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:	2026.1
Date of this version:	21 June 2026
Author:	ST4S Team
Document Version Number:	V1.0 Released
Location:	Latest official version available www.st4s.edu.au

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.

Contents

Version Control & Latest Version

Note: The latest copy of the ST4S Supplier Guide is available from www.st4s.edu.au

Version Control			
Version	Date:	Author/Organization:	Comments
V1.0 V2026.1	19/06/2026	ST4S Team / Education Services Australia	Simplified question wording through minor adjustments across the Full Assessment and AI Module. Expanded the HR controls to include HR4 and HR4A to expand on child safety screening where applicable. Adjustments of some risk levels for authentication controls to ensure stronger alignment with Australian and New Zealand ISM. Conducted a review of standards/references for controls.
V1.0 V2025.1	02/12/2025	ST4S Team / Education Services Australia	Simplified question wording through minor adjustments across the Full Assessment and AI Module. Enhanced authentication controls introduced to reflect evolving methods and align with international standards. PF9 and PF10 have been restructured into sub questions to better capture non-compliant responses. Privacy controls updated to ensure stronger alignment with Australian and New Zealand privacy principles as well as ISMs.
V1.0 – v2024.1	23/01/2025	ST4S Team / Education Services Australia	AI Module updated with new criteria. The framework version has been incremented to v2024.1. Review Appendix D for upgrade/transition information. The assessment process information, disclaimer, conditions have been reorganised along with other sections to improve readability. Our approach to assessments and how we work with suppliers has been added in a new section along with notes for small business and large multi nationals on common items The Supplier Code of Conduct (the code) has been adjusted and reorganised to the Appendix of this guide. The conditions contained within this guide have also been adjusted, notable to improve the wording regarding complying with the code and other clauses
V1.2 – v2023.2	11/12/2024	ST4S Team / Education Services Australia	AI Module criteria updated as approved by the ST4S WG. Updates to the exclusion list. Minimum AI criteria now noted in the guide. Corrections to codes such as G01 vs GO1 (e.g. replacing the numeric zero with the letter 'O'). Supplier code of conduct moved to an appendix.
V1.1 – v2023.2	17/07/2024	ST4S Team / Education Services Australia	Minor updates to wording. Updates to excluded list. Corrections and adjustments to AI controls AI_PR2, AI_PA2 and AI_SF4. Clarified AI Pilot Information.
V1.0 – v2023.2	06/06/2024	ST4S Team / Education Services Australia	Interim release. Introduction of first release of AI control questions

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 Key terminology

Term	Definition
AIS	Australian Independent Schools, including their bodies and representatives across States/Territories within Australia.
Education authority	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
ESA	Education Services Australia Limited (www.esa.edu.au)
NERA	National Education Risk Assessment (name changed to ST4S Assessment)
ST4S	Safer Technologies for Schools (www.st4s.edu.au)
ST4S WG	Safer Technologies for Schools Working Group
NEDAG	National Education Digital Advisory Group (formerly known as the NSIP Steering Group)
NSIP	National Schools Interoperability Program (www.nsip.edu.au), 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.
- 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.

- ESA began piloting the ST4S AI Module in July 2024 to address services making use of artificial intelligence (AI) which was then finalised in December 2024. The initial release (v2023.2) addressed critical criteria whilst a second update under v2024.1 addressed additional criteria and improvements.
- Australian privacy laws are being modernised in two main phases (Tranches 1 and 2) to give Australians greater privacy rights and protections. Protecting young people is a core focus, highlighted by the upcoming Children's Online Privacy Code, which will be registered by December 2026.
- Australia's online safety framework is also being updated. Revisions to the Basic Online Safety Expectations (BOSE), enforceable industry codes, and social media minimum age laws set strict expectations for platforms to protect children and young adults online.

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 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.

Not all services may be assessable. For further information on what types of services may or may not be assessed, please review the ST4S Excluded / High Risk List on our website.

1.6 Start-ups and Small Businesses – Quick Notes

For many organisations, a ST4S assessment is their first external review. Our approach to the ST4S assessment is to work with you to help you achieve a compliant outcome. Upon submitting an assessment, we review and engage with you to understand your service and to provide time to remediate any items as required.

Many organisations make changes, update privacy policies and improve security to meet the criteria. We have assessed organisations of all sizes from 1-2 employees to large multinationals. We have also supported small businesses with multiple non-compliant outcomes achieve a compliant outcome.

Our recommendation is to first explore the Readiness Check on our website and upon receiving your result, get in contact with us to understand what the next best steps are and how you can meet compliance. We find after a discussion with small businesses / start-ups that they are more comfortable with the assessment process and how

they can achieve a compliant outcome. Many small businesses / start-ups find they may meet criteria already, they are on the right path or that there are small changes that when implemented can meet the criteria.

Please also ensure you read the 'Support' section of this guide for more information on how we support organisations throughout the assessment process.

We also recommend reviewing publications from OWASP for security information including the OWASP Cheat Sheet series. These publications provide key security information in an easier to read format, and cover core topics of authentication, file upload security, best practices and more.

1.7 Large Organisations and International Companies – Quick Notes

ST4S is an international initiative to establish a single assessment framework to reduce company effort in completing multiple assessments for school authorities and education departments across Australia and New Zealand. If your service is in use by schools in Australia and New Zealand, it is recommended you complete an ST4S assessment.

An ST4S assessment is similar to undertaking an ISO27001, SOC2 audit or other review. ST4S is not simply a questionnaire to complete for a customer. Documentation and evidence must be lodged. It is important to ensure your CIO is aware your company is interested in participating in the ST4S so they can support you in providing you with the documentation and evidence you require.

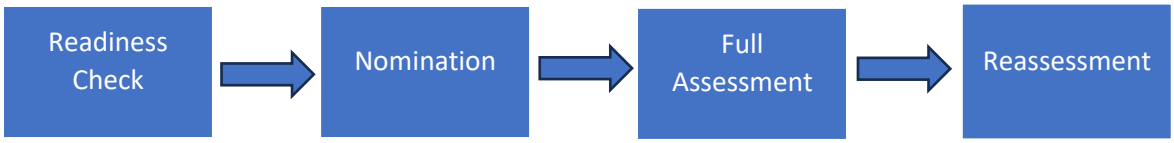
We are in the process of mapping certifications and other audit reviews to our assessment framework and will be publishing more information on this shortly. These will result in some criteria being automatically accepted, but not all. Companies with existing accreditations or audits are still required to submit a questionnaire and engage in the assessment process.

For international companies, we strongly encourage you to consider offering data residency options in Australia. Storing information offshore does not necessarily disqualify your company from a compliant outcome with ST4S however we are aware that the Department of Education in some States/Territories within Australia have required companies to store information in Australia for their schools. Further information on outcomes we make, and how the ST4S WG review our outcomes are described within this guide.

2. Assessment process

A summary of the assessment process is described below. Further information on each of the assessment stages are broken down into sub-sections.

Overview:



1. **Readiness Check:** 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 'Ready' for a Full Assessment, the supplier can optionally submit their product or service for prioritisation. If any items are noted as 'Not Ready' the supplier will need to undertake remediation and update their response. Once all items are 'Ready' the supplier can then submit.
2. **Nomination:** Products and services submitted for full assessment are verified by the ST4S Team and then prioritised by the ST4S WG once a month. We set a maximum quota each month.
    a. Services not suitable for an assessment (e.g. noted on the ST4S Exclusion List in the appendix of this guide) are not included.

b. ST4S WG members nominate services based on school demand and other factors. If a service is not nominated, it will roll over to the next month until a new framework or substantial change has been made.
c. If a service is not nominated but the quota is not filled, the ST4S Team may provide an opportunity to other assessments without any nominations. This is done in order of the submission date.

3. **Full Assessment:** Once prioritised, suppliers are invited to participate in the Full Assessment which requires the submission of the full questionnaire and documentation.
4. **Reassessment:** Required every 2 years to remain current, unless major changes are introduced to your service or a ST4S Working Group member or ESA requests a reassessment.

At any time a supplier may withdraw from the process or the ST4S Team may discontinue an assessment. Further information on withdrawing or discontinuing is 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 ST4S 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
Company and product details	C0, C1, C2, C3, C4, C5
Product information	P1, P2, P3, P4, P5, P6, P9, P10, P11, P12, P13
Hosting and location	H1, H5
Security – Technical	S1, S2, S3, S4, S5, S7, S8, S9, S10, S11, S13
Access	A1, A2, A5, A6, A7, A10, A11, A13, A16A, A16B
HR	HR1, HR2, HR3

Processes and testing	T1, T2, T3, T6, T6A*, T7
Plans and quality	Q5, Q7
Data deletion and retention	D3
Compliance controls	CC2
Privacy – Requests	PR1, PR1A, PR1B, PR1C, PR2, PR10, PR12, PR13, PR14, PR16, PR17
Privacy - Functionality	PF4, PF6*, PF7*, PF8*, PF9D*, PF10D*, PF13*, PF36*
Governance	GO1, GO2
Integrations	INT5, INT7
Safety Criteria and Safety Principles	SC3, SC5
Mobile Applications/ Browser Extensions	AP0, AP1, AP2
Artificial Intelligence	AI_G1, AI_G1A, AI_H2, AI_HR1, AI_T1, AI_T2, AI_T3, AI_T4, AI_5, AI_T6, AI_T7, AI_T8, AI_T9, AI_T10, AI_I2, AI_GO1, AI_PA2, AI_PR1, AI_PR3, AI_PR3, AI_PR4, AI_PR6, AI_PF1, AI_PF1A*, AI_PF4, AI_PF5, AI_PF8, AI_PF9, AI_SF4, AI_SF5, AI_SF6

Please note that functionality questions marked with * are presented based on previous responses.

