendor nominated country (specify country) C. In multiple vendor nominated countries: - Live solution (please specify country/s) - Other components (backup, etc) (please specify country/s)	AUISM Security Control: 1452 Revision 3 NZISM 22.1.22 NZISM 12.7 NZPP-11
H2	From what countries do vendor staff, including support, administration, development and testing, and external contractors or associates, access user data and any related data (e.g., metadata, logs) collected or used by the service (including backups and recovery)?	1 & 2	<b>A. Entirely from Australia and / or New Zealand (please specify)</b> B. From other countries (please specify country/s)	AUISM Security Control: 0975 Revision 7 NZISM 22.1.22 NZISM 12.7
H3	Retired (2022)			
H4	At a minimum, are the following physical access controls in place at the locations where data is stored: <ul style="list-style-type: none"> <li>• No public access;</li> <li>• Visitor access only for visitors with a need to know and with a close escort;</li> <li>• Restricted access for authorised personnel with appropriate security clearance;</li> <li>• Single factor authentication for access control using secure swipe card, biometrics, coded access, other; and</li> <li>• Security alarm system?</li> </ul>	1	<b>A. Yes – all of the above (T1)</b> B. Yes – some of the above C. No – none of the above	AUISM Security Control: 1296 NZISM 8

<b>H5#</b>	Would customers be notified of any relocation or expansion (i.e. change of country) of: <ul style="list-style-type: none"> <li>the cloud infrastructure, including system components, user data and related data; and</li> <li>any person (vendor or cloud infrastructure staff, external contractors or associates) with access to unencrypted customer data or any person with a means of accessing or extracting unencrypted data (e.g., those with access to encryption keys and encrypted customer data), prior to relocation?</li> </ul>	1 & 2	A. No (#T1, #T2) <b>B. Yes (specify average notification lead time) (T1, T2)</b>	AUISM Security Control: 1578 Revision 0 NZISM 22.1.22 NZISM 12.7
<b>H6</b>	Are all hosting providers, cloud-based services and other service components IRAP assessed?  See <a href="https://www.cyber.gov.au/irap">https://www.cyber.gov.au/irap</a> for information about IRAP assessment.	1 & 2	A. No or unknown B. Yes – some hosting providers, cloud-based services and other components are IRAP assessed <b>C. Yes – all cloud-based services and other components are IRAP assessed (T1, T2)</b>	AUISM Security Control: 1570 Revision 0

### 6.2.3 Security – Technical

Q	Question	Tier	Response options	Standard / References
<b>S1#</b>	What are the minimum encryption algorithms applied to protect all data <b>in transit</b> over networks, including encryption of data that is communicated between the user, web applications and system components (e.g., database systems)?	1 & 2	A. No encryption (#T1, #T2)  B. Encryption: DES, RC4, 3DES using three distinct keys; (#T1, #T2) Hashing: Message Digest (MD to MD6), RIPEMD-128 or above, SHA-0, SHA-1; Digital Signatures: DSA (1024) or RSA (1024); Key Exchange: DH (1024) or RSA (1024); Protocol: TLS1.1 or below  <b>C. Encryption: AES 128 or above;  Hashing: SHA-224 or above  Digital Signatures: DSA (2048) FIPS 186-4, ECDSA (224+) preferably using NIST P-384 curve or RSA (1024+);</b>	AUISM Security Control: 1139, revision 5; ISM Security Control: 0471, revision 6; AUISM Security Control: 1277, revision 2. AUISM Security Control: 0994. NZISM 17.2 NZISM 17.3



			<p><b>Key Exchange: DH (2048+), ECDH (256+) preferably using NIST P-384 curve and/or RSA (2048+);</b>  <b>Protocol: TLS 1.2 or above only(T2)</b></p> <p><b>D. Encryption: AES 192 GCM/CCM, CHACHA20 POLY 1305 or above only (AES 256 GCM/CCM recommended);</b>  <b>Hashing: SHA-256 or above only (SHA-384 recommended);</b>  <b>Digital Signatures: DSA (2048+) FIPS 186-4, ECDSA (224+) using NIST P-384 curve or RSA (2048+);</b>  <b>Key Exchange: DH (3072+), ECDH (256+) using NIST P-384 curve and/or RSA (3072+);</b>  <b>Protocol: TLS 1.2 or above only (TLS 1.3 recommended) (T1)</b></p>	
<b>S2#</b>	What are the minimum encryption algorithms applied to protect data at rest, including backups, data storage and auditable logs?	1 & 2	<p>A. No encryption (#T1, #T2)  B. DES, RC4, 3DES using three distinct keys  <b>C. AES 128 (T2)</b>  <b>D. AES 192, AES 256 (AES 256 recommended) (T1)</b>  E. Encryption algorithm equivalent to options C or D (please specify equivalent algorithms)</p>	AUSIM Security Control: 0459, revision 3 NZISM 17.2
<b>S3#</b>	If customer data is uploaded to the service using a mechanism such as encrypted USB, SFTP, Secure API, etc., what are the minimum encryption methodologies applied?	1 & 2	<p>A. No encryption (#T1, #T2)</p> <p>B. Encryption: DES, RC4, 3DES using three distinct keys; (#T1, #T2)  Hashing: Message Digest (MD to MD6), RIPEMD-128 or above, Secure Hash Function (SHA-0, SHA-1);  Digital Signatures: DSA (1024) RSA (1024);  Key Exchange: DH (1024), RSA (1024);  Protocol: TLS 1.1 or below</p> <p><b>C. Encryption: AES 128 or above;</b>  <b>Hashing: SHA-224 or above</b></p>	AUSIM Security Control: 1139, revision 5; AUSIM Security Control: 0471, revision 6; AUSIM Security Control: 0472, revision 6; AUSIM Security Control 1759, revision 0; AUSIM Security Control 0474, revision 6; AUSIM Security Control 1761, revision 0;

			<p><b>Digital Signatures: DSA (2048) FIPS 186-4, ECDSA (224+) preferably using NIST P-384 curve or RSA (1024+);</b>  <b>Key Exchange: DH (2048+), ECDH (256+) preferably using NIST P-384 curve and/or RSA (2048+);</b>  <b>Protocol: TLS 1.2 or above only(T2)</b></p> <p><b>D. Encryption: AES 192 GCM/CCM, CHACHA20 POLY 1305 or above only (AES 256 GCM/CCM recommended);</b>  <b>Hashing: SHA-256 or above only (SHA-384 recommended);</b>  <b>Digital Signatures: DSA (2048+) FIPS 186-4, ECDSA (224+) using NIST P-384 curve or RSA (2048+);</b>  <b>Key Exchange: DH (3072+), ECDH (256+) using NIST P-384 curve and/or RSA (3072+);</b>  <b>Protocol: TLS 1.2 or above only (TLS 1.3 recommended) (T1)</b></p> <p>E. N/A - Customer data is not uploaded to the service</p>	<p>NZISM 17.2  NZISM 17.3</p>
<b>S4#</b>	<p>If multi-tenancy is used (i.e. system components are shared between multiple customers), are partitioning controls implemented to securely segregate one customer's data from another customer's data? E.g.</p> <ul style="list-style-type: none"> <li>Assign a unique customer ID when same table is used to store multiple customers' data</li> <li>Use separate table or database for each customer</li> <li>Use a separate instance, environment or VPC</li> </ul>	1 & 2	<p><b>A. Yes (T1, T2)</b>  <b>B. No (#T1, #T2)</b>  <b>C. Not applicable</b></p>	<p>AUISM Security Control: 1436, revision 1  NZISM 10.8  NZISM 22.2</p>
<b>S5#</b>	<p>Are all of the service's web servers secured with digital certificates signed by a reputable trusted authority?</p>	1 & 2	<p><b>A. Yes (please specify CA) (T1, T2)</b>  <b>B. No (#T1, #T2)</b></p>	<p>AUISM Security Control: 1161  NZISM 17.1  NZISM 17.2</p>

<b>S6</b>	<p>Does your organisation have a documented and implemented key management process which describes at a minimum:</p> <ul style="list-style-type: none"> <li>• Key generation;</li> <li>• Key registration;</li> <li>• Key storage;</li> <li>• Key distribution and installation;</li> <li>• Key use;</li> <li>• Key rotation;</li> <li>• Key backup;</li> <li>• Key recovery;</li> <li>• Key revocation;</li> <li>• Key suspension; and</li> <li>• Key destruction?</li> </ul>	1	<p>A. No - none of the above  B. Yes - some of the above  <b>C. Yes - all of the above (T1)</b></p>	NZISM 17.9
<b>S7#</b>	<p>Are production servers (e.g., authentication servers, Domain Name System (DNS), web servers, file servers and email servers), containers, serverless services and all end points protected by:</p> <ul style="list-style-type: none"> <li>- Host based intrusion detection and prevention systems (HIPS, IDS/IPS);</li> <li>- Software-based application firewalls / web application firewalls (WAF);</li> <li>- Anti-virus and malware detection</li> </ul>	1 & 2	<p>A. No - none of the above (#T1, #T2)  B. Yes - some of the above  <b>C. Yes – all of the above except HIPS, IDS/IPS (T2)</b>  <b>D. Yes - all of the above (T1)</b></p>	<p>AUISM Security Controls:  1341, 1034, 1416, 1417  NZISM 14.1  NZISM 18.4</p>
<b>S8#</b>	<p>Does your organisation enforce the following controls on database management system (DBMS) software:</p> <ul style="list-style-type: none"> <li>• Follow vendor guidance for securing the database;</li> <li>• DBMS software features and stored procedures, accounts and databases that are not required are disabled or removed;</li> <li>• Least privileges;</li> <li>• File-based access controls;</li> <li>• Disable anonymous and default database administrator account;</li> </ul>	1 & 2	<p>A. No - none of the above (#T1, #T2)  B. Yes - some of the above  <b>C. Yes - all of the above (T1, T2)</b></p>	<p>AUISM Security Controls:  1246, 1247, 1249, 1250,  1260, 1262, 1263, 1273  NZISM 20.4  NZISM 14.1  NZISM 10.8</p>

	<ul style="list-style-type: none"> <li>• Unique username and password for each database administrator account;</li> <li>• Use database administrator accounts for administrative tasks only; and</li> <li>• Segregate test and production environment?</li> </ul>			
<b>S9#</b>	<p>Are internet facing components (e.g., web servers) separated from other online components (e.g. databases) using the following controls:</p> <ul style="list-style-type: none"> <li>• Secure communication between network segments (e.g., using firewalls), including filtering between network segments</li> <li>• DMZ for internet-facing components and separate trusted zones for other components</li> <li>• Virtual (e.g., VLAN) or physical network segregation</li> </ul>	1 & 2	<p>A. No – none of the above (#T1)  B. Partial – secure communication or DMZ  C. Partial – virtual or physical network segregation (T2)  <b>D. Yes – all of the above (T1, T2)</b></p>	<p>AUISM Security controls:  1181, 1577, 1532, 0529,  1364, 0535, 0530, 0520,  1182, 0385, 1479, 1006,  1437, 1436, 0628  NZISM 10.8  NZISM 14.1.11  NZISM 19.1  NZISM 22.2</p>
<b>S10#</b>	<p>Does your organisation have a documented and implemented system hardening process which:</p> <ul style="list-style-type: none"> <li>• Includes in scope operating systems, virtualization platforms, storage, network, applications, workstations and other end-user devices;</li> <li>• Includes the management of default user accounts and access levels and the uninstallation or disablement of the unnecessary services;</li> <li>• Ensures only required ports, protocols, services and authorisations are enabled (all others are restricted); and</li> <li>• Is reviewed annually and when significant changes occur?</li> </ul>	1 & 2	<p>A. No – none of the above (#T1, #T2)  B. Yes – some of the above  C. Yes – all of the above except annual review (T2)  <b>D. Yes – all of the above (T1)</b></p>	<p>AUISM Security Control:  1406 Revision: 2; Security Control: 1585 Revision: 0;  Security Control: 1605 Revision: 0;  Security Control: 1588 Revision: 0.  NZISM 14.1  NZISM 22.2</p>
<b>S11#</b>	<p>Has your organisation implemented the following perimeter controls:</p> <ul style="list-style-type: none"> <li>• External Firewall;</li> </ul>	1 & 2	<p>A. No - none of the above (#T1, #T2)  B. Yes - some of the above  <b>C. Yes - all of the above except for Web Application Firewall (WAF) (T2)</b></p>	<p>AUISM Security Control:  1528 Revision: 1; Security Control: 1435; Revision: 1.  NZISM 10.8</p>

	<ul style="list-style-type: none"> <li>• IDS/IPS (Intrusion Detection System/Intrusion Prevention System);</li> <li>• DMZ (Demilitarised Zone) for hosting external sites;</li> <li>• Content filtering (including blocking of unnecessary file types);</li> <li>• DoS/DDoS (Denial of Service/Distributed Denial of Service) defence;</li> <li>• Web Application Firewall (WAF);</li> <li>• Filtering and monitoring of outgoing traffic (spikes, unusual activity, malicious content);</li> <li>• Network segmentation;</li> <li>• VPN required for remote access;</li> <li>• Detection and monitoring of unauthorised devices on the network;</li> <li>• DNS filtering and network URL based filters; and</li> <li>• Organisation assets are configured to use trusted DNS servers?</li> </ul>		<b>D. Yes - all of the above (T1)</b>	NZISM 18.4 NZISM 19.1 NZISM 19.3
<b>S12</b>	Has your organisation documented and implemented a security policy governing the management of mobile devices, including use of a Mobile Device Management solution applied to all mobile devices?	1 & 2	A. No - none of the above (T2) B. Policy documented and implemented, but MDM not applied to all devices (T2) <b>C. Yes - all of the above (T1)</b>	NZISM 21.1 NZISM 21.4
<b>S13#</b>	Is production data used in non-production (e.g., test and development) environments?	1 & 2	A. Yes – without identical security controls applied and de-identification of production data. (#T1, #T2) B. Yes - with identical security controls applied and/or with production data de-identified (T1, T2) <b>C. No (T1, T2)</b>	AUISM Security Control: 1420 Revision: 2. NZISM 14.4 NZISM 20.1

<b>S14</b>	<p>Does your organisation:</p> <ul style="list-style-type: none"> <li>- disable the internal use of business productivity tool macros (e.g., Microsoft Office macros) and scripts (VB, java, PowerShell) for users that don't have a demonstrated business requirement;</li> <li>- block macros in files originating from the internet;</li> <li>- enable macro antivirus scanning; and</li> <li>- ensure macro security settings can't be changed by users?</li> </ul>	1 & 2	<p>A. No  B. Yes – some of the above  <b>C. Yes – all of the above (T1, T2)</b>  <b>D. N/A (T1, T2)</b></p>	<p>AUISM Security Controls:  1487, 1488, 1489  NZISM 20.3</p>
------------	---	-------	---	---

#### 6.2.4 Security – Logging

Q	Question	Tier	Response options	Standard / References
<b>L1</b>	<p>Does your organisation have a documented and implemented logging procedure which requires all systems in your organisation (e.g., servers, storage, network, applications, etc.) to log the following and synchronise logs to a consistent time source:</p> <ul style="list-style-type: none"> <li>• Authentication logs (e.g., successful login, unsuccessful login, logoff)</li> <li>• Privileged operations logs (e.g., access to logs, changes to configurations or policy, failed attempts to access data and resources)</li> <li>• User administration logs (e.g., addition/ removal of users, changes to accounts, password changes)</li> <li>• System logs (e.g., system shutdown/ restarts, application crashes and error messages)</li> </ul>	1 & 2	<p>A. No - none of the above  B. Yes - some of the above (T2)  <b>C. Yes - all of the above (T1)</b></p>	<p>AUISM Security Controls:  0584, 0585, 0582, 1536, 1537  NZISM 16.6</p>

<b>L2</b>	Does your organisation have a documented and implemented event log auditing procedure which outlines, at a minimum: <ul style="list-style-type: none"> <li>• Schedule of audits (annual or real-time for sensitive data);</li> <li>• Definitions of security violations;</li> <li>• Actions to be taken when violations are detected; and</li> <li>• Reporting requirements?</li> </ul>	1 & 2	A. No <b>B. Yes - all of the above without real-time monitoring (T2)</b> <b>C. Yes - all of the above with real-time monitoring (T1)</b>	AUISM Security Control: 0109 NZISM 7.1.7 NZISM 16.6
<b>L3</b>	Will you supply all relevant audit and logging data in response to customer requests?	1 & 2	A. No <b>B. Yes (T1, T2)</b>	
<b>L4</b>	Has your organisation implemented a centralised logging facility to store logs?	1	A. No <b>B. Yes (T1)</b>	AUISM Security Control: 1405 NZISM 16.6 NZISM 18.4.12

#### 6.2.5 Security – Access

Q	Question	Tier	Response options	Standard / References
<b>A1#</b>	Are all users of the service (e.g. Teachers, Parents, Students, Admins etc) required to be uniquely authenticated and identifiable within the service (e.g. each user is assigned a username and login credential)?	1 & 2	A. No <b>B. Yes for all users – excluding students (Please detail why this exception is required and specify any controls in place for students) (T1, T2)</b> <b>C. Yes for all users (T1, T2)</b>	AUISM Security Control: 0414 NZISM 16.1
<b>A2#</b>	Are all passwords used to access the service (i.e. end-users of the service, system, and privileged account passwords): <ul style="list-style-type: none"> <li>• Protected in line with at least one of the following: <ul style="list-style-type: none"> <li>○ Australian Cyber Security Centre Information Security Manual (ISM);</li> <li>○ New Zealand Information Security Manual;</li> <li>○ OWASP Application Security Verification Standard.</li> </ul> </li> <li>• Minimum 14 characters with complexity (e.g. letters, symbols and numbers), and</li> <li>• Hashed, salted and encrypted following the recommendations by OWASP.</li> </ul>	1 & 2	A. No (#T1, #T2) <b>B. Yes for all users – excluding students (T1, T2). Please detail why this exception is required and specify any controls in place for student accounts.</b> <b>C. Yes for all users (T1, T2)</b>	AUISM Security Control: 1252 NZISM 16.1 NZISM 16.1.41

<b>A3</b>	At a minimum, are the following password requirements enforced for vendor staff, external contractors or associates with access to the organisation's systems and the service: <ul style="list-style-type: none"> <li>• if using single factor authentication, passwords are a minimum of 14 characters with controls that limit predictability (inc. complexity)</li> <li>• if using multi-factor authentication, passwords are a minimum of six characters</li> </ul>	1 & 2	A. No <b>B. Yes (T1, T2)</b>	AUISM Security Control: 0421, 1559 NZISM 16.1
<b>A4</b>	Within the service, do you offer multi-factor authentication for end-users?	1	A. No <b>B. Yes, offered as an option (T1)</b> <b>C. Yes, mandated for end users (T1)</b>	AUISM Security Control: 0974 NZISM 16.1 NZISM 21.4.11
<b>A5#</b>	Does your organisation <b>mandate</b> two factor authentication for: <ul style="list-style-type: none"> <li>• Vendor staff, external contractors or associates accessing systems remotely;</li> <li>• System administrators;</li> <li>• Support staff; and</li> <li>• Staff with privileged accounts?</li> </ul>	1 & 2	A. No – none of the above (#T1) B. Yes – some of the above (#T1) <b>C. Yes – all of the above (T1, T2)</b>	AUISM Security Control: 1173 Revision 3 NZISM 16.4 NZISM 16.7 NZISM 19.1.20 NZISM 21.4.11
<b>A6#</b>	Does your organisation provide access to systems based on roles (e.g., role-based access control (RBAC)), and is this process documented for all systems including the service?	1 & 2	A. No (#T1) B. Yes, for some systems <b>C. Yes, for all systems (T1, T2)</b>	NZISM 16.2 NZISM 16.4
<b>A7#</b>	At a minimum, are vendor staff, external contractors or associates with access to systems, applications and information (including audit logs): <ul style="list-style-type: none"> <li>• Validated and approved by appropriate personnel;</li> <li>• Periodically reviewed (at least annually) and revalidated or revoked; and</li> <li>• Reviewed and revalidated or revoked following changes to role, employment and/or inactivity?</li> </ul>	1 & 2	A. No (#T1) <b>B. Yes (T1, T2)</b>	AUISM Security Controls: 0405, 0430, 1404 NZISM 16.3 NZISM 16.5



<b>A8</b>	Do your organisation/vendor staff, external contractors or associates <b>require</b> remote access, terminal access or similar to customer devices, servers, networks or other ICT infrastructure?	1 & 2	A. Yes (please specify) <b>B. No (T1, T2)</b>	
<b>A9</b>	Are vendor staff, external contractors or associates with non-privileged accounts restricted from installing, uninstalling, disabling or making any changes to software and system configuration on servers and endpoints?	1 & 2	A. No <b>B. Yes (T1, T2)</b>	AUISM Security Control: 1503 NZISM 14.1
<b>A10#</b>	Are all internal organisation systems configured with a session or screen lock that: <ul style="list-style-type: none"> <li>• activates after a maximum of 15 minutes of user inactivity or if manually activated by the user;</li> <li>• completely conceals all information on the screen;</li> <li>• ensures that the screen does not enter a power saving state before the screen or session lock is activated;</li> <li>• requires the user to reauthenticate to unlock the system; and</li> <li>• denies users the ability to disable the session or screen locking mechanism?</li> </ul>	1 & 2	A. No (#T1) B. Yes, some of the above <b>C. Yes, all of the above (T1, T2)</b>	AUISM Security Control: 0428 NZISM 16.1.45
<b>A11#</b>	When a password reset is requested by the user, are: <ul style="list-style-type: none"> <li>• the newly assigned passwords (e.g., temporary initial passwords) randomly generated;</li> <li>• users required to provide verification of their identity (e.g., answering a set of challenge-response questions);</li> <li>• new passwords provided via a secure communication channel or split into parts; and</li> <li>• users required to change their assigned temporary password on first use?</li> </ul>	1 & 2	A. No (#T1) B. Yes, some of the above <b>C. Yes, all of the above (T1, T2)</b>	AUISM Security Controls: 1227, 1593, 1594, 1595 NZISM 16.1.41 NZISM 16.1.42
<b>A12</b>	Does the service allow user registration or logon/authentication or Single Sign-on (SSO) via	1 & 2	A. Yes (please specify). B. No (T1, T2)	

	credentials provided by another Identity Provider (IDP) such as RealMe, Facebook, Google, Microsoft etc.			
<b>A13#</b>	What is the service's approach to default user access permissions (e.g., all access is denied unless specifically allowed, all access is allowed unless specifically denied)?	1 & 2	<b>A.</b> Protection by exception (Allow access unless specifically denied) (#T1, #T2) <b>B. Protection by default (Deny unless approved) (T1, T2)</b>	
<b>A14</b>	Does the service support Single Sign-On (SSO)?	1 & 2	A. No B. Yes – Optional. Please specify SSO supported. C. Yes – Mandatory. Please specify SSO supported.	
<b>A15</b>	If customers can or are required to supply data to the service, what methods or mechanisms are available to support this?	1 & 2	Select all that apply: A. Flat file upload (e.g. CSV, XLS) B. API C. Creating or using a user/admin account in a third party service to directly access the data D. Direct access to the customer's database (e.g. SQL user, database agent software) E. Third party data integration platform (please specify) F. Other (please specify) G. Not applicable	
<b>A15A</b>	Please provide further information on all methods available to supply data to the service, including any references or support articles if available.	All		
<b>A16A</b>	Does your organisation or service request a school share access credentials or create a user account in another system or service (e.g. creating a user account in another service to facilitate data extraction)?	1 & 2	A. Yes (Please specify) B. No (T1, T2)	
<b>A16B #</b>	In relation to the creation of accounts in third party services, are enforceable written agreements in place	1 & 2 Condi tional	A. No (#T1, #T2) <b>B. Yes (T1, T2)</b>	

	with all of these third-party services covering this arrangement?	(A15 – yes)		
<b>A16C</b>	Who creates the account/s in the third-party service?	1 & 2 Conditional (A15 – yes)	A. The school, school system or jurisdiction B. The third-party service C. The service (responding to this assessment)	
<b>A17</b>	Within the vendor organisation, is application control: <ul style="list-style-type: none"> <li>• Implemented on all workstations;</li> <li>• Implemented on internet-facing and non-internet facing servers;</li> <li>• Enabled to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set;</li> <li>• Enabled to restrict the execution of drivers to an organisation-approved set;</li> <li>• Implemented using cryptographic hash rules, publisher certificate rules or path rules;</li> <li>• Rulesets are validated on an annual or more frequent basis; and</li> <li>• When implementing application control using publisher certificate rules, both publisher names and product names are used.</li> </ul>	1 & 2	A. No, none of the above B. Yes, some of the above <b>C. Yes, all of the above (T1, T2)</b>	AUISM Security Controls: 0843, 1490, 1656, 1657, 1658, 0955, 1582, 1471 NZISM 14.2

#### 6.2.6 Security – HR

Q	Question	Tier	Response options	Standard / References
<b>HR1#</b>	Do all vendor staff, external contractors and associates who have access to user data or user content undergo employment screening (e.g., criminal history checks,	1	A. No (#T1) <b>B. Yes (T1, T2)</b>	AUISM Security Control: 0434 NZ PSR PERSEC1

	working with children checks) as per applicable regulatory requirements?			
<b>HR2#</b>	<p>Does your organisation run a security, privacy and online safety awareness/education program for your staff which addresses the following at a minimum:</p> <ul style="list-style-type: none"> <li>• Identification of who the awareness training needs to be delivered to;</li> <li>• Identification of when awareness training needs to be delivered (e.g., during induction, annually, etc.);</li> <li>• Identification of how the awareness training is to be delivered (e.g., classroom training, online course, security awareness posters, emails, etc.); and</li> <li>• The content to be delivered for each awareness session such as: <ul style="list-style-type: none"> <li>o Basic understanding of the need for information security, privacy and online safety;</li> <li>o Actions to maintain security, privacy and online safety;</li> <li>o Actions to respond to suspected security, privacy and online safety incidents;</li> <li>o Applicable policies and laws;</li> <li>o Practical security, privacy and online safety awareness exercises, and</li> <li>o Disciplinary actions for significant security and privacy breaches by staff?</li> </ul> </li> </ul>	1 & 2	<p>A. No - none of the above (#T1)  B. Yes - some of the above  <b>C. Yes - all of the above (T1, T2)</b></p>	<p>AU ISM Security Control: 0252  NZISM 9.1  NZISM 3.2.18  NZISM 3.3.13  NZISM 7.1.7</p>
<b>HR3#</b>	<p>Is there a documented and implemented process to remove access to systems, applications and data repositories for personnel (vendor staff, external contractors and associates) that:</p> <ul style="list-style-type: none"> <li>• no longer have a legitimate requirement for access (implemented on the same day); and</li> <li>• are detected undertaking malicious activities (implemented immediately)?</li> </ul>	1 & 2	<p>A. No (#T1, #T2)  B. Yes – but not implemented within required timeframes  <b>C. Yes – (T1, T2)</b></p>	<p>AUISM Security Control: 0430, 1591  NZISM 16.1.46  NZISM 16.4.33</p>