Learn more about the ST4S Readiness Check here: 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 steps

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 a Supplier chooses not to accept a report, or we are unable to finalise a report we may discontinue the assessment.

Remediation:

The requirement to complete the Readiness Check prior to the Full Assessment ensures services are meeting the minimum standards for a compliant outcome prior to the ST4S Team beginning assessment activities. Suppliers need to ensure all remediation has been completed and the criteria has been met before successfully submitting the Readiness Check.

There are cases where an item may not be compliant in the Full Assessment either due to genuine error, we assess an outcome differently to what the supplier may have expected, or we do not accept the relevant documentation etc. In this instance, we provide a period to remediate (generally 3 months maximum) subject to review by the ST4S WG. If remediation items are substantial, or we do not believe an organisation may be able to remediate in time, we may discontinue an assessment and ask the organisation to return later when ready.

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 may also discuss compliance matters with the ST4S WG or issues relating to the assessment and how it is progressing.

Communication of updates, findings, outcomes etc to schools are a local matter and are decided by the education authority, ST4S WG member and/or NEDAG as relevant

Assessment Approach:

The ST4S assessment process requires open communication and transparency. Technologies and topics of cybersecurity, privacy and online safety can be complex and how each supplier implements technologies and features to meet ST4S criteria can differ.

Where a supplier has a different approach to meet a control (e.g. using a different technical service or solution), the supplier can provide additional information during the clarification process to support the assessment.

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.

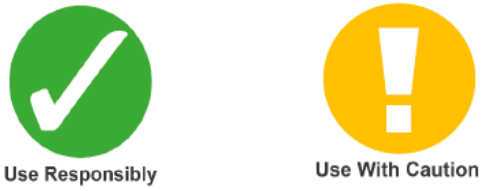
For Tier 1 and 2 services, the assessment of a product or service results in one of the following outcomes:

Low risk *Medium risk* *High risk* *Non-compliant*

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:

Use Responsibly *Use with Caution*



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.

Important: 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

Acceptance of outcomes:

Suppliers are advised 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 Alternative findings and challenging findings

ST4S criteria is designed to be worded generically, and we acknowledge that each service and supplier may implement criteria differently. The ST4S Team reviews how criteria may apply in different circumstances, such as where you may be using a different tool to combat cybersecurity risks, or you have implemented other measures to protect the privacy of your users. The ST4S Team maintains an internal register of previous decisions to ensure we apply findings and decisions fairly.

Common examples include:

- Certain cybersecurity vulnerability scanner tools that we have accepted previously;
- AI foundational models and inference providers, and the types of tools that may be used by these providers to satisfy or partially satisfy safety criteria;
- Password requirements for Students and young people including shorter passwords, providing an alternative access mechanism (email link, OTP code, passkey etc), room codes for games and collaborative learning activities;
- Services provided by Cloud Service Providers and built-in tools for threat detection;
- Server-less architectures and how security and technical criteria may best apply;
- Human Resources (HR) and corporate governance (GO) requirements (e,g. appointing a CIO and Privacy Officer role) and how these apply to small businesses and sole traders;
- Classification of what is appropriate content (e.g. text, images, videos etc) to display in education contexts, to younger audiences and other users. We generally refer to the Australian Media Classification Guidelines and the New Zealand equivalent for these cases.

Alternative findings are not guaranteed and are made in consultation with members of the ST4S Working Group. Our recommendation to suppliers is throughout the assessment process is to provide as much technical information as possible to help us in our review. This allows your assessment officer to properly review and search through decisions and come to a fair conclusion.

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 with a sufficient amount of information including technical information to assist the team in its review. Where applicable, we recommend providing technical information on the products you use on the cloud service provider and configuration settings you may have applied to help our technical team members review.

Any challenge to a finding or outcome is first reviewed by the ST4S Team and presented to the ST4S WG if necessary. Should a matter be referred to the ST4S WG, a decision by a ST4S WG member, the ST4S WG and/or NEDAG is final.

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. Simply disagreeing with a criterion or claiming you should not be required to meet the criteria without genuine explanation or information is insufficient for a challenge to occur.

In almost all cases, the ST4S Team and the immediate assessment officer is able to resolve matters with suppliers without the need to engage with the ST4S WG.

2.2.6 Re-assessment

Assessments are valid for 2 years unless withdrawn beforehand.

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.

A reassessment will generally always be necessary in the following circumstances:

- The organisation that owns the service changes for example by sale, license transfer or similar.
- Features or functionality changes (either new or a modification and/or removal) which results in the new categories being relevant to the assessment.
- Changes in data types where many new data types are added, removed. Changes to any data types that are classed by the ST4S as sensitive or protected.
- A change in hosting location or infrastructure (e.g. you migrate regions of infrastructure from within the same cloud service provider or you migrate one or more components from one cloud service provider to another).
- Changes to the privacy policy that warrant a new assessment such as the introduction or change to advertising, usage of data for advertising (including where de-identified)
- Adding or removing features/functionality related to artificial intelligence or changes in how your organisation or any other organisation may use data on the service (including where deidentified) for training or development of AI models.

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 is not ready for an assessment due to incomplete documentation, lack of pen test or other critical items.
- The service being assessed is not suitable for an assessment or the ST4S Team postpones an assessment to a newer framework. We may communicate an outcome of 'postponed' to the ST4S WG along with a note on when we expect an assessment to begin.
- Where an excessive number of non-compliant outcomes are identified in the Full Assessment, and we reasonably believe you may have misrepresented (whether intentionally or not) your service's level of compliance in the Readiness Check and we do not believe you can remediate the items during a 3 month period.
- Whilst genuine errors can occur, if we reasonably believe a supplier is not being transparent, omitting important information or is misleading the ST4S Team throughout the assessment process.
- 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. Examples include where a ST4S WG is engaging with the Privacy Commissioner in their jurisdiction, a ST4S WG is requesting advice or engaging with legal counsel, or another government agency or department has requested to review the report.

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. Assessments may not cover all features, functionalities, or configurations. Any applicable scope limitations, exclusions, or conditions are specified in the assessment report
9. Suppliers should ensure that all communications regarding an ST4S assessment appropriately reflect any applicable limitations, exclusions, or conditions identified in the assessment.

10. 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).
11. 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.
12. Suppliers must not publish in whole or in part the ST4S assessment results for another supplier's service.
13. Suppliers must notify the ST4S Assessment Team if they come into possession of some or all of another supplier's ST4S report or results.
14. If a supplier does not comply with the above usage conditions, the ST4S Assessment Team may rescind/withdraw/modify that supplier's assessment outcome.
15. 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) for the latest usage conditions

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

- Government Schools:
  - NSW cybercompliance@det.nsw.edu.au
  - QLD riskreviews@qed.qld.gov.au
  - SA education.ictcybersecurity@sa.gov.au
  - TAS security@education.tas.gov.au
  - NT Digitalanddata.doe@education.nt.gov.au
  - WA privacy@education.wa.edu.au
  - VIC security.assessments@education.vic.gov.au
  - ACT 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.

Suppliers should direct New Zealand school enquiries to: 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

Our goal of ST4S is to help suppliers obtain a compliant outcome at the end of the assessment process. The majority of organisations (including start-ups and small businesses) that choose to participate in ST4S are able to work with us on making improvements, clarifying items and achieve a compliant outcome at the end of the assessment.

The ST4S Team supports suppliers to achieve a compliant outcome by:

1. Responding to an enquiry you have on the criteria. Just reach out on the contact form on our website.
2. Providing time to remediate for items you have genuinely missed or where we may have a differing assessment outcome.
3. Clarifying responses with you and allowing additional information to be submitted throughout the process, particularly where you may implement a differing approach to meet a control.
4. Providing you with support materials and general guidance on how to meet compliance.
5. Meeting with you (phone, video chat etc) to discuss the criteria or your concerns.

Additional Support:

If you require additional support such as extended discussions with development teams on technical matters, additional reviews on documentation etc, we can provide this subject to availability of our team. We generally prioritise organisations who need our support the most such as small businesses or start-ups that may not have access to a cybersecurity engineer or privacy expert, not for profits or charities, organisations delivering services which process highly sensitive information (e.g. mental health data), and services which address high priority initiatives as determined by the Australian or New Zealand curriculum or government

5. Terms and Conditions

A Supplier electing to participate in the ST4S assessment process, the ST4S Product Badge programme, or any other related ST4S activity shall agree to and abide by the applicable terms and conditions.

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 or participate in the ST4S assessment process

- 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.
- The ST4S assessment process encompasses the entire solution, including services, applications, and other components that form the overall solution. If an application processes information but does not store it or communicate the information back to the organisation, it may still be within scope. This aligns with the principles of privacy by design, where organisations should embed privacy throughout the development of the application and its ongoing activities. Additionally, cybersecurity and online safety best practices apply to mobile applications and extensions, even when not operating in a connected environment. This ensures data

safeguarding and protects organisations from other attacks that may result in compromised deployments and other attack vectors.