## 6.2.7 Security – Processes and Testing

Q	Question	Tier	Response options	Standard / References
<b>T1#</b>	<p>Does your organisation have an implemented continuous monitoring plan for all organisational systems and infrastructure that includes:</p> <ul style="list-style-type: none"> <li>conducting vulnerability scans for systems at least monthly</li> <li>conducting penetration tests for systems after a major change or at least annually</li> <li>analysing identified security vulnerabilities to determine their potential impact and appropriate mitigations based on effectiveness, cost and existing security controls</li> <li>using a risk-based approach to prioritise the implementation of identified mitigations.</li> </ul>	1 & 2	<p>A. No (#T1, #T2)</p> <p>B. Yes - meets all of the requirements above but conducted less frequently</p> <p><b>C. Yes - meets all requirements above (T1, T2)</b></p> <p><b>D. Yes – meets all requirements above including the use of external independent resources to conduct penetration testing (T1, T2)</b></p>	<p>AUISM Security Control: 1163</p> <p>NZISM 4.1.26-29</p> <p>NZISM 4.3</p> <p>NZISM 6.1-6.2</p> <p>NZISM 14.4-14.5</p>
<b>T2#</b>	<p>Does your organisation use a centrally managed approach to patch or update applications, drivers, operating systems, and firmware which includes ensuring:</p> <ul style="list-style-type: none"> <li>- the integrity and authenticity of patches;</li> <li>- successful application of patches; and</li> <li>- that patches remain in place?</li> </ul>	1 & 2	<p>A. No – none of the above (#T1)</p> <p>B. Yes – some of the above</p> <p><b>C. Yes – all of the above (T1, T2)</b></p>	<p>AUISM Security Controls: 0298 revision 7, 0303, 1499, 1497, 1500.</p> <p>NZISM 12.4</p> <p>NZISM 14.5.8</p>
<b>T3#</b>	<p>Are patches, updates or vendor mitigations for security vulnerabilities in:</p> <ul style="list-style-type: none"> <li>- internet facing services (including operating systems of internet-facing services);</li> <li>- workstation, server and network device operating systems;</li> <li>- operating systems of other ICT equipment; and</li> <li>- drivers and firmware;</li> </ul> <p>applied within two weeks of release, or within 48 hours if an exploit exists?</p>	1	<p>A. No (#T1)</p> <p><b>B. Yes (T1, T2)</b></p>	<p>AUISM Security Controls: 1690, 1694, 1695, 1696, 1751, 1697</p> <p>NZISM 12.4</p>

<b>T4</b>	Are patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software and security products applied within two weeks of release, or within 48 hours if an exploit exists?	1 & 2	A. No <b>B. Yes (T1, T2)</b>	AUISM Security Control: 1691, 1692 NZISM 12.4
<b>T5</b>	Are patches, updates or vendor mitigations for security vulnerabilities in other applications applied within one month of release?	1 & 2	A. No <b>B. Yes (T1, T2)</b>	AUISM Security Controls: 1693 NZISM 12.4
<b>T6#</b>	Does your organisation have a formal, documented and implemented incident response plan which requires security, privacy and online safety incidents to be: <ul style="list-style-type: none"> <li>• Investigated;</li> <li>• Remediated; and</li> <li>• Recorded in a register with the following information at a minimum: <ul style="list-style-type: none"> <li>o Date incident occurred;</li> <li>o Date incident discovered;</li> <li>o Description of the incident;</li> <li>o Actions taken in response to the incident; and</li> <li>o Name of person to whom the incident was reported?</li> </ul> </li> </ul>	1 & 2	A. No - none of the above (#T1, #T2) <b>B. Yes - some of the above (T2)</b> <b>C. Yes - all of the above (T1)</b>	AUISM Security Control: 0125 NZISM 7 NZISM 5.6 NZISM 22.1.25
<b>T7#</b>	When a data breach occurs, are affected customers and/or organisations notified as soon as possible after a data breach is discovered and given all relevant details (including affected individuals and what information was disclosed)?	1 & 2	A. No (#T1, #T2) <b>B. Yes (T1, T2)</b>	AUISM Security Controls: 0123, 0141, 0140 NZISM 7.2 NZPP-5 NZISM 7.2.22 NZPP
<b>T8</b>	When a data loss/corruption event occurs, are affected customers and/or organisations notified as soon as possible after this is discovered and given all relevant details?	1 & 2	A. No – none of the above <b>B. Yes – some of the above (T2)</b> <b>C. Yes – all of the above (T1, T2)</b>	AUISM Security Controls: 0123, 0141, 0140 NZISM 7.2 NZPP-5

## 6.2.8 Security – Plans and Quality

Q	Question	Tier	Response options	Standard / References
Q1	(Question removed from 2021.1)			
Q2	Does your organisation have a documented and implemented Business Continuity Plan for the service which includes: <ul style="list-style-type: none"> <li>• Backup strategies (including automated backups and backups that are stored disconnected);</li> <li>• Restoration strategies (e.g., disaster recovery); and</li> <li>• Preservation strategies?</li> </ul>	1	A. No B. Yes - meets some requirements <b>C. Yes - meets all requirements (T1)</b>	AUISM Security Controls: 1547, 1548, 1510 NZISM 6.4
Q3	Does your organisation have a documented and implemented IT Change management process and supporting procedures which includes the following at a minimum: <ul style="list-style-type: none"> <li>• Applicable criteria for entry to and exit from the change management process</li> <li>• Categorisation of IT change (e.g., Standard, Pre-Approved, Emergency, etc.);</li> <li>• Approval requirements for each category of IT change;</li> <li>• Assessment of potential security impacts;</li> <li>• Prerequisites for the IT change (e.g., the IT change has been tested in a non-production environment);</li> <li>• Documentation requirements in regard to the change (e.g., completion of a template in an IT change management tool, completion of a rollback plan, etc.);</li> <li>• Documentation that needs to be updated as a result of the change (e.g., as-built documentation, IT Disaster Recovery Plans, etc.); and</li> <li>• IT change communication processes (e.g., notifications to users)?</li> </ul>	1 & 2	A. No change management process B. Yes, change management process meets some requirements <b>C. Yes, change management process meets all requirements (T1, T2)</b>	AUISM Security Control: 1211 NZISM 6.3
Q4	Does your organisation have a documented and implemented security, privacy and online safety risk management framework and supporting processes, which outlines at a minimum:	1 & 2	A. No - none of the above B. Yes - some of the above <b>C. Yes - all of the above (T1, T2)</b>	AUISM Security Control: 1636, revision 0, ISM Security Control: 1526, revision 1 NZISM 3.2.10-13 NZISM 3.3.5-8

	<ul style="list-style-type: none"> <li>• Scope and categorisation of information assets and systems;</li> <li>• Identification and assessment of risks/ threats, including those relating to the supply chain (e.g. from outsourced services that the solution relies on);</li> <li>• Selected and implemented controls to manage risks with the following details recorded in a risk register: <ul style="list-style-type: none"> <li>o Identified security risks, categories and risk ratings;</li> <li>o Risk owner(s);</li> <li>o Mitigation actions;</li> <li>o Accepted risks (where applicable) and;</li> <li>o Residual risk ratings after implementing mitigation actions</li> </ul> </li> <li>• Proactive monitoring and testing of information assets and systems to maintain the security posture on an ongoing basis?</li> </ul>			NZISM 4.1
<b>Q5#</b>	Are all service application developments assessed as per a security testing methodology that is consistent with the guidance provided by the latest industry standard frameworks (e.g., Open Web Application Security Project (OWASP) Testing Guide v4.2, Building Security In Maturity Model (BSIMM))?	1 & 2	A. No (#T1, #T2) B. Yes - security testing partially satisfies the guidance provided in an industry standard framework (please specify framework) <b>C. Yes - security testing fully satisfies the guidance provided in an industry standard framework (T1, T2) (please specify framework)</b>	AUISM Security Control: 1239 NZISM 14.4.6 NZISM 14.5.8
<b>Q6</b>	Does your organisation have a documented and implemented IT Asset management process including: <ul style="list-style-type: none"> <li>• A register of all components that make up the service, including software, databases, middleware, infrastructure etc (their version numbers, patch levels and configuration);</li> <li>• An ICT equipment and media register that is maintained and regularly audited;</li> <li>• A directive that ICT equipment and media are secured when not in use;</li> </ul>	1	A. No - none of the above B. Yes - some of the above <b>C. Yes - all of the above (T1, T2)</b>	AUISM Security Control: 0336, revision 4, ISM Security Control: 0159, revision 4 NZISM 8.4 NZISM 12.6 NZISM 13.4-13.6



	<ul style="list-style-type: none"> <li>The secure disposal of ICT equipment and media (including sanitising/removal of any data or secure destruction/shredding)?</li> </ul>			
<b>Q7#</b>	<p>Does your organisation have a documented and implemented information security policy that outlines the following at a minimum:</p> <ul style="list-style-type: none"> <li>management direction and support for information security;</li> <li>requirement to comply with applicable laws and regulations;</li> <li>information security roles and corresponding responsibilities/accountabilities; and</li> <li>requirement for communication to management to ensure they maintain an awareness of, and focus on, addressing privacy and security issues?</li> </ul>	1 & 2	<p>A. No (#T1)  <b>B. Yes (T1, T2)</b></p>	<p>AUISM Security Control: 1478 revision 1.  NZISM 5.1.7  NZISM 5.2</p>
<b>Q8</b>	<p>Does the service's application development have the following characteristics:</p> <ul style="list-style-type: none"> <li>Environments are separated into at least development, testing and production environments;</li> <li>Development and modification of software only takes place in development environments;</li> <li>Unauthorised access to the authoritative software source is prevented;</li> <li>Secure-by-design principles and secure programming practices are used as part of application development;</li> <li>Privacy-by-design principles; and</li> <li>Threat modelling is used in support of application development?</li> </ul>	1 & 2	<p>A. No – none of the above  B. Yes - some of the above  <b>C. Yes - all of the above (T1, T2)</b></p>	<p>NZISM 14.4  NZISM 14.5</p>

#### 6.2.9 Security – Incidents

Q	Question	Tier	Response options	Standard / References
<b>I1</b>	Has the organisation, platform, or service had a recent security and/or privacy incident or breach?	1 & 2	<p>A. Yes – less than 12 months ago  <b>B. Yes – greater than 12 months ago (T1, T2)</b>  <b>C. No (T1, T2)</b></p>	

### 6.2.10 Security – Data Deletion and Retention

Q	Question	Tier	Response options	Standard / References
<b>D1</b>	Are all data backups stored for a minimum of 3 months?	1 & 2	A. No <b>B. Yes (T1, T2)</b>	AUISM Security Control: 1514 NZISM 6.4
<b>D2</b>	After customer data is deleted or removed from the service, is written confirmation or certification provided?	1 & 2	A. No B. Yes - written confirmation or certification is provided, but only upon request from the customer <b>C. Yes - written confirmation or certification is automatically provided to the customer (T1, T2)</b>	NZISM 13.1 NZISM 13.4-13.6 NZISM 22.1.26
<b>D2A</b>	Please specify the timeframe for removing or deleting customer data from the service.	1 & 2		
<b>D3#</b>	Is the full restoration of backups tested at least once when initially implemented and each time major information technology infrastructure changes occur, and at least annually? (e.g., technology stack changes, vendor changes, platform changes)	1 & 2	A. No (#T1, #T2) <b>B. Yes (T1, T2)</b>	AUISM Security Control: 1515 NZISM 6.4
<b>D4</b>	(Question removed 2023)	1 & 2		
<b>D5</b>	Does the organisation have a process to delete and remove inactive or dormant users and their related data?	1 & 2	A. No <b>B. Yes (T1, T2)</b>	
<b>D5A</b>	Describe the process including how the organisation determines a user is inactive or dormant and the timeframes for deleting their data.	1 & 2		
<b>D6</b>	Is all user data within the service available for export in a reusable form?	1 & 2	A. Yes (Self service at no cost) B. Yes (Upon requests at no cost) C. Yes (Upon requests with a cost) D. No	

### 6.2.11 Security – Compliance Controls

Q	Question	Tier	Response options	Standard / References
<b>CC1</b>	Select the compliance certifications or security assessments that have been completed for the service and	1 & 2	A. ISO/IEC27001 B. SOC 2 Type II	NZISM 5.8 NZ PSR – INFOSEC3, GOV8

	your organisation, or another organisation contracted by you to perform the development, maintenance and/or support of your solution (excluding the infrastructure provider e.g., AWS, Azure, Sendgrid)		C. FEDRAMP (NIST) D. IRAP E. Privacy confirmation (GDPR, SOPAA, Privacy Shield) F. Cloud Security Alliance STAR G. Cloud Vendor Assessment Tool (HECVAT) H. 1EdTech TrustEd Apps(TM) Certification I. Other (please specify) J. None of the above	
<b>CC2#</b>	If the solution processes electronic payments or holds credit card data is it Payment Card Industry Data Security Standards (PCI DSS) compliant?	1 & 2	A. No (#T1, #T2) <b>B. Yes – service is PCI compliant (T1, T2)</b> <b>C. Yes – outsourced to PCI compliant third party (please specify) (T1, T2)</b> <b>D. N/A – Solution does not process payments or hold credit card data (T1, T2)</b>	NZISM 5.8

#### 6.2.12 Security – Governance

Q	Question	Tier	Response options	Standard / References
<b>G01#</b>	Is there a nominated and suitably qualified individual within the organisation responsible for: <ul style="list-style-type: none"> <li>Coordinating and reporting on cyber security</li> <li>Overseeing information security risk management including supply chain risks</li> <li>Leading cyber security improvement activities</li> <li>Overseeing cyber security awareness and training</li> <li>Overseeing cyber security incident response</li> </ul>	1 & 2	A. No (#T1, #T2) <b>B. Yes, with some of the specified responsibilities (specify the substantive role of the individual) (T2)</b> <b>C. Yes, with all of the specified responsibilities (T1, T2) (specify the substantive role of the individual)</b>	AUISM 0714 NZISM 3.2
<b>G02#</b>	Is there a nominated Privacy Officer within the organisation who has a good understanding of privacy requirements and is responsible for: <ul style="list-style-type: none"> <li>Providing privacy advice internally.</li> </ul>	1 & 2	A. No (#T1, #T2) <b>B. Yes, with some of the specified responsibilities (specify the substantive role of the individual)</b> <b>C. Yes, with all of the specified responsibilities (T1, T2) (specify the substantive role of the individual)</b>	AU PP NZ PP

	<ul style="list-style-type: none"> <li>• Liaising with the Office of the Australian Information Commissioner and the New Zealand Office of the Privacy Commissioner (as relevant).</li> <li>• Co-ordinating the handling of internal and external privacy enquiries, privacy complaints and requests for access to, and correction of, personal information.</li> <li>• Maintaining a record of your organisation's personal information holdings.</li> <li>• Assisting with the preparation of privacy impact assessments.</li> <li>• Measuring and documenting your organisation's performance against its privacy management plan.</li> </ul>			
<b>G03</b>	Has responsibility for and ownership and accountability of critical system assets been assigned to individual/s in the organisation?	1 & 2	A. No <b>B. Yes (T1, T2)</b>	NZISM 3.4
<b>G04</b>	What countries are your organisation's security and privacy operations teams and real-time monitoring and incident response systems located?	1 & 2	<b>A. Entirely within Australia and/or New Zealand (please specify) (T1, T2)</b> B. From other countries (please specify country/s) C. No defined security and privacy operations teams	

## 6.3 Criteria – Privacy

### 6.3.1 Privacy

Q	Question	Tier	Response options	Standard / References
<b>PA1</b>	Are the terms of service/use made available free of charge, and, published on the internet or provided to customers prior to use of the service?	1 & 2	A. No <b>B. Yes (T1, T2)</b>	

<b>PA2</b>	As per the terms of service, what, if any, age restrictions apply to the use of the service?	1 & 2	A. Users must be over the age of 18 B. Users under the age of 18 can use the service with parent/guardian consent <b>C. No age restrictions apply (T1, T2)</b> D. Other (please specify) <b>E. NA - this service will not be used by students (T1, T2)</b>	
<b>PA3</b>	What are the specified definitions of intellectual property ownership, including copyright, in the terms of use for the service? (e.g., user generated content)? Include excerpt from terms of use.	1 & 2	A. Not specified B. Service provider has ownership or licence to copy, alter, distribute, perform, display to all other users, third parties, affiliated organisations, etc. The service provider notifies users if their intellectual property is used for any of these purposes. C. Service provider has ownership or licence to copy, alter, distribute, perform, display to all other users, third parties, affiliated organisations etc. The service provider does not notify users if their intellectual property is used for any of these purposes. <b>D. Service provider does not have ownership or licence to copy, alter, distribute, perform, display to all other users, third parties, affiliated organisations etc. (T1, T2)</b>	
<b>PA4</b>	As per the terms of service, are users forewarned in the event the service provider wishes to terminate their account?	1 & 2	A. No <b>B. Yes (T1, T2)</b> <b>C. N/A - Service provider does not terminate accounts (T1, T2)</b>	

### 6.3.2 Privacy – General

Q	Question	Tier	Response options	Standard / References
<b>PR1#</b>	Is the privacy policy made available free of charge, and: • Published on the internet; or	1 & 2	A. No (#T1, #T2) <b>B. Yes (T1, T2)</b>	APP: 1.5 NZPP-3

*Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.*

	<ul style="list-style-type: none"> <li>• Provided to customers prior to use of the service?</li> </ul>			
<b>PR1A</b>	Enter the URL for the service's Privacy Policy or upload the Privacy Policy document	1 & 2		NZPP-3
<b>PR2#</b>	<p>Does the privacy policy for the service outline the following requirements about the collection and management of personal information at a minimum:</p> <ul style="list-style-type: none"> <li>• The kinds of personal information that the entity collects and holds;</li> <li>• How the entity collects and holds personal information;</li> <li>• The purposes for which the entity collects, holds, uses and discloses personal information;</li> <li>• How an individual may access personal information about the individual that is held by the entity and seek the correction of such information;</li> <li>• How an individual may complain about a breach of their privacy, and how the entity will deal with such a complaint;</li> <li>• Whether the entity is likely to disclose personal information to overseas recipients; and</li> <li>• If the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy?</li> </ul>	1 & 2	<p>A. No (#T1, #T2)</p> <p>B. Yes - includes some of the above (#T1, #T2)</p> <p><b>C. Yes - includes all of the above (T1, T2)</b></p>	<p>APP: 1.4</p> <p>NZPP-3</p> <p>NZPP-6</p> <p>NZPP-7</p>
<b>PR3A</b>	What <b>mandatory</b> information is collected by the service when <b>school staff</b> generate their own accounts for this service? Select all that apply. If not required, select N/A.	1 & 2	<p>A. Title</p> <p>B. First name</p> <p>C. Surname</p> <p>D. Email address</p> <p>E. Gender</p> <p>F. Date of birth (i.e., dd/mm/yy)</p> <p>G. Age, month and year of birth, or year of birth</p> <p>H. Year level</p> <p>I Country or state/province</p> <p>J. Role (for school leaders)</p> <p>K. Evidence of identity</p>	NZPP-3

			L. Other (please specify): M. N/A - school staff do not register their own accounts for this service	
<b>PR3B</b>	What <b>mandatory</b> information is collected by the service when <b>students</b> generate their own accounts for this service? Select all that apply. If not required, select N/A.	1 & 2	A. Title B. First name C. Surname D. Email address E. Gender F. Date of birth (i.e., dd/mm/yy) G. Age, month and year of birth, or year of birth H. Year level I. Country or state/province J. Role (for school leaders) K. Evidence of identity L. Other (please specify): M. N/A - students do not register accounts for this service N. N/A - students do not register their own accounts for this service	NZPP-3
<b>PR3C</b>	What <b>mandatory</b> information is collected by the service when <b>parents</b> generate their own accounts for this service? Select all that apply. If not required, select N/A.  <b>NOTE:</b> This question relates to when parent accounts are required for school use of the service. If parent accounts are not required, select, "N/A parent accounts are not required for school use of this service".	1 & 2	A. Title B. First name C. Surname D. Email address E. Gender F. Date of birth (i.e., dd/mm/yy) G. Age, month and year of birth, or year of birth H. Year level I. Country or state/province J. Evidence of identity K. Other (please specify): L. N/A - parent accounts are not required for school use of this service	NZPP-3

			M. N/A - parents do not register their own accounts for this service	
<b>PR4A</b>	What <b>mandatory</b> information is collected by the service when a school-based administrator (or the service) generates accounts on behalf of school <b>staff</b> ? Select all that apply. If not required, select N/A.	1 & 2	A. Title B. First name C. Surname D. Email address E. Gender F. Date of birth (i.e., dd/mm/yy) G. Age, month and year of birth, or year of birth H. Year level I. Country or state/province J. Evidence of identity K. Other (please specify): L. N/A - school-based administrators or teachers or the service provider cannot generate accounts on behalf of staff	NZPP-3
<b>PR4B</b>	What <b>mandatory</b> information is collected by the service when a school-based administrator (or the service) generates accounts on behalf of <b>students</b> ? Select all that apply. If not required, select N/A.	1 & 2	A. Title B. First name C. Surname D. Email address E. Gender F. Date of birth (i.e., dd/mm/yy) G. Age, month and year of birth, or year of birth H. Year level I. Country or state/province J. Evidence of identity K. Other (please specify): L. N/A - school based-administrators, teachers or the service provider cannot generate accounts on behalf of students	
<b>PR4C</b>	What <b>mandatory</b> information is collected by the service when a school-based administrator (or the service)	1 & 2	A. Title B. First name	



	generates accounts on behalf of <b>parents</b> ? Select all that apply. If not required, select N/A.		C. Surname D. Email address E. Gender F. Date of birth (i.e., dd/mm/yy) G. Age, month and year of birth, or year of birth H. Year level I. Country or state/province J. Evidence of identity K. Other (please specify): L. N/A - school based-administrators, teachers or the service provider cannot generate accounts on behalf of parents	
<b>PR5</b>	Do the terms of use for the service (ToS) or the privacy policy (PP) require complete and accurate information to be entered when registering accounts for the service (e.g., use of pseudonym or de-identified information is prohibited)?  Please include excerpt from the terms of service or privacy policy.	1 & 2	A. Yes (please provide excerpt from ToS or PP) <b>B. No (please provide excerpt from ToS or PP) (T1, T2)</b>	
<b>PR6</b>	Are customers/users offered anonymity and/or pseudonymity when dealing with the service provider in some circumstances (e.g., providing feedback)?	1 & 2	A. No <b>B. Yes, please specify circumstances (T1, T2)</b>	APP: 2.1 NZPP-1
<b>PR7</b>	Are mandatory fields clearly distinguished from optional fields during the standard account registration process?	1 & 2	A. No <b>B. Yes (T1, T2)</b>	NZPP-3
<b>PR8</b>	Are mandatory fields clearly distinguished from optional fields when schools, teachers, or the service register accounts on behalf of other users (e.g., students, staff, or parents)?	1 & 2	A. No <b>B. Yes (T1, T2)</b>	NZPP-3
<b>PR9</b>	If unsolicited personal information is provided to the service (e.g., when existing customer data is uploaded to the service), is the information destroyed or de-identified as soon as practicable if it is lawful to do so?	1 & 2	A. No <b>B. Yes (T1, T2)</b>	NZPP-9

PR10#	<p>Does your organisation share user data with third parties in any circumstance other than the following? If yes, please specify.</p> <ul style="list-style-type: none"> <li>-the individual has consented to the use or disclosure of the information;</li> <li>-the use or disclosure of the information is required or authorised by or under a law or a court/tribunal order in the customer's country;</li> <li>- the use or disclosure is required or permitted under privacy legislation in the customer's country; or</li> <li>-the entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body?</li> </ul> <p>For service in Australia, refer to the Australian Privacy Principles, as well as the <a href="#">permitted general situations</a> and <a href="#">permitted health situations</a>.</p> <p>For service in New Zealand, refer to the <a href="#">Privacy Principles</a> and <a href="#">information sharing provisions</a> in the Privacy Act 2020, as well as the <a href="#">Oranga Tamariki Act 1989</a> and the <a href="#">Family Violence Act 2018</a>.</p>	1 & 2	<p>A. Yes (please specify) (#T1, #T2)</p> <p><b>B. No (T1, T2)</b></p>	<p>APP: 6.1, 6.2</p> <p>NZPP-11</p>
PR11	<p>Can users opt-in or opt-out to the service's commercial mailing list/promotional/marketing communications (e.g. email mailing lists)?</p> <p><i>Commercial mailing lists are those that are used for the purpose of distributing sales and marketing and promotional materials, including (but not limited to) competitions, education research related to the product, and end user feedback.</i></p>	1 & 2	<p>A. Users cannot opt-out. Users are automatically subscribed to receive commercial/promotional/marketing communications.</p> <p>B. Users can opt-out. Some or all users are automatically subscribed but can opt-out after the fact</p> <p><b>C. Users can opt-in. Users do not receive commercial/promotional/marketing</b></p>	

	<i>Commercial mailing lists do not include lists used for the purpose of sending important service information, such as notifications of service disruption, data breach or loss; upgrade notifications; and subscription renewals.</i>		<b>communications unless they explicitly opt-in (T1, T2)</b> <b>D. N/A – The service or organisation does not have any commercial/promotional/marketing communications (T1, T2)</b>	
<b>PR12#</b>	<p>Does the service adopt government related identifiers of individuals as its own identifier of the individual or use or disclose government related identifiers for any reasons other than the list below:</p> <ul style="list-style-type: none"> <li>• The government related identifier is required or authorised by or under a law or a court/tribunal order within the customer's country;</li> <li>• Use or disclosure is necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions;</li> <li>• Use or disclosure is necessary for the organisation to fulfil its obligations to a government agency or education authority within the customer's country;</li> <li>• Use or disclosure is required or authorised by or under a law or a court/tribunal order within the customer's country;</li> <li>• The organisation reasonably believes the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities;</li> <li>• The identifier, organisation or circumstances are prescribed by regulations?</li> </ul>	1 & 2	<p>A. Yes (provide details of the identifier(s) and how each is used) (#T1, #T2)</p> <p><b>B. No (T1, T2)</b></p>	APP: 9.1, 9.2 NZPP-13
<b>PR13#</b>	Does your organisation have a process which allows customers to request the service to provide access to, correct, or delete all personal information relating to them?	1 & 2	<p>A. No (#T1, #T2)</p> <p>B. Yes - with a cost and resolved outside of 3 months</p> <p>C. Yes - with a cost and resolved within 3 months</p> <p><b>D. Yes - free of charge and resolved outside of 3 months (T2)</b></p>	APP: 12.1, 13.1 NZPP-6 NZPP-7

			<b>E. Yes - free of charge and resolved within 3 months (T1, T2)</b> F. NA - service does not collect personal information (T1, T2)	
<b>PR14#</b>	Does the service provide any discovery functionality which allows users from one school to find, access or discover users or personal information from another school, or organisation? Examples include enabled searching (by user, user details or resources), or data sharing (e.g. to support student transfer) or integration (e.g. for analytics) between customers (e.g. different schools). Select all that apply.		<b>A. No discovery functionality exists within service (T1,T2)</b> B. Discovery functionality can be restricted to the user's current school/year level/class C. Discovery functionality is disabled by default D. An administrator can restrict discovery functionality at the user level (i.e. allow some but not all users access discovery functionality) E. Discovery is possible, but none of the controls above are available (#T1, #T2)	NZPP-11
<b>PR15</b>	Does the service capture a user's location data?		<b>A. No, user location data not required. (T1, T2)</b> <b>B. The service must capture user location data to function. Location data is captured with a user's explicit consent (T1, T2)</b> C. The service must capture user location data to function. Location data is captured without a user's explicit consent. D. The service does not require user location data to function, but does capture it with a user's explicit consent. E. The service does not require user location data to function, but does capture it without a user's explicit consent.	