- You will be required to provide evidence at a later date to support your responses. Evidence is closely inspected and reviewed to ensure organisations are meeting the criteria within the ST4S framework.
- 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, various Government information security classification frameworks and best practices in the industry across key principles of security by design, safety by design and privacy by design. Supplier responses will assist in the assessment, mitigation and monitoring of the risks associated with their product/service. Supplier responses will assist in the assessment, mitigation and monitoring of the risks associated with their product/service.
- Any individual completing the ST4S Readiness Check, the ST4S Full Assessment, or any other related ST4S activities on behalf of the Supplier must:
  - Be duly authorised by the Supplier's organisation to do so, and
  - Hold express written permission from the Chief Executive Officer (CEO), Chief Information Officer (CIO), or another senior officer of the Supplier with comparable authority for making executive decisions and directing the company's overall strategy.
- Similar to other assessments (including, but not limited to, ISO 27001, ISO 27701, and SOC 2), the ST4S framework sets a high standard that Suppliers may elect to meet. Suppliers who begin the ST4S assessment process but subsequently determine that they are unable or unwilling to remediate in order to meet the criteria, or who fundamentally disagree with the criteria or the high standard expected under the framework, shall promptly withdraw from the ST4S assessment process. Suppliers wishing to meet the criteria are encouraged to discuss any concerns with the ST4S Team and may collaborate on a remediation plan in order to achieve compliance.
- Suppliers shall provide all necessary information to support the ST4S assessment process, which may include documentation, evidence, and/or access to a trial or demonstration account.

- An assessment officer from the ST4S Team will be assigned to work with each Supplier throughout the ST4S assessment process. The Supplier shall comply with all instructions and requests made by the assigned assessment officer in relation to completing the ST4S assessment. Should the assessment officer require referral of any enquiry or matter to another department or individual within the Supplier's organisation, the Supplier shall promptly effect such referral.
- A Supplier Code of Conduct ('the Code') is included as an appendix to this guide. Compliance with and adherence to the Code is a condition of undertaking any assessments or related activities with NSIP concerning the ST4S initiative. Suppliers found to be in breach of the Code may be removed from the assessment process, have their assessment discontinued, or be subject to any other action NSIP deems appropriate. Determinations of whether a Supplier is in breach of the Code shall be made at the sole discretion of the ST4S Team. The Code may be updated periodically, and the most recent version will be published in this guide. Suppliers are responsible for remaining up to date with any changes to the Code. The ST4S Team may note a Supplier's engagement and conduct during the ST4S assessment process, or related activities, to the ST4S Working Group.
- It is a condition of participation that any correspondence provided by a Supplier to NSIP and/or the ST4S Team may be referred or made available to the ST4S Working Group and/or any member thereof for review. This includes correspondence from third-party organisations or individuals acting on behalf of the Supplier, or under the Supplier's instruction.
- Any challenges, disagreements, or disputes relating to the ST4S criteria or the assessment process shall initially be addressed by the ST4S Team. If further escalation is required, matters shall be referred to the ST4S Working Group ('ST4S WG') and/or NEDAG, in accordance with the escalation procedures outlined in the Supplier Code of Conduct. Suppliers shall at all times comply with this escalation process.

5.2 Completing 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. Please review '4.0 Support' of this guide for more information.

5.2.1 Completing the Artificial Intelligence (AI) Module

The ST4S assessment was expanded in second half of 2024 to include a new module on AI which addresses key concerns in the education sector, from the ST4S WG and incorporates emerging best practices and guidance from industry and the principles published by the Australian Ministerial Framework for AI in Education.

ST4S is not assessing all use cases of AI at this time, and some higher risk use cases or items which we do not yet have controls for are excluded. Review the 'ST4S Exclusion and High Risk list' on our website for more information. The AI Module in its first release focusses on establishing a foundation to further build compliance upon as AI technologies advance and new standards and guidance from industry is published.

The AI Module makes a distinction between whether a supplier is utilising a foundational model service (e.g. OpenAI GPT, Claude etc) vs an opensource model with further data sets, modification or training etc. The AI Module is anticipated to be updated rapidly as best practices an industry guidance is published.

AI is a complex topic and Suppliers are encouraged to make an attempt at the AI Module, provide additional information throughout the module to support the assessment process and the ST4S Team will be providing opportunities to remediate and further discuss criteria and how it best applies to Suppliers undertaking the AI Module. Suppliers with concerns on how to meet compliance are encouraged to contact the ST4S Team on our website or directly to further discuss

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

A supplier code of conduct applies to all suppliers. Agreeing to the conditions within this guide and the supplier code of conduct is a requirement of the assessment process. View Appendix G for the supplier code of conduct

5.7 Supplier communication requirements

Suppliers should be aware that the ST4S Team communicates regularly with ST4S Working Group members including staff at a State/Territory Department of Education, New Zealand Ministry of Education etc. We also monitor supplier communications including updates you may post to your website, your usage of the ST4S Product Badge (if you have been licensed to do so), changes to your privacy policy / terms of use etc.

What you must not do:

- Publish you are engaged in the ST4S assessment process or suggest/imply you are conforming to ST4S standards and criteria when you have only completed the Readiness Check and have not successfully completed a recent full assessment for the service which remains valid.

- Use ST4S, NSIP or ESA brand, logos, colour schemes and other materials in any communications or content related to the ST4S assessment or program. The only branding material currently is the ST4S Product Badge if your organisation has a licensing agreement with us.
- Produce your own ST4S like badge, images or content such that use our brand. Examples include using the words “ST4S Assessed” next to a shield icon which closely resembles the ST4S Product Badge, using the words “ST4S Certified” with a tick icon or image.
- Engage in misleading or deceptive conduct when communicating with a school, a government agency (e.g. a State/Territory Department of Education body, or the Ministry of Education in New Zealand) or another ST4S Working Group member as to the status of your assessment.

You are welcome to ask us to review any publications, media statements or drafts before you publish. Subject to availability of our team, we are happy to review material to ensure the usage of the ST4S product badge is compliant with the usage guidelines and that any other information you publish aligns with our expectations.

5.8 Compliance with the Terms and Conditions

The ST4S Team reserves the right to remove a Supplier from the ST4S assessment process, discontinue an assessment, or revise any outcome or decision in the event that any condition set forth above (or elsewhere in this guide or within section 5 of this guide) is breached, or if a Supplier fails to comply with the ST4S Supplier Code of Conduct.

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.

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.

Minimum criteria

Questions marked with a hash (#), can lead to a “Non-compliant” assessment outcome if the minimum preferred response/s are not met. The minimum criteria for each Tier is displayed Below. The AI Module has no Tier differentiation (e.g. a Tier 2 service with AI features/functions will be required to meet the AI Module minimum criteria noted below in the same way as a Tier 1 service would). Some items marked with a hash (#) and listed below are not necessarily critical criteria resulting in a non-compliant outcome, but also those which may result in a high risk outcome.

Tier 1: 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, T6A, T7, Q5, Q7, D3, CC2, PR1, PR1B, PR1C, PR2, PR10, PR12, PR13, PR14, PR16, PR17, PF6, PF7, PF8, PF9D, PF10D, PF36, G01, G02, INT7.

Tier 2: H5, S1, S2, S3, S4, S5, S7, S8, S10, S11, S13, A1, A2, A13, A16b, HR3, T1, T6, T6A, T7, Q5, D3, CC2, PR1, PR1B, PR1C PR2, PR17, PR10, PR12, PR13, PR14, PF6, PF7, PF8, PF9D, PF10D, PF36, G01, G02, INT7.

AI Module: AI_G1, AI_G1A, AI_H2, AI_HR1, AI_T1, AI_T2, AI_T3, AI_T4, AI_T5, AI_T6, AI_T7, AI_T8, AI_T9, AI_T10, AI_I2, AI_GO1, AI_PA2, AI_PR1, AI_PR2, AI_PR3, AI_PR4, AI_PR6, AI_PF1, AI_PF1A, AI_PF4, AI_PF5, AI_PF8, AI_SF4, AI_SF5, AI_SF6, AI_SF6A

6.1 Criteria – Company & product detail

#	Question	Tier	Notes
C0	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
C1	Vendor name	1 & 2	Informational
C2A	Vendor ABN	1 & 2	Informational (AU submissions)
C2B	Vendor NZBN	1 & 2	Informational (NZ submissions)
C3A	Registered Australian address of vendor	1 & 2	Informational (AU submissions)
C3B	Registered New Zealand address of vendor	1 & 2	Informational (NZ submissions)
C4A	Country in which the company is registered for Australian customers	1 & 2	Informational (AU submissions)
C4B	Country in which the company is registered for New Zealand customers	1 & 2	Informational (NZ submissions)
C5A	For Australian customers: Preferred vendor contact name Preferred vendor contact email Preferred vendor contact phone number	1 & 2	Informational (AU submissions)
C5B	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 *If no published version number, use date of version.*	All		
P2B	Is the service free or paid?	All	A. Free B. Paid	
P2C	For paid services, provide a URL to your pricing page or explain how pricing is determined.	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	URLs for Australian customers	All		
P3B	URLs 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. Yes - current policy with coverage of at least $1 million AUD (T1)** B. Yes - current policy but coverage is less than $1 million AUD C. No current policy	
P8	Are there any additional setup steps or requirements that your service needs to function for its intended purpose, including: • Requiring users to register or access another service in addition to yours (e.g. users must also be able to access YouTube for video content); • Unblocking additional domain names or IP addresses; • Adjusting DNS settings (e.g. adding a CNAME record etc); • Installing or deploying middleware (e.g. hybrid hosted setups); • Requiring specific hardware such as Internet of Things (IoT) devices, wearable devices etc; • Firewall or network changes	All	A. Yes, please specify B. No	NZISM 12.7