<b>PR16#</b>	How does the organisation notify users when updates occur to the Privacy Policy and the Terms and Conditions?	1 & 2	<p><b>A. Users are sent a notification when updates are made to the Privacy Policy and Terms and Conditions (T2)</b></p> <p><b>B. Users are sent a notification <u>prior to</u> updates being made to the Privacy Policy and Terms and Conditions (please specify minimum timeframe) (T1, T2)</b></p> <p><b>C. Users are required to review and explicitly consent to the latest Privacy Policy and Terms and Conditions prior to being able to continue using the service. (T1, T2)</b></p> <p><b>D. None of the above (#T1)</b></p>	
<b>PR17#</b>	<p>Does the Privacy Policy or other published document describe all of the service's sub processors including information on:</p> <ul style="list-style-type: none"> <li>• The name of the sub processor and its organisation;</li> <li>• Contact information of the sub processor (e.g. website URL, email address);</li> <li>• The data types disclosed to the sub processor including the purpose of the sub processor;</li> <li>• The lawful basis for processing the data where applicable;</li> <li>• Countries where data may be processed in or stored.</li> </ul>	1 & 2	<p><b>A. Yes - All of the above (Please specify) (T1)</b></p> <p><b>B. Yes - Some of the above including name of the sub processor and data types (T2)</b></p> <p>C. No (#T1, #T2)</p> <p>D. N/A - The service does not use any sub processors.</p>	
<b>PR18</b>	In addition to any published sub processors, does the organisation share, publish or provide access to any user data (including where de-identified, aggregated, etc) to a third party?	1 & 2	<p>A. Yes (Please specify)</p> <p><b>B. No (T1, T2)</b></p>	

<b>PR19</b>	Does the organisation or service use, share, publish or provide access to any user data (including where de-identified, aggregated, etc) for advertising, market research or similar purposes?	1 & 2	A. Yes (Please specify) <b>B. No (T1, T2)</b>	
<b>PR20</b>	Does the organisation or service use, share, publish or provide access to any user data (including where de-identified, aggregated, etc) for use in artificial intelligence or machine learning (including training or developing of AI or ML models)?	1 & 2	A. Yes (Please specify) <b>B. No (T1, T2)</b>	

### 6.3.3 Privacy – Functionality

Please note: Functionality questions allow us to better understand how given functionality works and what controls are available. Generally speaking, an ability to disable, restrict access to, or moderate functionality will result in a lower risk level.

Q	Question	Tier	Response options	Standard / References
<b>PF1</b>	When using the service, are any users exposed to advertising, marketing and/or offers?	All	A. Yes <b>B. No (T1, T2)</b>	
<b>PF2</b>	Does the service provide functionality that allows school-based administrator accounts to control role-based access for school users (e.g., staff or students) in order to restrict access to stored information and/or functionality within the system?	<b>1 &amp; 2</b>	A. No <b>B. Yes, please provide details (T1, T2)</b> <b>C. N/A (T1, T2)</b>	
<b>PF3</b>	Does the registration of an account or use of the service generate a user 'profile' within the service, and if so, can visibility be restricted (e.g., made private or restricted to known users)?	1 & 2	A. Profile is generated, but user or administrator cannot restrict visibility of their profile B. Profile is generated, and user or administrator can restrict visibility of their profile <b>C. Profile is generated but only visible to user (e.g., visibility is restricted by default) (T1, T2)</b> <b>D. No user profile is generated (T1, T2)</b>	

PF4	Select all functionality available within the service.	All	<p>Informational only, used to generate subsequent questions.</p> <ul style="list-style-type: none"> <li>A. Forms, surveys and eSignatures</li> <li>B. Online meetings, video conferencing, audio conferencing</li> <li>C. Remote access tools</li> <li>D. Screen Sharing</li> <li>E. Chat / Instant Messaging</li> <li>F. Commenting and communities/forum</li> <li>G. Quiz, poll, flashcard creation and/or distribution</li> <li>H. File download, including executable, developer tools, images etc.</li> <li>I. Direct email</li> <li>J. File upload and storage, and file sharing and collaboration</li> <li>K. Content creation and collaboration</li> <li>L. Content libraries</li> <li>M. Notifications and alerts</li> <li>N. Online learning activities, assessments and/or games</li> <li>O. Administrative support services and records management</li> <li>P. Data distribution, data broker, integration platforms as a service</li> <li>Q. Authentication as a service and identity providers</li> <li>R. Data aggregation, analytics, insights and reporting</li> <li>S. Assessment or collection of health and well-being information including socio-emotional factors (e.g., physical and mental health, well-being, behaviour)</li> <li>T. Other (please specify)</li> </ul>	
-----	--	-----	---	--

			U. None of the above	
<b>PF5</b>	In relation to the form, survey and/or eSignature functionality, select which features are offered within the service. Select all that apply.		A. Online forms - service provider generated, non-editable B. Online forms - customisable / editable / user generated C. Surveys - service provider generated, non-editable D. Surveys - customisable / editable / user generated E. eSignatures F. Forms/surveys can be distributed and/or shared via linked social media accounts (Facebook, Twitter etc.) G. Forms/surveys can be shared as templates for re-use by others	
<b>PF6#</b>	In relation to the online meeting, video conference, audio conferencing and/or livestreaming functionality available within the service, select all that apply.		A. Access to sessions can be made available to the public B. Access to sessions can be made private (e.g., access to sessions is invitation only) C. Participant details can be displayed to all session participants D. Participants can be displayed with de-identified/anonymous details or kept private E. Sessions can be recorded and made available to the public F. Sessions can be recorded and made private (e.g., participants only) G. Audit logs are not kept for all recordings (#T1, #T2) H. Participants are not notified if they are participating in a recorded session (e.g., via on screen prompt) (#T1, #T2)	
<b>PF7#</b>	In relation to the remote access tools available within the service, select all that apply.		A. Remote access tools can be disabled by an administrator or moderator	



			B. Remote access sessions can be initiated without the agreement of the user (#T1, #T2) C. Users cannot take back control during remote access sessions (#T1, #T2) D. Users cannot terminate remote access sessions once initiated (#T1, #T2) E. Onscreen notification is displayed throughout remote access sessions F. Remote access sessions are not logged (#T1, #T2)	
<b>PF8#</b>	In relation to the screen sharing functionality available within the service, select all that apply.		A. Use of screen sharing functionality is disabled by default B. Screen sharing can be disabled by an administrator or moderator C. Screen sharing sessions are initiated and/or accepted by the user who is sharing their screen D. Screen sharing sessions are not logged (#T1, #T2)	
<b>PF9#</b>	In relation to the chat/instant messaging functionality available within the service, select all that apply.		A. Chat/instant messaging is unmoderated B. The service moderates chat/messages using a profanity filter C. The service moderates chat/instant messaging and reserves the right to remove posts and/or users that breach the Terms of Use D. Users can report chat/instant messaging that breaches the Terms of Use E. Users can chat/message with non-account holders (i.e., no log in is required to participate in chat/messaging) F. Communication can be limited to restricted groups only (e.g., class, year level) G. Chat/instant messaging can be disabled by an administrator/moderator	

			<p>H. Chat/instant messaging is visible to an administrator (e.g., teacher) in real time</p> <p>I. Chat/instant messaging is not logged (#T1, #T2)</p> <p>J. None of the above</p>	
<b>PF10#</b>	In relation to the commenting and communities/forums functionality available within the service, select all that apply:		<p>A. Non-account holders can post comments (i.e., no log in is required to participate in commenting)</p> <p>B. The service applies a profanity filter prior to publishing</p> <p>C. The service moderates comments and reserves the right to remove posts and/or users that breach the Terms of Use</p> <p>D. Users can report comments that breach the service's Terms of Use</p> <p>E. Comments must be approved by an administrator or the service prior to publishing</p> <p>F. Commenting can be disabled by an administrator/moderator</p> <p>G. An administrator can control what users can comment on and which users can comment (e.g., a teacher can restrict students to only comment on the work of classmates)</p> <p>H. Commenting is unmoderated</p> <p>I. Comments are not logged (#T1, #T2)</p> <p>J. Users can upload files or share projects or files in forums/communities</p> <p>K. None of the above</p>	
<b>PF11</b>	In relation to the quiz, poll and flashcard functionality, select which features are offered within the service. Select all that apply.		<p>A. Quizzes - service provider generated, non-editable</p> <p>B. Polls - service provider generated, non-editable</p>	

			C. Flashcards - service provider generated, non-editable D. Quizzes - customisable / user generated E. Polls - customisable / user generated F. Flashcards - customisable / user generated G. Quizzes, polls and/or flashcards can be shared as templates for re-use by others	
<b>PF12</b>	(Question removed from 2021.1)			
<b>PF13</b>	In relation to the file download functionality available, select all files types that can be downloaded within the service.		A. Executable files and/or code (e.g., .exe) B. Desktop publishing files (e.g., .doc, .pdf, .ppt) C. Image files (e.g., .png, .jpg, .jpeg) D. Audio files (e.g., .mp3, .wma, .wav) E. Video files (e.g., .avi, .mov, .wmv, .gif) F. Database files (e.g., .dat, .csv, .log, .mdb) G. Other	
<b>PF14</b>	(Question removed from 2023.1)			
<b>PF15</b>	When sending correspondence via the service on behalf of the school, how does the service send email communication to the school's recipients/audience? Select all that apply.		A. Sent from the school user's registered email address B. Sent from the service's domain (e.g., user@servicename.com) C. Sent from unverified, anonymous or invalid email addresses D. Other	
<b>PF16</b>	What, if any, third party products are used to provide the file upload and storage functionality within the service? Select all that apply.		A. YouTube B. Vimeo C. Flickr D. Image Shack E. Picasa F. Other image and video streaming services G. DropBox H. Google Drive I. OneDrive	

			J. Box K. iCloud L. Other cloud storage and file sharing M. No third-party products are used	
<b>PF17</b>	In relation to the file upload and sharing functionality available within the service, select all that apply.		A. Authors have control over who can view and/or edit their files B. Administrators (e.g., teachers) can restrict who can view and/or edit users' files C. Administrators can disable file sharing D. None of the above E. Not applicable – file sharing is not supported	
<b>PF18</b>	(Question removed from 2023.1)			
<b>PF19</b>	In relation to the content creation functionality available within the service, select all that apply.		A. Users can share their content (e.g., via direct urls) B. Users have control over who can view or edit their content C. Administrators can restrict who can view and/or edit users' content D. Administrators can disable sharing of users' content E. None of the above	
<b>PF20</b>	Select the response option which best describes the publication of user generated content. Publication means visible to all members and/or visitors to the service.		A. User generated content can be published to the service but no privacy settings can be applied B. User generated content can be published to the service and privacy settings can be applied C. User generated content cannot be published to the service	
<b>PF21</b>	In relation to the content libraries available within the service, select all that apply. Content may include:		A. Educational or curriculum aligned content and activities B. Non-educational content and activities C. Template libraries (e.g., presentations, web design, surveys etc.) D. Image, video and audio libraries	

			<p>E. Search results that are not filtered based on user characteristics (e.g., age, year level, user type etc.)</p> <p>F. None of the above</p>	
<b>PF22</b>	<p>Who can publish content to content libraries within this service (i.e., users or service provider); and is content subject to moderation to ensure users are not exposed to information, including images, video, text and/or recordings, which may be deemed:</p> <ul style="list-style-type: none"> <li>• Offensive by a reasonable member of the school community (e.g., nudity, pornography, graphic content, profanity, racist, sexist etc. and/or</li> <li>• Inappropriate for users under 18 years?</li> </ul> <p>Moderation may include:</p> <ul style="list-style-type: none"> <li>• The service reserves the right to remove content that breaches the Terms of Use</li> <li>• The service applies a profanity filter</li> <li>• The service has an implemented assurance procedure to ensure content conforms to quality standards prior to publication</li> <li>• Users can report content that breaches the Terms of Use</li> </ul> <p>Select all that apply.</p>		<p>A. Service provider generated content with moderation</p> <p>B. Service provider generated content without moderation</p> <p>C. User generated content with moderation</p> <p>D. User generated content without moderation</p>	
<b>PF23</b>	<p>In relation to the notification and alert functionality available within the service, select all that apply.</p>		<p>A. Notifications and alerts can be one-way (broadcast)</p> <p>B. Notifications and alerts can be two-way e.g., parents/recipients can respond to notifications and alerts</p> <p>C. Notifications can be via email</p> <p>D. Notifications can be via SMS</p> <p>E. Notifications can be via push notifications</p> <p>F. Notifications and alerts can be disabled by an administrator/moderator</p>	