P9	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. ***Sensitive information*** *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:* *- Protection details (i.e., whether the user is under a protection order and/or the details of the order)* *- Legal custodian arrangements and court orders* *- Out of home care status* *- Records of behaviour incidents/discipline, behavioural observations/notes* *- Consent (e.g., collection and/or recording of consent)* *- Student absence details (i.e., records of attendance and reason for absence)* *- Records of contact (e.g., between parents, teacher, school, and/or student) and other agencies* *- Student/Learning support service information and support arrangements* *- Enrolment support records (sensitive case, complex case, adjustments, student plan, developmental map, transportation, Individual Education Plans, Oranga Tamariki 'All about Me' plan)*	All	•Protection order details (student) •Legal custodial arrangements (student) •Informal custodial arrangements •Legal status (criminal convictions, protection orders, police checks results etc) •Out of home care status (student) •Records of behaviour incidents (student) •Records of incidents •Behavioural observations/notes (student) •Records of contact or interview (student) •Sensitive social, emotional or mental health and well-being information (staff, student, parent) •Support arrangements (student) •Professional case notes (student) •Reason for absence (student) •Commonwealth Unique Student Identifier (AU) or National Student Number (NZ) •Health and medical details, including mental health diagnoses (staff, student, parent) •Personal health or fitness information (e.g. step counts, heart rate, calories burned, sleep duration / patterns, other fitness or physical activity metrics) (student, staff, parent) •Wellbeing information (e.g. mood check-ins, self-reflections, wellbeing journals etc) (student, staff, parent) •Financial information (staff, student, parent, organisation) •Identification documentation (staff, student, parent) •Digital signature (staff, student, parent) •Government related Identifiers (e.g., state or federal government assigned identifiers) •Official records •Racial or ethnic origin	NZ PSR – INFOSEC1

			•Religious beliefs or affiliations •Sexual orientation or practices •Biometric information (e.g., eye/retinal/facial imagery, fingerprints, biometric templates) •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) • Use of social services (Work & Income, ACC, CYPS, Women's refuge etc) • None of the above (T2)	
P10	Select the functionality available within the service. Select all that apply.	All	• Online meetings, video or audio conferencing, livestreaming (T1) • Consent Management (T1) • Financial management or payment processing systems (T1) • Enrolment management (T1) • Student information, student management system, school administration or student administration system (T1) • Customer relationship management (T1) • Ticketing system - Service Management, Helpdesk (T1) • Learning management system (T1) • Electronic document and records management systems (T1) • File hosting and synchronisation (T1) • Remote access (T1) • Data collection tools (non-curriculum) (T1) • Photo, image, video or audio storage, sharing and backup services (T1) • Two-way communication tools (T1)	

			• Data aggregation, Data broker, Data hub, Data distribution hub (T1) • Data aggregation, analytics, insights and reporting (T1) • Software and cloud developer tools (T1) • Mobile device management (MDM) (T1) • Authentication services (T1) • Collaboration and sharing (T2) • One-way communication tools (T2) • Career education, planning and guidance (T2) • Vocational training providers and courses, industry/employment registers, work placements (T2) • Learning activities, assessments and games (T2) • Content creation, presentation tools and publishing (T2) • Educational resources and content libraries (T2) • File download, including executables (T2) • Library Management (T2) • Visitor Management (T2) • Event management, bookings, online ordering or fundraising (T2) • Administrative support services and tools (T2) • None of the above (T2)	
P11	Does the service promote or display any of the following (e.g. via social media, ads, pop-ups): • Restricted products: alcohol, banned substances, gambling, tobacco, firearms, adult content. • Offensive content: e.g. racist, sexist, or pornographic material.	All	A. Yes (please specify) **B. No (T1,T2)**	
P12	With respect to any third-party providers that compose your solution or deliver services to your organization, does your organisation perform all of the following:	1	A. No B. Yes - for some third-party providers **C. Yes - for all third party-providers (T1)**	NZ PSR - GOV5 NZISM 12.7 NZPP-5 NZPP-11

	• Maintain an up-to-date inventory of all third-party service providers • Regularly assess and manage the risks associated with these providers • Have contractual agreements in place to ensure that third-party providers comply with your information security and privacy policies?		**D. NA - solution does not use third party providers (T1)**	
P13	How is the service deployed for customers?	All	A. Customer-hosted (self-managed environment) B. Supplier-hosted (e.g. cloud or managed service by your organisation) C. Hybrid – part hosted by customer, part by your organisation	
P14	Does the service meet the Web Content Accessibility Guidelines (WCAG) to ensure that digital content is accessible to people with disabilities? Specify the WCAG version and level	All	A. Not WCAG compliant B. Yes – all components meet WCAG 2.0 C. Yes – all components meet minimum of WCAG 2.1 D. Yes – all components meet minimum WCAG 2.2	NZ Govt Web Standards
P15	Retired (2025)			

6.2.2 Security – Hosting and Location

Q	Question	Tier	Response options	Standard / References
H0	Select from the following cloud service providers which are used by your service:		A. Amazon Web Services (AWS) B. Google Cloud (GCP) C. Microsoft Azure D. Digital Ocean E. Other cloud service provider (please specify) F. Other infrastructure provider (please specify) G. N/A - No third party infrastructure or cloud service providers used	
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,	1 & 2	**A. Entirely in a country nominated by the customer (specify supported countries for Australian and New Zealand customers) (T1, T2)**	AUISM Security Control: 1452 Revision 3 NZISM 22.1.22 NZISM 12.7

	including live solution, backup, disaster recovery, test environment, and development environments.		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)	NZPP-11
H2	From what countries do vendor staff, including support, administration, development and testing, and external contractors or associates, access or view user data and any related data (e.g., metadata, logs) collected or used by the service (including backups and recovery)?	1 & 2	**A. Entirely from Australia and / or New Zealand (please specify)** B. From other countries (please specify country/s)	AUISM Security Control: 0420 Revision 12 AUISM Security Control: 0409 Revision 8 NZISM 22.1.22 NZISM 12.7
H3	Retired (2022)			
H4	At a minimum, which of the following physical access controls are in place at data storage locations? Select all that apply.	1	A. No public access B. Only visitors with need to know permitted and have a close escort at all times C. Restrict access to authorised personnel with appropriate security clearance D. Access control using secure swipe card, biometrics, coded access, or similar E. Monitored security alarm system	AUISM Security Control: 1296 NZISM 8
H5#	Would customers be notified in advance if the cloud infrastructure, data-hosting environment, organisational staff, or any personnel with access to unencrypted customer data were to be relocated or expanded into another country?	1 & 2	A. No (#T1, #T2) **B. Yes (specify average notification lead time) (T1, T2)**	AUISM Security Control: 1572 Revision 3 NZISM 22.1.22 NZISM 12.7
H6	Are all infrastructure providers, cloud-based services and other service components assessed under either of the following: • IRAP • SOC2 Type 2 • ISO27001 See https://www.cyber.gov.au/irap for information about IRAP assessment.	1 & 2	A. No or unknown **B.** Yes – some hosting providers, cloud-based services and other components are IRAP, ISO27001, or SOC2 Type 2 assessed **C. Yes – all cloud-based services and other components are IRAP, ISO 27001 or SOC2 Type 2 assessed (T1, T2)**	AUISM Security Control: 1570 Revision 0

6.2.3 Security – Technical

Q	Question	Tier	Response options	Standard / References
S1#	What are the minimum encryption algorithms applied to protect all data **in transit** 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. Weak Encryption: DES, RC4, 3DES using three distinct keys; Hashing: Message Digest (MD to MD6), RIPEMD-128 or above, SHA-0, SHA-1; Digital Signatures: RSA (2048); Key Exchange: DH (1024) or RSA (2048); Protocol: TLS1.1 or below C. Standard Encryption: AES 128 or above; Hashing: SHA-224 or above; Digital Signatures: FIPS 186-5, ECDSA (224+) preferably using NIST P-384 curve or RSA (2048+); Key Exchange: DH (2048+), ECDH (256+) preferably using NIST P-384 curve or RSA (2048+); Protocol: TLS1.2. (T2) **D. Strong Encryption: AES 192 GCM/CCM, CHACHA20 POLY1305 or above only (AES 256 GCM/CCM recommended)** **Hashing: SHA-256 or above only (SHA-384 recommended)** **Digital Signatures: FIPS 186-5 ECDSA (224+) using NIST P-384 curve or RSA (2048+);** **Key Exchange: DH (3072+), ECDH (256+) using NIST P-384 curve or RSA (3072+)** **Protocol: TLS 1.3 (TLS 1.2 for compatibility). (T1, T2)**	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
S2#	What are the minimum encryption algorithms applied to protect data at rest, including backups, data storage, removable media and auditable logs?	1 & 2	A. No encryption (#T1, #T2) B. DES, RC4, 3DES using three distinct keys **C. AES 128 (T2)** **D. AES 192, AES 256 (AES 256 recommended) (T1)** E. Encryption algorithm equivalent to options C or D (please specify equivalent algorithms)	AUISM Security Control: 0459, revision 3 AU ISM Security Control: 0869 NZISM 21.1 .13 NZISM 17.2