			<p>G. For each notification and/or alert, the school and/or users can specify and/or limit the audience</p> <p>H. The school and/or user can create and manage a subscriber group, and only members of this group can receive notifications and/or alerts from the school and/or user</p>	
<b>PF24</b>	(Question removed from 2021.1)			
<b>PF25</b>	In relation to the online learning activities, assessment and/or game functionality available within the service, select all that apply.		<p>A. The service provides standardised testing</p> <p>B. The teacher or user can create their own online learning activities and/or games.</p> <p>C. Answers can include pre-defined response options (e.g., multiple choice, Likert scales etc.)</p> <p>D. Answers are numerical free text fields (e.g., 0-9)</p> <p>E. Answers are short response free text fields (e.g., typing, equations, units of measurement, spelling and vocabulary)</p> <p>F. Answers can include long response free text fields (e.g., sentences, paragraphs, essays etc.)</p> <p>G. Answers can include file uploads (e.g. uploading a word document, image file etc)</p> <p>H. Data analysis, analytics and/or reporting is generated</p> <p>I. Data analytics and/or reporting can be sent to parents via the service.</p> <p>J. Notes or comments can be made against a response, learning activity, assessment and/or game</p>	
<b>PF26</b>	Select the response option which best describes the publication of results on the service. Results are		A. Student results can be published on the service but privacy settings cannot be applied.	

	considered to be published if they are visible to anyone other than the owner of the results.		B. Student results can be published on the service and privacy settings can be applied. C. Student results cannot be published.	
<b>PF27</b>	In relation to any other functionality that is offered by the service, select all that apply.		A. Online ordering B. Financial management or payment processing systems C. Enrolment management D. Student information, student management system, school administration or student administration system E. Customer relationship management F. Ticketing systems G. Electronic document and records management systems H. Data integration, aggregation, data broker, data hub, data distribution hub I. Library Management J. Visitor Management K. Event management, bookings, online ordering or fundraising L. Subject selection M. Class formation N. Assignment submission O. Plagiarism detection P. Roll marking Q. Absence reporting and notifications R. Timetabling S. Academic reporting T. Other (please specify) U. None of the above	
<b>PF28</b>	What names do you, as the service provider, give to the various modules available within the service?		<i>Informational question- used to inform QA and data assets disclosed to service.</i>	
<b>PF29</b>	What additional student data - other than that which is mandatory to register an account - can be provided to / collected by the service when used for its intended		For each indicate mandatory, optional or not collected:	

	purpose? Please indicate whether this data field is mandatory or optional.		A. Protection details B. Legal custodian arrangements C. Out of home care status D. Records of behaviour incidents E. Behavioural observations/notes F. Support arrangements G. Professional case notes H. Consent I. Attendance, including reason for absence J. Records of interview and/or contact K. Academic results L. Academic testing M. Personality profiling, career goals and/or interests N. Commonwealth Unique Student Identifier (AU) or National Student Number (NZ) O. Timetabling P. Emergency contacts Q. Other (please specify) R. None of the above	
<b>PF30</b>	What additional student, staff and/or parent data - other than that which is mandatory to register an account - can be provided to / collected by the service when used by the school for its intended purpose? This question is not intended to collect information about parent's personal use of the service (e.g., when it is not associated with school use/subscription). For each data asset, please specify whether it relates to student, staff, or parent. Select N/A if not collected.		For each indicate mandatory, optional or not collected:  A. Medical details B. Well-being information C. Year level D. Class name E. School name F. Works G. Image H. Video or audio recording I. Email address J. First name K. Surname L. Date of Birth	



			M. Age, month and year of birth, or year of birth N. Home address O. Phone number P. Identification documentation Q. Electronic signature R. Cultural and citizenship details, racial or ethnic origin S. Religion T. Gender U. Languages spoken V. Username - determined by the user W. Country or State/province X. Responses - online learning, surveys, forms Y. Resume, CV, applications, references Z. Certificates and accreditation AA. User location data AB. N/A	
<b>PF31</b>	What, if any, other data not listed above can be disclosed to or collected by the service if used for its intended purpose? Please specify if data relates to student, staff or parent and whether it is mandatory or optional.		Free text field (informational)	
<b>Data integration, aggregation, data broker, data hub, data distribution hub control questions (PF32, PF33, PF35, PF36, PF40-PF50)</b>				
<b>PF32</b>	In relation to the data integration, aggregation, data broker, data hub, data distribution hub functionality, does the service (the collector of data/ data aggregator / data broker) assume ownership of any data transferred to, or transiting through, the service?		A. Yes <b>B. No (T1, T2)</b>	
<b>PF33</b>	In relation to the sharing of data with any third party (any service which receives data of any form from the service), are enforceable, written agreements in place with data suppliers or recipients that covers: <ul style="list-style-type: none"> <li>the purpose for data sharing;</li> </ul>		A. No B. Yes - Some of the above but data agreements not updated C. Yes - Some of the above with data agreements updated	

	<ul style="list-style-type: none"> <li>the scope of data to be shared (e.g., academic results);</li> <li>the scale of data sharing (e.g., current student records only, or a specific year level);</li> <li>the security and privacy controls in place in recipient systems; and</li> <li>ownership of data.</li> </ul> <p>Furthermore, data agreements are updated to reflect changes in any of the above?</p>		<b>D. Yes (T1, T2)</b>	
<b>PF34</b>	Retired			
<b>PF35</b>	Who authorises the transfer of data, including the data scope (e.g., student academic results) and scale (e.g., only year 8 students) from the service (data integration/aggregation service, data broker, data hub, data distribution hub) to recipient third party systems:		<p>Select all that apply:</p> <p><b>A. Data sharing can be controlled by the customer (school, school system or jurisdiction) (T1, T2)</b></p> <p>B. Data sharing can be controlled by the data aggregator (service being assessed)</p> <p>C. Data sharing can be controlled by the data recipient</p>	
<b>PF36#</b>	When a data breach or data loss event occurs in third party recipient systems, who notifies the customer (e.g., school, school jurisdiction or school system)?		<p><b>A. Data aggregator notifies customer as soon as possible after discovery and provides all relevant details (T1, T2).</b></p> <p>B. Data aggregator notifies customer without commitment to timeframe and/or details not provided.</p> <p>C. Third party service notifies customer as soon as possible after discovery and provides all relevant details.</p> <p>D. Third party service notifies customer without commitment to timeframe and/or details not provided.</p> <p>E. Unknown (#T1, #T2)</p> <p>F. No notification of customer occurs (#T1, #T2)</p>	

<b>PF40</b>	Does your service offer enterprise level controls (for example schools that belong to an owning higher authority (e.g. a Department or Education Authority))?	1 & 2	A. No B. Yes – two or more levels (e.g. school level controls and Departmental controls) <b>C. Yes – two or more levels with Departmental controls overriding school level controls (T1, T2)</b>	
<b>PF41</b>	When your service ingests data from a customer’s source system, does the customer have the ability to specify and restrict the exact data elements/fields (i.e. ‘select’ and ‘where’ clauses) shared with your service?	1 & 2	A. No (please specify) B. Yes - source system extract can be defined by the school only C. Yes - source system extracts can be defined by the school or higher (enterprise/departmental) authority. Higher authority settings can be altered by the school <b>D. Yes - source system extracts can be defined by the school or higher (enterprise/departmental) authority. Higher authority settings cannot be altered by the school (T1, T2)</b>	
<b>PF42</b>	Does your service offer the ability for the customer to restrict which recipient systems are available for integration?	1 & 2	A. No B. Yes - Recipient systems can be defined by the school only <b>C. Yes - Recipient systems can be defined by the school or higher (enterprise/departmental) authority and are not able to be modified schools (T1, T2)</b>	
<b>PF43</b>	Can the customer of your service restrict the data elements/fields that are shared with each individual recipient system?	1 & 2	A. No <b>B. Yes (please specify) (T1, T2)</b>	

<b>PF44</b>	Does your service have an administrative view that clearly shows to the customer which recipient systems your service is currently sharing customer's data with and the types of data being shared?	1 & 2	A. No B. <b>Yes (T1, T2)</b>	
<b>PF45</b>	Does your service require customers to regularly reauthorize all recipient and integrating systems and perform a review of all data elements/fields shared?	1 & 2	A. No B. <b>Yes (please describe the process including frequency) (T1, T2)</b>	
<b>PF46</b>	Does your service offer the ability to filter and thereby prevent, exclude or limit the collection or handling of a specific individual's information or their related data?	1 & 2	A. No B. Yes - filtering can be applied only <b>after</b> source data is consumed by your service. Filtered records are then not shared with recipient systems (please describe) C. <b>Yes - filtering can be applied prior to data being consumed by your service (T1, T2) (please describe)</b> D. Yes – other (please describe)	
<b>PF47</b>	When a customer withdraws data sharing approval for a recipient system what action does your service take?	1 & 2	A. The service immediately suspends all data sharing with the recipient system. B. The service notifies the recipient system of the withdrawal of approval. C. The service purges all data within the service it holds related to the recipient system. D. <b>All of the above (T1, T2)</b> E. None of the above.	
<b>PF48</b>	Does your service support the two-way flow of data i.e. data can be sent to a recipient system AND data can be returned from the recipient system to your service for write-back to customer systems?	1 & 2	A. No B. <b>Yes. Please specify which systems and data are supported for write-back from your service. (T1, T2)</b>	

<b>PF49</b>	Prior to onboarding a recipient system to your service, what due diligence checks and verifications are performed by your organisation on recipient systems?	1 & 2	<p>A. Security check performed or evidence of security maturity obtained (please specify including details of any industry standard or other certifications)</p> <p>B. Privacy check performed or evidence of privacy maturity obtained (please specify including details of any industry standard or other certifications)</p> <p>C. Security and privacy requirements are detailed in contracts between the service's organisation and the recipient system</p> <p><b>D. All of the above (T1, T2)</b></p> <p>E. None of the above.</p>	
<b>PF50</b>	Are ongoing checks and monitoring performed by your organisation on the service's recipient systems to ensure compliance with security and privacy requirements?	1 & 2	<p><b>A. Yes (please detail and specify frequency) (T1, T2)</b></p> <p>B. No</p>	
<b>PF37</b>	In relation to the assessment or collection of health and well-being information through functionality available within the service, select all that apply:		<p>A. Online forms – service provider generated, non-editable</p> <p>B. Surveys – service provider generated, non-editable</p> <p>C. Quizzes – service provider generated, non-editable</p> <p>D. Polls – service provider generated, non-editable</p> <p>E. Learning activities and/or game-based assessment</p> <p>F. Diagnostic and/or standardised testing</p> <p>G. Online forms – customisable / user generated</p> <p>H. Surveys – customisable / user generated</p> <p>I. Quizzes – customisable / user generated</p> <p>J. Polls – customisable / user generated</p>	

		<p>K. Learning activities and/or game-based assessment – customisable / user generated</p> <p>N. Data analysis, analytics and/or reporting is generated for users based on their responses</p> <p>P. Well-being data analytics and/or reporting can be sent to parents via the service.</p> <p>Q. In-built monitoring and/or reporting tools identify respondents who may require follow-up or additional support.</p> <p>R. No in-built monitoring and/or reporting tools are provided to identify respondents who may require follow-up or additional support.</p>	
<b>PF38</b>	In relation to the response options available within the service to assess or collect health and well-being information, select all that apply:	<p>A. Responses can include pre-defined response options (e.g., multiple choice, Likert scales etc.)</p> <p>B. Responses are numerical free text fields (e.g., 0-9)</p> <p>C. Responses are short response free text fields (e.g., typing, equations, units of measurement, spelling, and vocabulary)</p> <p>D. Responses can include long response free text fields (e.g., sentences, paragraphs, essays etc.)</p> <p>E. Users can request further assistance or to talk to someone.</p> <p>F. Users can request further assistance or to talk to someone and this automatically notifies the school-nominated staff member.</p> <p>G. Users are de-identified and response data is aggregated/summarised so users and respondent data and reports are anonymous.</p> <p>H. Response data is aggregated/summarised so respondent data and reports do not identify the user.</p>	

			I. Respondent data and reports identify individuals for the purpose of monitoring, action and follow-up. J. Other	
<b>PF39</b>	With regards to personal information in the service, does the service log the following events: - Creation - Access - Modification - Deletion	1 & 2	A. No – None of the above B. Yes – Some of the above <b>C. Yes – All of the above (T1, T2)</b>	NZPP
<b>PF51</b>	In relation to file upload functionality within the service, are the principles and techniques from the OWASP followed?	1 & 2	A. No - None of the principles or techniques are followed B. Yes - Only some of the principles and techniques are followed C. Yes - Majority of the principles and techniques are followed excluding AV scanning D. Yes - Majority of the principles and techniques are followed including AV scanning <b>E. Yes - All of the principles and techniques are followed (T1, T2)</b>	

## 6.4 Criteria – Interoperability

### 6.4.1 Interoperability – Data Standards

#	Question	Tier	Response options
<b>DS4</b>	Select from the following education specific data standards that are supported by the service for importing or exporting data.	All	A. SIF Australia (AU) B. SIF New Zealand (NZ) C. IMS OneRoster D. Other (please specify) E. None of the above

<b>DS5</b>	Has the service undertaken any assurance or compliance testing against any education specific integration technologies or data standards?	All	A. SIF Assurance B. IMS OneRoster conformance certification C. IMS Learning Tools Interoperability (LTI) D. NSIP HITS Testing E. Other (please specify) F. None of the above
<b>DS6</b>	After exchanging or consuming data into the product how soon is this information available to end users of the product? (e.g., if a new set of school master data is imported via an API, is this available immediately in the product drop downs, reports, etc., is the import manually reviewed and available within 5 business days etc.)?	All	Collected for reference only  A. Immediately B. Other time frame (Please specify)