S3#	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	A. No encryption (#T1, #T2) B. Weak Encryption: DES, RC4, 3DES using three distinct keys; Hashing: Message Digest (MD to MD6), RIPEMD-128 or above, SHA-0, SHA-1; Digital Signatures: RSA (2048); Key Exchange: DH (1024) or RSA (2048); Protocol: TLS1.1 or below C. Standard Encryption: AES 128 or above; Hashing: SHA-224 or above; Digital Signatures: FIPS 186-5, ECDSA (224+) preferably using NIST P-384 curve or RSA (2048+); Key Exchange: DH (2048+), ECDH (256+) preferably using NIST P-384 curve or RSA (2048+); Protocol: TLS1.2. (T2) **D. Strong Encryption: AES 192 GCM/CCM, CHACHA20 POLY1305 or above only (AES 256 GCM/CCM recommended)** **Hashing: SHA-256 or above only (SHA-384 recommended)** **Digital Signatures: FIPS 186-5 ECDSA (224+) using NIST P-384 curve or RSA (2048+);** **Key Exchange: DH (3072+), ECDH (256+) using NIST P-384 curve or RSA (3072+)** **Protocol: TLS 1.3 (TLS 1.2 for compatibility). (T1, T2)** E. N/A - Customer data is not uploaded to the service	AUISM Security Control: 1139, revision 5; AUISM Security Control: 0471, revision 6; AUISM Security Control: 0472, revision 6; AUSIM Security Control 1759, revision 0; AUSIM Security Control 0474, revision 6; AUSIM Security Control 1761, revision 0; NZISM 17.2 NZISM 17.3
S4#	If the system uses multi-tenancy architecture (where system components are shared across multiple customers), which of the following controls are implemented to ensure secure segregation of each customer's data? Select all that apply:	1 & 2	A. Unique customer identifiers when a shared table stores data for multiple customers B. Separate tables or databases for each customer C. Dedicated instances, environments, or VPCs D. All of the above E. None of the above (#T1, #T2)	AUISM Security Control: 1436, revision 1 NZISM 10.8 NZISM 22.2

			F. Not applicable, multi-tenancy is not used	
S5#	Are all of the service's web servers secured with digital certificates signed by a reputable trusted authority?	1 & 2	**A. Yes (please specify CA) (T1, T2)** B. No (#T1, #T2)	AUISM Security Control: 0465 AUISM Security Control: 0457 AUISM Security Control: 1273 NZISM 17.1 NZISM 17.2
S6	Does your organisation have a documented and implemented certificate and key management process which describes at a minimum: • Key generation; • Key registration; • Key storage; • Key distribution and installation; • Key use; • Key rotation; • Key backup; • Key recovery; • Key revocation; • Key suspension; and • Key destruction?	1	A. No - none of the above B. Yes - some of the above **C. Yes - all of the above (T1)**	NZISM 17.9
S7#	Which of the following protections are in place for your production environments (production servers, containers, serverless services and endpoints)? Select all that apply.	1 & 2	A. Intrusion detection systems (IDS), Host-based intrusion detection (HIPS) B. Software-based application or web application firewall (WAF) (T2) C. Anti-virus and malware detection **D. All of the above (T1)** E. None of the above (#T1, #T2)	AUISM Security Controls: 1341, 1034, 1416, 1417 NZISM 14.1 NZISM 18.4
S8#	Does your organisation enforce the following controls on database management system (DBMS) software: • Follow vendor guidance for securing the database;	1 & 2	A. No - none of the above (#T1, #T2) B. Yes - some of the above **C. Yes - all of the above (T1, T2)**	AUISM Security Controls: 1246, 1247, 1249, 1250, 1260, 0414, 1263, 1273 NZISM 21.4 NZISM 14.1

	• DBMS software features and stored procedures, accounts and databases that are not required are disabled or removed; • Least privileges; • File-based access controls; • Disable anonymous and default database administrator account; • Unique username and password for each database administrator account; • Use database administrator accounts for administrative tasks only; and • Segregate production from any non-production environments?			NZISM 10.8
S9#	Are internet facing components (e.g., web servers) separated from other online components (e.g. databases) using the following controls: • Secure communication between network segments (e.g., using firewalls), including filtering between network segments • DMZ for internet-facing components and separate trusted zones for other components • Virtual (e.g., VLAN) or physical network segregation	1 & 2	A. No – none of the above (#T1) B. Partial – secure communication or DMZ C. Partial – virtual or physical network segregation (T2) **D. Yes – all of the above (T1, T2)**	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
S10#	Does your organisation maintain a documented and implemented system hardening standard, that applies to all infrastructure and endpoint components (e.g., OS, hypervisors, storage, network, applications, and user devices), that: • incorporates vendor and industry best practice, • enforces the removal of default credentials and unnecessary services, • restricts non-essential ports/protocols • includes regular audit of configurations • and is reviewed at least annually or upon significant change?	1 & 2	A. No – none of the above (#T1, #T2) B. Yes – some of the above C. Yes – all of the above except annual review (T2) **D. Yes – all of the above (T1)**	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

S11#	Has your organisation implemented the following perimeter controls: • External Firewall; • IDS/IPS (Intrusion Detection System/Intrusion Prevention System); • DMZ (Demilitarised Zone) for hosting external sites; • Content filtering (including blocking of unnecessary file types); • DoS/DDoS (Denial of Service/Distributed Denial of Service) defence; • Web Application Firewall (WAF); • Filtering and monitoring of outgoing traffic (spikes, unusual activity, malicious content); • Network segmentation; • VPN required for remote access; • Detection and monitoring of unauthorised devices on the network; • DNS filtering and network URL based filters; and • Organisation assets are configured to use trusted DNS servers?	1 & 2	A. No - none of the above (#T1, #T2) B. Yes - some of the above **C. Yes - all of the above except for Web Application Firewall (WAF) (T2)** **D. Yes - all of the above (T1)**	AUISM Security Control: 1528 Revision: 1; Security Control: 1431; Revision: 5; Security Control: 0637, Revision: 6 NZISM 10.8 NZISM 18.4 NZISM 19.1 NZISM 19.3
S12	Has your organisation documented and implemented a security policy for managing mobile devices, including the use of a Mobile Device Management (MDM) solution on all mobile devices? Please select the option that best reflects your current practices:	1 & 2	A. No – Neither a policy nor MDM has been implemented. (T2) B. Partially – A policy is in place, but MDM is not applied to all devices. (T2) **C. Yes – A policy is in place and MDM is applied to all mobile devices. (T1)**	NZISM 21.1 NZISM 21.4
S13#	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) **C. No (T1, T2)**	AUISM Security Control: 1420 Revision: 2. NZISM 14.4 NZISM 20.1

S14	Does your organisation: • 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; • block macros in files originating from the internet; • enable macro antivirus scanning; and • ensure macro security settings can't be changed by users?	1 & 2	A. No B. Yes – some of the above **C. Yes – all of the above (T1, T2)** **D. N/A (T1, T2)**	AUISM Security Controls: 1487, 1488, 1489 NZISM 20.3

6.2.4 Security – Logging

Q	Question	Tier	Response options	Standard / References
L1	Does your organisation enforce a documented logging policy requiring all systems (e.g., servers, storage, network, applications) to capture: • successful and unsuccessful authentication attempts including multi-factor, • privileged activity, • user administration, • and system events, • information about each event per the ISM-1683 logging requirements, • with logs synchronised to a unified time source and protected against unauthorised access or tampering? ISM-1683 logging requirement: • the date and time of the event, • the relevant user or process, • the relevant filename, • the event description, • and the information technology equipment involved are captured.	1 & 2	A. No - none of the above B. Yes - some of the above (T2) **C. Yes - all of the above (T1)**	AUISM Security Controls: 1683, 0585, 0582, 1536, 1537 NZISM 16.6

L2	Does your organisation have a documented and implemented event log auditing procedure which outlines, at a minimum: • Schedule of audits (annual or real-time for sensitive data); • Definitions of security violations; • Actions to be taken when violations are detected; and • Reporting requirements?	1 & 2	A. No B. Yes - all of the above without real-time monitoring (T2) **C. Yes - all of the above with real-time monitoring (T1)**	AUISM Security Control: 0109 NZISM 7.1.7 NZISM 16.6
L3	Will you supply all relevant audit and logging data in response to customer requests?	1 & 2	A. No **B. Yes (T1, T2)**	
L4	Has your organisation implemented a centralised logging facility to store logs?	1	A. No **B. Yes (T1)**	AUISM Security Control: 1405 NZISM 16.6 NZISM 18.4.12

6.2.5 Security – Access

Q	Question	Tier	Response options	Standard / References
A0	What authentication methods are available for end users, select all that apply:	1 & 2	A. Username/email address and password B. Passkeys / WebAuthn (e.g. FIDO2-compliant hardware or platform authenticators) C. Magic link (one-time login link sent via email) D. One-time password (OTP) via SMS or email E. Time-based one-time password (TOTP) apps (e.g. Google Authenticator) F. Hardware token (e.g. YubiKey, RSA SecurID) G. Single Sign-On (SSO) via SAML, OAuth2 / OIDC, etc. H. Biometrics (please specify) I. Other (please specify)	
A1#	Are all users of the service (e.g. Teachers, Parents, Students, Admins etc) required to be uniquely	1 & 2	A. No	AUISM Security Control: 0414

	authenticated and identifiable within the service (e.g. each user is assigned a username and login credential)?		**B. Yes for all users – excluding students (Please detail why this exception is required and specify any controls in place for students) (T1, T2)** **C. Yes for all users (T1, T2)**	NZISM 16.1
A2#	Are all passwords used to access the service protected in line with the following: • Passwords are hashed using a strong, salted, one-way algorithm (e.g., Argon2id, bcrypt, scrypt, PBKDF2) following OWASP recommendations; • Support for long passphrases (≥64 characters), Unicode characters, and a minimum length aligned with relevant standards (e.g., ≥14 under ISM or shorter with MFA); • New passwords are checked against lists of weak, common, or breached passwords; • Authentication attempts are throttled (e.g., rate-limiting/backoff).	1 & 2	A. No (#T1, #T2) B. Yes - for all user accounts, with exceptions for student accounts (please describe). **C. Yes for all users (T1, T2)**	AUISM Security Control: 0421, 1559 NZISM 16.1 NZISM 16.1.41
A3	Do all supplier staff, external contractors, or associates with access to the organisation's systems and the service meet the following minimum password requirements? • Single-factor authentication: Minimum 15-character password with complexity controls to prevent predictability • Multi-factor authentication (MFA): Minimum 8-character password	1 & 2	A. No **B. Yes (T1, T2)**	AUISM Security Control: 0421, 1559 NZISM 16.1
A4#	Within the service, do you offer multi-factor authentication for end-users including school staff, parents and students?	1	A. No (#T1) B. Yes, MFA is offered for all account types (T2) **C. Yes, MFA is mandated for all non-student accounts (T1)** **D. Yes, MFA is mandated for all account types (T1)**	AUISM Security Control: 0974 NZISM 16.1 NZISM 16.7
A5#	Does your organisation **mandate** two factor authentication for:	1 & 2	A. No – none of the above (#T1) B. Yes – some of the above (please specify which accounts)	AUISM Security Control: 1173 Revision 3 NZISM 16.4

	• Vendor staff, external contractors or associates accessing systems remotely; • System administrators; • Support staff; and • Staff with privileged accounts?		**C. Yes – all of the above (T1, T2)**	NZISM 16.7 NZISM 19.1.20 MCSS MFA Level 2
A6#	Does your organisation implement documented role-based access control (RBAC) for all systems, requiring formal approval of roles, identification of systems and roles that must follow least-privilege principles, and prohibit the use of privileged accounts for non-administrative activities?	1 & 2	A. No (#T1) B. Yes, for some systems **C. Yes, for all systems (T1, T2)**	NZISM 16.2 NZISM 16.4
A7#	At a minimum, are vendor staff, external contractors or associates with access to systems, applications and information (including audit logs): • Validated and approved by appropriate personnel; • Periodically reviewed (at least annually) and revalidated or revoked; and • Reviewed and revalidated or revoked following changes to role, employment and/or inactivity?	1 & 2	A. No (#T1) **B. Yes (T1, T2)**	AUISM Security Controls: 0405, 0430, 1404 NZISM 16.3 NZISM 16.5
A8	Do supplier personnel (including contractors) have remote or terminal access to customer/school ICT infrastructure such as devices, servers, networks, or systems?	1 & 2	A. Yes (please specify) **B. No (T1, T2)**	
A9	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, and are dedicated privileged accounts used for duties requiring privileged access?	1 & 2	A. No B. Yes, non-privileged accounts are restricted C. Yes, non-privileged accounts are restricted and dedicated privileged accounts are used (T1,T2)	AUISM Security Control: 0863, 1688 NZISM 14.1 MCSS level 2
A10#	Are all internal organisation systems configured with a session or screen lock that: • activates after a maximum of 15 minutes of user inactivity or if manually activated by the user; • completely conceals all information on the screen;	1 & 2	A. No (#T1) B. Yes, some of the above **C. Yes, all of the above (T1, T2)**	AUISM Security Control: 0428 NZISM 17.5.9

	• ensures that the screen does not enter a power saving state before the screen or session lock is activated; • requires the user to reauthenticate to unlock the system; and • denies users the ability to disable the session or screen locking mechanism?			
A11#	Does the service's password reset/recovery process meet the following security requirements: • issues a single-use and time-limited reset link / token • delivers tokens only via verified, trusted channels (e.g. registered email or SMS with safeguards); • requires the user to create a new password immediately after token validation and invalidates the token after use/expiry; • implements rate-limiting and monitoring of reset requests and prevents account enumeration (no disclosure of whether an account exists); and • invalidates active sessions/refresh tokens upon a successful password reset.	1 & 2	A. No (#T1) B. Yes, some of the above **C. Yes, all of the above (T1, T2)**	AUISM Security Controls: 1227, 1593, 1594, 1595 NZISM 16.1.41 NZISM 16.1.42
A12	In relation to Single Sign-On (SSO) please specify all standards or providers supported:	1 & 2	A. OAUTH 2.0 B. OIDC C. SAML 2.0 D. Microsoft Entra E. Google Classroom / Workspace F. Other (please specify)	
A13#	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	A. Protection by exception (Allow access unless specifically denied) (#T1, #T2) **B. Protection by default (Deny unless approved) (T1, T2)**	
A14	Retired 2025			
A15	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	
A15A	Please provide further information on all methods available to supply data to the service, including any references or support articles if available.	All		
A16A	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)	
A16B #	In relation to the creation of accounts in third party services, are enforceable written agreements in place with all of these third-party services covering this arrangement?	1 & 2 Conditional (A15 – yes)	A. No (#T1, #T2) **B. Yes (T1, T2)**	
A16C	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)	
A17	Within the vendor organisation, is application control: • Implemented on all workstations; • Implemented on internet-facing and non-internet facing servers; • Enabled to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set;	1 & 2	A. No, none of the above B. Yes, some of the above **C. Yes, all of the above (T1, T2)**	AUISM Security Controls: 0843, 1490, 1656, 1657, 1658, 0955, 1582, 1471 NZISM 14.2

	• Enabled to restrict the execution of drivers to an organisation-approved set; • Implemented using cryptographic hash rules, publisher certificate rules or path rules; • Rulesets are validated on an annual or more frequent basis; and • When implementing application control using publisher certificate rules, both publisher names and product names are used.			
A18	Does your service offer alternative access methods such as reduced password requirements for younger students, temporary session join codes for classroom activities or similar?	1 & 2	A. No B. Yes (please specify including any reasoning for review)	
A19	What options are available for an administrator to configure and apply secure authentication policies for their school / user base?	1 & 2	A. Administrator can set a minimum password length and complexity rule for users B. Administrator can enforce MFA for users C. Other (please specify)	

6.2.6 Security – HR

Q	Question	Tier	Response options	Standard / References
HR1#	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, working with children checks) as per applicable regulatory requirements?	1	A. No (#T1) **B. Yes (T1, T2)**	AUISM Security Control: 0434 NZ PSR PERSEC1
HR2#	Does your organisation run a security, privacy and online safety awareness/education program for your staff which addresses the following at a minimum: • Identification of who the awareness training needs to be delivered to; • Identification of when awareness training needs to be delivered (e.g., during induction, annually, etc.);	1 & 2	A. No - none of the above (#T1) B. Yes - some of the above **C. Yes - all of the above (T1, T2)**	AU ISM Security Control: 0252 AU ISM Security Control: 1565 NZISM 9.1 NZISM 3.2.18 NZISM 3.3.13 NZISM 7.1.7 MCSS Security awareness level 2

	• Identification of how the awareness training is to be delivered (e.g., classroom training, online course, security awareness posters, emails, etc.);
	• Recording all training in a training register;
	• Reporting, regular review and updates as part of the organisation's training progrmme;
	• Delivery of the following training content to all personnel including as part of onboarding:
	  ○ Basic understanding of the need for information security, privacy and online safety;
	  ○ Awareness of the causes of unintentional data exposure and the dangers of connecting to insecure networks;
	  ○ Actions to maintain security, privacy and online safety;
	  ○ How to recognise and respond to suspected security, privacy and online safety incidents;
	  ○ Applicable policies and laws;
	• Annual tailored training for privileged users
	• Practical security, privacy and online safety awareness exercises, and
	  ○ Disciplinary actions for significant security and privacy breaches by staff?			

HR3#	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: • no longer have a legitimate requirement for access (implemented on the same day); and • are detected undertaking malicious activities (implemented immediately)?	1 & 2	A. No (#T1, #T2) B. Yes – but not implemented within required timeframes **C. Yes – (T1, T2)**	AUISM Security Control: 0430, 1591 NZISM 16.4.33
HR4	Does the service enable vendor personnel (including employees, contractors, or volunteers) to interact directly with students in any form? This includes, but is not limited		A. No – The service does not enable any direct interaction between vendor personnel and students	

	to, 1:1 or group instruction, tutoring, mentoring, messaging or chat functions, discussion forums, email, screen sharing, video or audio communication, or any other form of direct or indirect communication.		B. Yes – The service enables direct interaction between vendor personnel and students	
HR4A	Where direct interaction with students occurs, does the organisation ensure that all personnel comply with applicable child safety, screening, and engagement requirements in relevant jurisdictions?		A. Yes – All personnel meet jurisdictional requirements (e.g. Working with Children Check), with verification and ongoing monitoring in place B. Partially - Some controls are in place, but not all requirements are consistently met or monitored C. No - Personnel are not required to meet jurisdictional child safety or screening requirements	

6.2.7 Security – Processes and Testing

Q	Question	Tier	Response options	Standard / References
T1#	Does your organisation have an implemented continuous monitoring plan for all organisational systems and infrastructure that includes: • conducting automated discovery of assets • conducting regular automated vulnerability scans to identify missing patches or updates for vulnerabilities using an up to date vulnerability database • conducting penetration tests for systems after a major change or at least annually • analysing identified security vulnerabilities to determine their potential impact and appropriate mitigations based on effectiveness, cost and existing security controls • using a risk-based approach to prioritise the implementation of identified mitigations.	1 & 2	A. No (#T1, #T2) **B. Yes - meets all requirements above (T1, T2)** **C. Yes – meets all requirements above including the use of external independent resources to conduct penetration testing (T1, T2)**	AUISM Security Control: 1163 NZISM 4.1.26-29 NZISM 4.3 NZISM 6.1-6.2 NZISM 14.4-14.5