#### 6.4.2 Interoperability – Technical Integration

#	Question	Tier	Response options
<b>INT5</b>	Please select from the following integrations or connections that are available within the service.	1 & 2	A. Native connections/integrations to other 3rd party services B. Partner built connections/integrations to other 3rd party services (e.g. available on your marketplace/extension store) C. Open APIs (e.g. REST, GraphQL etc for custom built integrations) D. FTP/SFTP (e.g. automatically importing or exporting data from a FTP server) E. Data feed (e.g. routinely fetching an XML file from a URL) F. Direct database connection (e.g. SQL user or via an agent software) G. Other (please specify) H. None of the above
<b>INT6</b>	What role types are available to restrict which integrations and connections are available to users within the service?	1 & 2	A. School Administrator B. Department / Jurisdiction / District Administrator C. Other (please specify) D. None of the above
<b>INT7#</b>	In relation to <b>native and partner built connections or integrations</b> , are agreements in place between the organisation and all 3rd party services being connected or integrated with and do these agreements cover: <ul style="list-style-type: none"> <li>the purpose for data sharing;</li> </ul>	1 & 2	<b>A. Yes (please specify) (T1, T2)</b> B. No (#T1, #T2)



	<ul style="list-style-type: none"> <li>• the scope of data to be shared (e.g. academic results);</li> <li>• the scale of data sharing (e.g. current student records only, or a specific year level);</li> <li>• the security and privacy controls in place in recipient systems; and</li> <li>• ownership of data.</li> </ul> <p>Furthermore, data agreements are updated to reflect changes in any of the above?</p>		
<b>INT8</b>	In relation to <b>partner built connections or integrations</b> , what due diligence checks and verifications are performed by your organisation prior to the connection or integration being made available to users?	1 & 2	<p>A. Security check performed or evidence of security maturity obtained (please specify including details of any industry standard or other certifications)</p> <p>B. Privacy check performed or evidence of privacy maturity obtained (please specify including details of any industry standard or other certifications)</p> <p>C. Security and privacy requirements are detailed in contracts with the organisation that develops and manages the integration or connection</p> <p><b>D. All of the above (T1, T2)</b></p> <p>E. None of the above.</p>
<b>INT9</b>	In relation to <b>partner built connections or integrations</b> , does your organisation conduct ongoing monitoring to ensure compliance with your privacy and security requirements (e.g. developer guidelines, platform rules etc).	1 & 2	<p><b>A. Yes (please specify) (T1, T2)</b></p> <p>B. No</p>
<b>INT10</b>	In relation to <b>native and partner built connections or integrations</b> , does your service require the user to re-authorise or reconfirm integrations are still valid on a periodic basis?	1 & 2	<p><b>A. Yes (please specify timeframe) (T1, T2)</b></p> <p>B. No</p>
<b>INT11</b>	In relation to <b>native and partner built connections or integrations</b> , does the service provide privacy controls to restrict a users information (and any related information) from being shared to the integration (e.g. toggle opt-in/opt-out of certain users).	1 & 2	<p><b>A. Yes (please specify) (T1, T2)</b></p> <p>B. No</p> <p>C. N/A - Connections or integrations do not share user data or any related data</p>
<b>INT12</b>	In relation to <b>native and partner built connections or integrations</b> , if a user removes or deactivates the integration/connection, is the 3rd party system	1 & 2	<p><b>A. Yes (please specify) (T1, T2)</b></p> <p>B. No</p> <p>C. N/A - Connections or integrations do not share any user data</p>

	required to delete any information it had received from the integration?		
--	--	--	--

## 6.5 Criteria – Safety

#	Question	Tier	Response options
<b>SFP1</b>	Does the organisation regularly review and incorporate the Safety by Design principles into the product design and throughout operation of the service?	1 & 2	<b>A. Yes (T1, T2)</b> B. No
<b>SC1</b>	Is there an acceptable usage policy for the service that is freely available and: - Published on the internet, or - Provided to customers prior to usage of the service?	1 & 2	<b>A. Yes - Published on the website (please provide a link) (T1, T2)</b> <b>B. Yes - Provided to users prior to usage of the service (please specify) (T1, T2)</b> C. No
<b>SC1A</b>	If students use or interact with the service, is the acceptable usage policy written in child friendly language?	1 & 2	A. No <b>B. Yes (T1, T2)</b> C. N/A - Students do not use or interact with the service
<b>SC1B</b>	Please provide details on how to access the service's acceptable usage policies, weblinks and any other relevant materials.	1 & 2	
<b>SC2</b>	Does the organisation (which provides the service) have a process to handle the following from customers: • Technical and operational fault reports • Security incidents and concerns • Privacy complaints and requests; and • Child safety complaints?	1 & 2	A. No B. Yes - includes some of the above <b>C. Yes - includes all of the above (T1, T2)</b>
<b>SC3</b>	Has the organisation's staff (or contractors) been found guilty of any child safety misconduct or other related child safety offenses?	1 & 2	<b>A. No (T1, T2)</b> B. Yes
<b>SC4</b>	Does the organisation that provides the product or service ensure all of its staff/contractors: • Receive induction regarding the importance of child safety; • Are appropriately supervised to ensure they are behaving in a child safe way when supporting schools; • Receive training that acknowledges student diversity;		A. No B. Yes - some of the above <b>C. Yes - all of the above (T1, T2)</b>

	<ul style="list-style-type: none"> <li>Consider diversity (gender-diversity, religious beliefs, indigenous cultural safety, etc) in the product design?</li> </ul>		
<b>SC5</b>	Are controls in place within the service to restrict non-school users from interacting with the school's students except where the user has been individually authorised by the school to do so?		A. No B. N/A - There are no student communication features or methods <b>C. Yes - Please specify (T1, T2)</b>
<b>SC6</b>	Does the service have real time detection tools to quarantine and alert administrators to offensive and/or inappropriate comments, messaging and content?  For each functionality, select whether this control is available.		A. Available B. Not Available  Applicable functionality: - Chat / Instant Messaging - Content creation - Commenting / Community Forums

## 6.6 Criteria – Desktop and Mobile Applications, Browser Extensions

#	Question	Tier	Response options
<b>AP0</b>	Please select if any of the following application types are available	1 & 2	A. Mobile Application (e.g. Phone or Tablet App) B. Browser Extension/Plugin C. Desktop Application D. Other (please specify) E. None of the above
<b>AP1</b>	Does your organisation conduct a vulnerability scan on all of the service's application types: - Upon each deployment (e.g. when publishing a new version), and - Periodically on a monthly or more frequent basis.	1 & 2	A. No <b>B. Yes - meets all of the requirements above but conducted less frequently (T2)</b> <b>C. Yes - meets all requirements above (T1, T2)</b>
<b>AP2</b>	Is the mobile app, browser extension and/or desktop application assessed per a security testing methodology that is consistent with the guidance provided by the latest industry standard frameworks (e.g. for Mobile Applications, the OWASP Mobile Application Security Testing Guide)?	1 & 2	<b>A. Yes - security testing fully satisfies the guidance provided in an industry standard framework (please specify framework) (T1, T2)</b> B. Yes - security testing partially satisfies the guidance provided in an industry standard framework (please specify framework) C. No

<b>MA1</b>	Please select from the following channels the mobile app offered by your organisation.	1 & 2	A. Apple App Store B. Google Play Store C. Other Android marketplace (please specify) D. Manual installation (please specify) E. Other (please specify)
<b>MA1A</b>	Apple App Store URL, Google Play Store URL, Other Android marketplace URL	1 & 2	
<b>MA2</b>	Select the device permissions that may be requested by the mobile app.	1 & 2	A. Camera B. Photo / Media Library C. Calendar D. Reminders E. Microphone F. Location G. Local Network H. Bluetooth I. Notification J. Health and Motion Data or Activity (e.g. Apple Health Kit, Google Health, Samsung Health) K. No device permissions are requested L. Other (please specify)
<b>MA3</b>	Does the mobile app only request permissions that are necessary for the app to function for its expected purpose?	1 & 2	<b>A. Yes (T1, T2)</b> B. No
<b>BE1</b>	Select from the following channels the browser extension offered by your organisation:	1 & 2	A. Apple App Store or Safari Extension Store B. Mozilla Firefox Extension Store C. Google Chrome Extension Store D. Microsoft Edge Add-ons Store E. Manual installation or installation outside of an extension store or marketplace (please specify) F. Other (please specify)
<b>BE2</b>	Select the browser/device permissions that are requested by the browser extension.	1 & 2	A. Location B. Camera C. Microphone D. Motion sensors E. Bookmarks

			F. Browser history G. Browser tabs H. Clipboard I. Browser settings J. Read or change site data K. Other (please specify) L. No browser/device permissions are requested
<b>BE3</b>	Does the browser extension only request permissions that are necessary for it to function for its expected purpose?	1 & 2	<b>A. Yes (T1, T2)</b> B. No

### 6.7 Criteria – Informational

#	Question	Tier	Response options
<b>INF1</b>	Can the service be configured to only allow access from a given IP address/range?	1 & 2	Collected for reference only  A. Yes (Please specify) B. No

### 6.8 Evidence

Depending on supplier responses to prior questions, the following documentary evidence is required to be uploaded (system accepts PDF, .DOC, .DOCX).

#	Evidence	Related to question ID
EV1	Attestation of PCI-DSS Compliance	CC2
EV2	ISO27001 Certificate of Compliance / Statement of applicability	CC1
EV3	SOC 2 Type II Certification	CC1
EV4	FEDRAMP (NIST) Certification	CC1
EV5	IRAP Accreditation	CC1
EV6	Your organisation's Information Security Policy	Q7
EV7	Business Continuity Plan for the service	Q2
EV8	Disaster Recovery Plan for the service	Q2
EV9	Incident Response Plan or Security Incident Management Plan	T6
EV10	Most recent penetration testing report (redacted) for the service	T1
EV11	Most recent vulnerability assessment reports (redacted) for the service	T1

EV12	Patch management standards / process	T3, T4, T5
EV13	Your organisation's Secure Software Development Lifecycle process	Q5
EV14	Privacy compliance/certification	CC1
EV15	CSA Star	CC1
EV16	HECVAT	CC1
EV17	Sample agreement between service (data integrator, aggregator, data broker, data hub, data distribution hub) and third party	PF33
EV18	A list of all third-party services (company and service names) for which service accounts are required to be created (including access levels e.g., administrator, regular user)	A16A
EV19	Please supply a list of all third-party recipient services (company and service names) including the data types shared (e.g., personal information, medical information, financial data), and the purpose for sharing, with whom the service currently shares data.	PF32
EV20	Evidence of WCAG compliance for the service.	P14
EV21	1EdTech TrustEd Apps(TM) Certification	CC1

In addition, other evidence may be requested or inspected throughout the assessment process. This includes information on a supplier's website, terms and conditions, privacy policies and other documentation or information.

In assessing and reviewing documentation requirements, the ST4S Team makes considerations to:

- Content: Does the document contain the sections per the relevant ST4S control as described in the table above. Documentation should contain specific and relevant technical information to the service being assessed.
- Quality: Does the document demonstrate a level of standard relevant to the determined tier of the service.

#### Documentation Requirements:

All documentation provided throughout the assessment must be in English, be an authorised and final copy by the organisation and contain the organisation's name and company number.

If the supplier holds a valid ISO27001 certification or has undertaken a Soc2Type2 Audit, the ST4S Team may upon review, choose to accept this certificate as meeting some evidence and documentation requirements. Please ensure the relevant certification has been selected within the assessment questionnaire and that you upload the certificate or audit report. Importantly, ISO27001 and Soc2Type2 are only accepted where the supplier's organisation is named on the certificate and their service was in scope of the review.

#### Verification and Validation:

The ST4S Team may contact the author, certifying body etc to verify the authenticity of documentation, evidence, and other information. For example, we may contact the ISO accrediting body to verify an ISO certificate, ask a pen tester to provide evidence of their certification (e.g. providing a certificate number for us to verify) etc.

## 6.6 Minimum criteria

Questions marked with a hash (#), can lead to a “Non-compliant” assessment outcome if the minimum preferred response/s are not met.

These questions are for Tier 1 products/services: H5, S1, S2, S3, S4, S5, S7, S8, S9, S10, S11, S13, A1, A2, A5, A6, A7, A10, A11, A13, A16b, HR1, HR2, HR3, T1, T2, T3, T6, T7, Q5, Q7, D3, CC2, PR1, PR2, PR10, PR12, PR13, PR14, PR16, PR17, PF6, PF7, PF8, PF9, PF10, PF36, G01, G02, INT7.

For Tier 2 products/services: H5, S1, S2, S3, S4, S5, S7, S8, S10, S11, S13, A1, A2, A13, A16b, HR3, T1, T6, T7, Q5, D3, CC2, PR1, PR2, PR17, PR10, PR12, PR13, PR14, PF6, PF7, PF8, PF9, PF10, PF36, G01, G02, INT7.

## 6.7 Updates to the ST4S Criteria, Response Options & Minimum Standards

Given the rapid change to the underlying standards which the ST4S criteria draw on, the ST4S Team is estimating that the ST4S criteria (as represented in this document) will be updated every six months, with release likely occurring in January/February and June/July each year. In addition, the ST4S Team may make interim updates to ST4S criteria and/or this guide. This may include changes such as: correcting the wording of a question and response options, adding/removing/adjusting criteria etc. Suppliers are advised to frequently check for the latest version of the ST4S Supplier Guide as published on the ST4S website.

### 6.7.1 Key Changes to the ST4S Criteria (from 2022.1):

The following is a list of the key changes to the ST4S Criteria for 2023.1:

Criteria ID	Change	Description
H5	Change	Updated question text
H6	Change	Updated question text and answer options
P2F	New	New informational question
P10	Change	Updated answer options
S7	Change	Updated question text
A1	Change	Updated question text
A2	Change	Updated question text
A8	Change	Updated question text
A15	Change	Updated answer options
A15A	New	New informational question
A16A	Change	Updated question text

Criteria ID	Change	Description
HR2	Change	Updated question text
D2	Change	Updated question text and answer options
D4	Retired	
D5	New	New question relating to data management
D5A	New	New question relating to data management
D6	New	New question relating to data management
PR5	Change	Updated question text
PR16	New	New question relating to changes to the Privacy Policy and Terms of Service
PR17	New	New question relating to sub processors
PR18	New	New question relating to sharing of data
PR19	New	New question relating to sharing of data
PR20	New	New question relating to sharing of data
CC1	Change	Updated answer options
GO1	Change	Updated question text
GO2	Change	Updated question text
PA3	Change	Updated answer options
PF1	Change	Updated question text
PF4	Change	Updated answer options
PF 14	Retired	
PF51	New	New question relating to anti-virus/malware scanning
PF18	Retired	
PF25	Change	Updated answer options
PF29	Change	Updated answer options
DS1	Retired	
DS2	Retired	
DS3	Retired	
DS4	New	New question relating to data standards
DS5	New	New question relating to data standards
DS6	New	New question relating to data standards
DA1	Retired	
INF1	New	New informational question
INT1	Retired	
INT2	Retired	

*Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.*



Criteria ID	Change	Description
INT3	Retired	
INT4	Retired	
INT5 - INT12	New	Data Broker / Integrations
SFP1	New	Safety Criteria and Safety Principles
SC1 - SC6	New	Safety Criteria and Safety Principles
AP0 - AP2	New	Application General
MA1 - MA3	New	Mobile Applications
BE1 - BE3	New	Browser Extensions
EV21	New	New evidence requirement for added response option in CC1
EV20	New	New evidence requirement for WCAG compliance in P14

## Appendix A – Tier Self-Assessment

The breadth and depth of an assessment performed on a supplier's service is based on the assessment tier. Three factors contribute to a service's tier categorisation:

1. Data: The data stored or processed by the service.
2. Functionality: The service's functions, including any permissions a service or application may request of a device.
3. Reasonableness: The service's display and communication of advertising or other materials which may cause offence.

The tier used for assessment purposes is the highest tier that the service qualifies against across all three categories.

1) Data		
Assessment Tier	Data Definitions	Data examples
Tier 1	Sensitive information is a type of personal information that is given extra protection and must be treated with additional care. It includes any information or opinion about an individual's racial or ethnic origin, political opinions,	Sensitive information, including: <b>for students:</b> religion, birth certificate, language spoken at home, religious records (for example Baptism Certificate), religious education, whether Aboriginal or Torres Strait Islander, nationality, country of birth, legal

1) Data		
Assessment Tier	Data Definitions	Data examples
	<p>membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record. It also includes health information and biometric information.</p> <p>Health information is a subset of sensitive information. It is any information or opinion about the health or disability of an individual, the individual's expressed wishes about the future provision of health services and a health service provided, currently or in the future, to an individual that is also personal information. Health information also includes personal information collected in the course of providing a health service.</p> <p>Financial information covers individual, family, staff, student financial records, bank details, debts, debt reminders etc.</p> <p>Identifiers covers government or other allocated identifiers which are possibly sensitive for the purposes of tracking an individual.</p>	<p>information (custody, legal orders, out of home care), geographic location (GPS/lat/long), biometric data (eye/retinal imagery, fingerprints), welfare and discipline reports, passport details</p> <p>for parents: place of birth, religions, religious education, criminal record check, relevant child protection information (including working with children checks if volunteering to assist in the classroom), country of birth, whether Aboriginal or Torres Strait Islander, and nationality, legal information (custody, legal orders, out of home care), marital status/problems, voting in board elections</p> <p><b>for job applicants, staff and contractors:</b> place of birth, religion, religious education, criminal record check, relevant child protection information (including working with children checks), member of professional associations, trade union membership, country of birth, nationality, OHS incident reports, staff complaints, workplace issue reports, letters of appointment/ complaint/ warning/ resignation, professional development appraisals, performance review, passport details</p> <p><b>Health information, including:</b></p> <ul style="list-style-type: none"> <li>• for students: medical background, immunisation records, medical records, medical treatments, accident reports, absentee notes; medical certificates, health and weight, nutrition and dietary requirements, assessment results for vision, hearing and speech, reports of physical disabilities, illnesses, operations, paediatric medical, psychological, psychiatric, learning details (recipient special procedures), assessment for speech, occupational, hearing, sight, ADD, Educational Cognitive (IQ), health or other gov. service referrals</li> <li>• for parents: history of genetic and familial disorders (including learning disabilities), miscellaneous sensitive information contained in a doctor or health report; and</li> <li>• for job applicants, staff members and contractors: medical condition affecting ability to perform work, health information, medical certificates and compensation claims.</li> </ul>

1) Data		
Assessment Tier	Data Definitions	Data examples
		<p><b>Financial information including:</b> Credit card details, account details, payment overdue notices, financial information relating to payment of school and administrative fees, banking details, scholarship details and information about outstanding fees, donation history, details of previous salary, salary being sought and other salary details, superannuation details</p> <p><b>Identifiers includes:</b> local, state and federally or nationally assigned student, parent or staff identifiers (government related identifiers) Examples: Tax File Number, Victorian Student Number, Medicare number, Drivers License number, Passport, teacher registration number.</p>
Tier 2	<p>Personal information not captured in the 'High' tier: Personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable whether the information is true or not, and whether the information is recorded in a material form or not. It includes all personal information regardless of its source.</p> <p>In other words, if the information or opinion identifies an individual or allows an individual to be identified it will be 'personal information' within the meaning of the Privacy Act. It can range from very detailed information, such as medical records, to other less obvious types of identifying information, such as an email address. Personal information does not include information that has been de-identified so that the individual is no longer identifiable</p>	<p><b>for students:</b> name, sex/gender, physical address, email address, social media handles, phone number, date of birth (and age), conduct reports, next of kin details, emergency contact numbers, names of doctors, school reports and exam/test results, attendances, assessments, previous school history, referrals (e.g. government welfare agencies/departments), correspondence with parents, photos, current/previous school, health fund details</p> <p><b>for parents:</b> name, physical address, email address, phone number, date of birth, vehicle registration details, occupation, doctor's name and contact information, other children's details, maiden name of ex-pupils, alumni year, whether alumni had further education, professional experience and personal news</p> <p><b>for job applicants, staff and contractors:</b> name, company name and ABN, phone number, physical address, email address, date of birth and age, contact details of next of kin, emergency contact numbers, including doctor, residency status/work visa status, qualifications, education, academic transcript, work permit, details of referees, marital status, record of interview, leave applications, photograph, applications for promotions, references, commencement date, employment agency details, former employers.</p>

1) Data		
Assessment Tier	Data Definitions	Data examples
Tier 3	Non-PII data. Data not falling into either the High or Medium sensitivity tiers. Data in this tier is typically in the public domain or presumed to pose low or no risk.	Data assumed to be in public domain or low / no risk data

2) Functionality / Purpose of service & 3) Reasonableness		
Tier	Functionality	Reasonableness
Tier 1	<p>Products which offer generic functionality in any of the following categories will be deemed as falling into tier 1:</p> <ul style="list-style-type: none"> <li>o Remote access</li> </ul> <p>Products in the following broad product categories will be deemed as tier 1:</p> <ul style="list-style-type: none"> <li>o Learning Management/ Student management and learning support systems e.g., student work, assessment, academic results, timetabling, pastoral care, communication;</li> <li>o School administration systems, including student records, attendance, data collection e.g., enrolment, consent management;</li> <li>o Financial management/ payment collection systems;</li> <li>o Behaviour management systems;</li> <li>o Teacher professional development tools/record keeping systems;</li> <li>o File storage e.g., iCloud, Dropbox, Google Drive;</li> <li>o Services with customisable functionality - site specific (including integration with enterprise solutions or additional third-party services);</li> <li>o Video or student diary or communication tools (parent, teacher, child);</li> <li>o Video capture/audio/webcam functions;</li> <li>o Services with multiple primary purposes/functionalities (e.g., combination of those listed in Tier 2)</li> </ul>	<p>Products which may contain, display or promote the following categories of information will be deemed as falling into tier 1:</p> <ul style="list-style-type: none"> <li>o Advertising of products/services in the following categories: alcohol, controlled or banned substances, gambling, tobacco products, firearms and fire arm clubs, adult products and pornography.</li> <li>o Any function or display of information which may be deemed offensive by a reasonable member of the school community (e.g. racist, sexist content)</li> </ul>

Tier 2	<p>Products which offer functionality in any of the following categories will be deemed as falling into tier 2:</p> <ul style="list-style-type: none"> <li>o Chat/Instant or delayed messaging</li> <li>o Blogs</li> <li>o Email</li> <li>o Message boards</li> <li>o Screen sharing</li> <li>o Group calls</li> <li>o File sharing</li> <li>o Photo posting/sharing</li> <li>o Social media account sharing/integration (e.g., Facebook, Google)</li> <li>o Market places for the exchanges of goods/services</li> </ul>	<p>Products which may contain, display or promote the following categories of information will be deemed as falling into tier 2:</p> <ul style="list-style-type: none"> <li>o Political material</li> <li>o Sensitive topics which may cause offense in the community</li> </ul>
Tier 3	N/A	N/A

## Appendix B – Standards, Frameworks and References

Standard / Reference	Weblink
<b>Australian Information Security Manual</b>	<a href="https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism">https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism</a>
<b>New Zealand Information Security Manual</b>	<a href="https://www.gcsb.govt.nz/our-work/national-cyber-security-centre-ncsc/new-zealand-information-security-manual-nzism/">https://www.gcsb.govt.nz/our-work/national-cyber-security-centre-ncsc/new-zealand-information-security-manual-nzism/</a>
<b>OWASP</b>	<a href="https://owasp.org/">https://owasp.org/</a>
<b>Australian Privacy Principles</b>	<a href="https://www.oaic.gov.au/privacy/australian-privacy-principles">https://www.oaic.gov.au/privacy/australian-privacy-principles</a>
<b>New Zealand Privacy Principles</b>	<a href="https://www.privacy.org.nz/privacy-act-2020/privacy-principles/">https://www.privacy.org.nz/privacy-act-2020/privacy-principles/</a>
<b>Australian eSafety Commissioner’s Safety by Design Principles</b>	<a href="https://www.esafety.gov.au/industry/safety-by-design/principles-and-background">https://www.esafety.gov.au/industry/safety-by-design/principles-and-background</a>

## Appendix C – Storage and Processing of Information

The information within this appendix describes how information submitted as part of the Safer Technologies for Schools (ST4S) assessment process may be stored, processed and handled. For information regarding how we share results, submission data and other information with other parties please refer to ‘3. *Sharing and use of full assessment reports, findings and outcomes*’.

### Transmission of Information:

- a. We are committed to maintaining the confidentiality and security of the documentation you upload. We employ industry-standard security measures to assist us in safeguarding supplier’s information from unauthorised access, disclosure, alteration, or destruction.

- b. We use technologies such as HTTPS and file encryption to protect files as they are transmitted from suppliers to our devices and other services we use to store and process information.
- c. You understand and acknowledge that while we take reasonable precautions to protect your information, no method of transmission over the internet or electronic storage is completely secure, and we cannot guarantee absolute security.
- d. When transmitting information to us, it is your responsibility to ensure that you access the file hosting and transfer services in a secure manner. This includes applying protections such as installing and using antivirus and malware protection on your devices and verifying you are connecting to the correct website address.
- e. We use services and other tools which may reside outside of Australia. This means your information may be transferred and potentially stored in other countries.

#### **Storage and Retention:**

- 1. We store the documentation you upload on company devices and various online services we use at our organisation and as part of the ST4S program (referred to as sub processors). These services are described within the ST4S Privacy Policy and includes services such as Alchemer or Zendesk which we use to collect and process information.
- 2. Sub processors we use may store and process information differently to us. This may include storing information in different countries, encrypting files to a different standard and more. You can find out more information about how our sub processors process, store and secure your information by visiting their privacy policies and other published information (e.g. security documentation) the sub processor has published on their website.
- 3. We retain documentation and information for as long as we deem reasonably necessary (generally a minimum of 7 years) in order to:
  - a. Fulfill our obligations to the ST4S WG and facilitate business activities related to the ST4S program;
  - b. Support a ST4S WG member in complying with their archival and information keeping rules, legislation, regulations and policies;
  - c. Conduct ST4S assessment activities and ongoing monitoring and compliance of services to the ST4S framework, standards and requirements;
  - d. Conducting audits, reviews and other activities related to the ST4S program;
  - e. Other business purposes relating to the ST4S program, cybersecurity, privacy or online safety.
- 4. If documents or evidence is being submitted in relation to an assessment completed for a specific ST4S WG member, then the evidence and documentation may be shared with them. Examples may include where you or your organisation has been invited to complete the ST4S assessment on behalf of, or by a government agency and we have noted within the invitation, by email or other methods that the evidence will be shared with the ST4S WG member/s.