T2#	Does your organisation use a centrally managed approach to patch or update applications, drivers, operating systems, software defined infrastructure and firmware which includes ensuring: • the integrity and authenticity of patches; • approval of patches as part of change management processes; • successful application of patches; • rollback procedures are in place if a patch deployment is unsuccessful • that patches remain in place, and • that services, software and operating systems are retired, upgraded or replaced at least 6 months before their end-of-support date?	1 & 2	A. No B. Yes – centrally managed patching with retirement before end-of-support **C. Yes – all of the above (T1, T2)**	AUISM Security Controls: 0298 revision 7 NZISM 12.4 NZISM 14.5.8 MCSS Patching level 2
T3#	Are patches, updates or vendor mitigations for security vulnerabilities in: • internet facing services (including operating systems of internet-facing services); • workstation, server and network device operating systems; • operating systems of other ICT equipment; and • drivers and firmware; applied within two weeks of release, or within 48 hours if an exploit exists?	1	A. No (#T1) **B. Yes (T1, T2)**	AUISM Security Controls: 1690, 1694, 1695, 1696, 1751, 1697 NZISM 12.4
T4	Are patches, updates, or vendor-provided 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 the manufacturer making them available, or within 48 hours if identified as critical by vendors or working exploit is known to exist?	1 & 2	A. No **B. Yes (T1, T2)**	AUISM Security Control: 1691, 1692 NZISM 12.4
T5	Are patches, updates or vendor mitigations for security vulnerabilities in other applications applied within one month of release?	1 & 2	A. No **B. Yes (T1, T2)**	AUISM Security Controls: 1693 NZISM 12.4
T6#	Does your organisation have a formal, documented and implemented incident response plan which:	1 & 2	A. No - none of the above (#T1, #T2) **B. Yes - some of the above (T2)**	AUISM Security Control: 0125

	• Defines roles and responsibilities for incident response;
	• Requires security, privacy and online safety incidents to be investigated, remediated, and recorded in a register with the following information at a minimum:
	  ○ Date incident occurred;
	  ○ Date incident discovered;
	  ○ Description of the incident;
	  ○ Actions taken in response to the incident; and
	  ○ Name of person to whom the incident was reported?
			C. Yes - all of the above (T1)	NZISM 7
				NZISM 5.6
				NZISM 5.1.12
				MCSS Response planning level 2

T6A#	How frequently are incident response plans tested and updated?	1 & 2 Conditional (T6 – yes)	**A. Annually and after major incidents (T1, T2)** B. Every 2 years (T2) C. Other (#T1, # T2)	MCSS Response planning level 2
T7#	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. Yes (T1, T2)**	AUISM Security Controls: 0123, 0141, 0140 NZISM 7.2 NZPP-5 NZISM 7.2.22 NZPP
T8	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. Yes – some of the above (T2)** **C. Yes – all of the above (T1, T2)**	AUISM Security Controls: 0123, 0141, 0140 NZISM 7.2 NZPP-5
T8A	Please specify how customers are notified	1 & 2 Conditional (T8 – yes)		

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: • Backup strategies (including automated, time synchronised backups, secure storage of all backups); • Restoration strategies (e.g., disaster recovery); and • Preservation strategies?	1 & 2	A. No **B. Yes - meets some requirements (T2)** **C. Yes - meets all requirements (T1)**	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: • Applicable criteria for entry to and exit from the change management process • Categorisation of IT change (e.g., Standard, Pre-Approved, Emergency, etc.); • Approval requirements for each category of IT change; • Assessment of potential security impacts; • Prerequisites for the IT change (e.g., the IT change has been tested in a non-production environment); • 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.); • Documentation that needs to be updated as a result of the change (e.g., as-built documentation, IT Disaster Recovery Plans, etc.); and • IT change communication processes (e.g., notifications to users)?	1 & 2	A. No change management process B. Yes, change management process meets some requirements **C. Yes, change management process meets all requirements (T1, T2)**	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: • Scope and categorisation of information assets and systems;	1 & 2	A. No - none of the above B. Yes - some of the above **C. Yes - all of the above (T1, T2)**	AUISM Security Control: 1636, revision 0, ISM Security Control: 1526, revision 1 NZISM 3.2.10-13 NZISM 3.3.5-8 NZISM 4.1

	• Identification and assessment of risks/ threats, including those relating to the supply chain (e.g. from outsourced services that the solution relies on);
	• Identification of risk escalation thresholds, and risk acceptance delegations;
	• Selected and implemented controls to manage risks with the following details recorded in a risk register:
	  ○ Identified security risks, categories and risk ratings;
	  ○ Risk owner(s);
	  ○ Mitigation actions with clear ownership, prioritisation, target implementation date;
	  ○ Accepted risks (where applicable) and;
	  ○ Residual risk ratings after implementing mitigation actions
	• Proactive monitoring and testing of information assets and systems to maintain the security posture on an ongoing basis?
				MCSS Risk management level 2

Q5#	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) **C. Yes - security testing fully satisfies the guidance provided in an industry standard framework (T1, T2) (please specify framework)**	AUISM Security Control: 1239 NZISM 14.4.6 NZISM 14.5.8
Q6	Does your organisation have a documented and implemented IT Asset management process including: • A register of all components that make up the service, including software, databases, middleware, infrastructure etc (their version numbers, patch levels and configuration); • An ICT equipment and media register that is maintained and regularly audited;	1	A. No - none of the above B. Yes - some of the above **C. Yes - all of the above (T1, T2)**	AUISM Security Control: 0336, revision 4, ISM Security Control: 1493, revision 7 NZISM 8.4 NZISM 12.6 NZISM 13.4-13.6 MCSS Asset management level 2

	• A directive that ICT equipment and media are secured when not in use; • The secure disposal of ICT equipment and media (including sanitising/removal of any data or secure destruction/shredding)?			
Q7#	Does your organisation have a documented and implemented information security policy that outlines the following at a minimum: • management direction and support for information security; • requirement to comply with applicable laws and regulations; • information security roles and corresponding responsibilities/accountabilities; and • requirement for communication to management to ensure they maintain an awareness of, and focus on, addressing privacy and security issues?	1 & 2	A. No (#T1) **B. Yes (T1, T2)**	AUISM Security Control: 1478 revision 1. NZISM 5.1.7 NZISM 5.2
Q8	Does the service's application development have the following characteristics: • Environments are separated into at least development, testing and production environments; • Development and modification of software only takes place in development environments; • Unauthorised access to the authoritative software source is prevented; • Secure-by-design principles and secure programming practices are used as part of application development; • Privacy-by-design principles; and • Threat modelling is used in support of application development?	1 & 2	A. No – none of the above B. Yes - some of the above C. **Yes - all of the above (T1, T2)**	NZISM 14.4 NZISM 14.5

6.2.9 Security – Incidents

Q	Question	Tier	Response options	Standard / References

I1	Has the organisation, platform, or service had a recent security and/or privacy incident or breach in the last three years? If so were all incidents: • Managed according to the incident response plan and/or privacy breach management plan; • Notified to central agencies and affected individuals; and • Properly investigated with appropriate control improvements made as a result?	1 & 2	A. Yes - but not all requirements were met **B. Yes - all response, notification, investigation and improvement requirements were met (T1, T2) (please specify)** **C. Yes - response, notification, investigation, remediation in progress (T1, T2) (please specify)** **D. No known incidents or breaches have occurred (T1, T2)**	

6.2.10 Security – Data Deletion and Retention

Q	Question	Tier	Response options	Standard / References
D1	Are all data backups stored for a minimum of 3 months?	1 & 2	A. No **B. Yes (T1, T2)**	NZISM 6.4
D2	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 **C. Yes - written confirmation or certification is automatically provided to the customer (T1, T2)**	NZISM 13.1 NZISM 13.4-13.6
D2A	Please specify the timeframe for removing or deleting customer data from the service.	1 & 2		
D3#	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. Yes (T1, T2)**	AUISM Security Control: 1515 NZISM 6.4
D4	(Question removed 2023)	1 & 2		
D5	Does the organisation have a process to delete and remove inactive or dormant users and their related data?	1 & 2	A. No **B. Yes (T1, T2)**	
D5A	Describe the process including how the organisation determines a user is inactive or dormant and the timeframes for deleting their data.	1 & 2		
D6	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
CC1	Select the compliance certifications or security assessments that have been completed for the service and 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)	1 & 2	A. ISO/IEC27001 B. SOC 2 Type II 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. ISO/IEC 27701 (Privacy Information Management) J. HIPAA/HITECH (for handling protected health information) K. HITRUST CSF (Common Security Framework) L. Other (please specify) M. None of the above	NZISM 5.8 NZ PSR – INFOSEC3, GOV8
CC2#	Does the solution store, process, transmit, or otherwise handle cardholder data (CHD) or sensitive authentication data (SAD)?	1 & 2	**A. Yes – The solution is PCI DSS validated. (T1, T2)** **B. Yes – All payment functions are fully outsourced to a PCI DSS validated third party (please specify). (T1, T2)** C. No – The solution handles CHD/SAD but is not PCI DSS compliant. **D. N/A – The solution does not store, process, transmit, or interact with CHD/SAD. (T1, T2)**	NZISM 5.8

6.2.12 Security – Governance

Q	Question	Tier	Response options	Standard / References

GO1#	Is there a nominated and suitably qualified individual within the organisation responsible for: • Coordinating and reporting on cyber security • Overseeing information security risk management including supply chain risks • Leading cyber security improvement activities • Overseeing cyber security awareness and training • Overseeing cyber security incident response	1 & 2	A. No (#T1, #T2) **B. Yes, with some of the specified responsibilities (specify the substantive role of the individual) (T2)** **C. Yes, with all of the specified responsibilities (T1, T2) (specify the substantive role of the individual)**	AUISM 0714 NZISM 3.2
GO2#	Is there a nominated Privacy Officer within the organisation who has a good understanding of privacy requirements and is responsible for: • Providing privacy advice internally. • Liaising with the Office of the Australian Information Commissioner and the New Zealand Office of the Privacy Commissioner (as relevant). • Co-ordinating the handling of internal and external privacy enquiries, privacy complaints and requests for access to, and correction of, personal information. • Maintaining a record of your organisation's personal information holdings. • Assisting with the preparation of privacy impact assessments. • Measuring and documenting your organisation's performance against its privacy management plan.	1 & 2	A. No (#T1, #T2) **B. Yes, with some of the specified responsibilities (specify the substantive role of the individual)** **C. Yes, with all of the specified responsibilities (T1, T2) (specify the substantive role of the individual)**	AU PP NZ PP
GO3	Has responsibility for and ownership and accountability of critical system assets been assigned to individual/s in the organisation?	1 & 2	A. No **B. Yes (T1, T2)**	NZISM 3.4
GO4	What countries are your organisation's security and privacy operations teams and real-time monitoring and incident response systems located?	1 & 2	**A. Entirely within Australia and/or New Zealand (please specify) (T1, T2)** 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
PA1	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. Yes **(T1, T2)**	
PA2	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 **C. No age restrictions apply (T1, T2)** D. Other (please specify) **E. NA - this service will not be used by students (T1, T2)**	
PA3	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. **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)** **E. N/A - There is no content that may be regarded as intellectual property (T1, T2)**	

PA4	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. Yes (T1, T2)** **C. N/A - Service provider does not terminate accounts (T1, T2)**	

6.3.2 Privacy – General

Q	Question	Tier	Response options	Standard / References
PR1#	Does the organisation have a Privacy Policy that is: • made available free of charge; • published online or otherwise provided to customers before they use or purchase the service?	1 & 2	A. No - one or more of the above is not met (#T1, #T2) **B. Yes - all requirements are met (T1, T2)**	APP: 1.5 NZPP-3 APP 1.3
PR1A	Enter the URL for the service's Privacy Policy	1 & 2		NZPP-3
PR1B#	Is the Privacy Policy kept up to date, reviewed at least annually, and revised as necessary to ensure accuracy, relevance and clear and accessible language?	1 & 2	A. No - no review process or version/date control (#T1, #T2) **B. Yes - reviewed at least annually (or on changes) and version/date are documented (T1, T2)**	APP 1.3
PR1C#	How are users informed of the Privacy Policy before using or purchasing the service?	1 & 2	A. Users must review and agree to the Privacy Policy before use (e.g., checkbox, signature). B. The Privacy Policy is shown to users before use; consent is implied if they continue using the service. C. The Privacy Policy exists but users are not required to review or consent before use	APP 1.3
PR2#	Does the privacy policy or privacy collection notice for the service outline the following requirements about the collection and management of personal information at a minimum: • The kinds of personal information the entity collects and holds; • How the entity collects and holds personal information;	1 & 2	A. No (#T1, #T2) B. Yes - includes some of the above (#T1, #T2) **C. Yes - includes all of the above (T1, T2)**	APP: 1.4 NZPP-3 NZPP-4 NZPP-6 NZPP-7 ISO/IEC 27701:2019 – 7.3.2 & 7.3.3 EU GDPR – Articles 12–14

	• The purposes for which the entity collects, holds, uses, and discloses personal information; • The intended recipients of the information; • The consequences, if any, for an individual if all or part of the requested information is not provided; • How an individual may access personal information about the individual that is held by the entity and seek the correction of such information; • How an individual may complain about a breach of their privacy, and how the entity will handle such a complaint; • The company's contact details for privacy concerns or requests; • Whether the entity is likely to disclose personal information to overseas recipients; and • If overseas disclosure is likely, the countries in which such recipients are likely to be located, if it is practicable to specify them.			
PR3A	What **mandatory** information is collected by the service when **school staff** 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. Racial or Ethnic Origin or Affiliation M. Aboriginal or Torres Strait Islander status N. Other (please specify):	NZPP-3

			O. N/A - school staff do not register their own accounts for this service	
PR3B	What **mandatory** information is collected by the service when **students** 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. Racial or Ethnic Origin or Affiliation M. Aboriginal or Torres Strait Islander status N. Other (please specify): O. N/A - students do not register their own accounts for this service P. N/A - students do not require accounts for this service	NZPP-3
PR3C	What **mandatory** information is collected by the service when **parents** generate their own accounts for this service? Select all that apply. If not required, select N/A. **NOTE:** *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. Racial or Ethnic Origin or Affiliation L. Aboriginal or Torres Strait Islander status M. Other (please specify):	NZPP-3

			N. N/A - parent accounts are not required for school use of this service O. N/A - parents do not register their own accounts for this service	
PR4A	What **mandatory** information is collected by the service when a school-based administrator (or the service) generates accounts on behalf of school **staff**? 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. Racial or Ethnic Origin or Affiliation L. Aboriginal or Torres Strait Islander status M. Other (please specify): N. N/A - school-based administrators or teachers or the service provider cannot generate accounts on behalf of staff	NZPP-3
PR4B	What **mandatory** information is collected by the service when a school-based administrator (or the service) generates accounts on behalf of **students**? 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. Racial or Ethnic Origin or Affiliation L. Aboriginal or Torres Strait Islander status M. Other (please specify):	

			N. N/A - school based-administrators, teachers or the service provider cannot generate accounts on behalf of students	
PR4C	What **mandatory** information is collected by the service when a school-based administrator (or the service) generates accounts on behalf of **parents**? 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. Racial or Ethnic Origin or Affiliation L. Aboriginal or Torres Strait Islander status M. Other (please specify): N. N/A - school based-administrators, teachers or the service provider cannot generate accounts on behalf of parents	
PR5	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. No (please provide excerpt from ToS or PP) (T1, T2)**	
PR6	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. Yes, please specify circumstances (T1, T2)**	APP: 2.1 NZPP-1
PR7	Are mandatory fields clearly distinguished from optional fields during the standard account registration process?	1 & 2	A. No **B. Yes (T1, T2)**	NZPP-3
PR8	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. Yes (T1, T2)**	NZPP-3

PR9	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. Yes (T1, T2)**	NZPP-9 APP4 QPP4
PR10#	Does your organisation share user data with third parties in any circumstance other than the following? If yes, please specify. • the individual has consented to the use or disclosure of the information; • 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; • the use or disclosure is required or permitted under privacy legislation in the customer's country; or • 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? For service in Australia, refer to the Australian Privacy Principles, as well as the permitted general situations and permitted health situations. For service in New Zealand, refer to the Privacy Principles and information sharing provisions in the Privacy Act 2020, as well as the Oranga Tamariki Act 1989 and the Family Violence Act 2018	1 & 2	A. Yes (please specify) (#T1, #T2) **B. No (T1, T2)**	APP: 6.1, 6.2 NZPP-11
PR11	Can users opt-in or opt-out to the service's commercial mailing list/promotional/marketing communications (e.g. email mailing lists)? *Commercial mailing lists are those that are used for the purpose of distributing sales and marketing and promotional materials, including (but not limited to)*	1 & 2	A. Users cannot opt-out. Users are automatically subscribed to receive commercial/promotional/marketing communications. B. Users can opt-out. Some or all users are automatically subscribed but can opt-out after the fact	APP7 and Spam Act 2003

	competitions, education research related to the product, and end user feedback. *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.*		**C. Users can opt-in. Users do not receive commercial/promotional/marketing communications unless they explicitly opt-in (T1, T2)** **D. N/A – The service or organisation does not have any commercial/promotional/marketing communications (T1, T2)**	
PR12#	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: • The government related identifier is required or authorised by or under a law or a court/tribunal order within the customer's country; • 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; • Use or disclosure is necessary for the organisation to fulfil its obligations to a government agency or education authority within the customer's country; • Use or disclosure is required or authorised by or under a law or a court/tribunal order within the customer's country; • The organisation reasonably believes the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities; • The identifier, organisation or circumstances are prescribed by regulations?	1 & 2	A. Yes (provide details of the identifier(s) and how each is used) (#T1, #T2) **B. No (T1, T2)**	APP: 9.1, 9.2 NZPP-13

PR13#	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	A. No (#T1, #T2) B. Yes - with a cost and resolved outside of 3 months C. Yes - with a cost and resolved within 3 months **D. Yes - free of charge and resolved outside of 3 months (T2)** **E. Yes - free of charge and resolved within 3 months (T1, T2)** F. NA - service does not collect personal information **(T1, T2)**	APP: 12.1, 13.1 NZPP-6 NZPP-7
PR14#	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.		**A. No discovery functionality exists within service (T1,T2)** 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
PR15	Does the service capture a user's location data?		**A. No location data processed (T1, T2)** **B. The service must capture user location data to function. Location data is captured with a user's explicit consent (T1, T2)** 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.	

PR16#	How does the organisation notify users when updates occur to the Privacy Policy and the Terms and Conditions?	1 & 2	A. Users are sent a notification when updates are made to the Privacy Policy and Terms and Conditions B. Users are sent a notification prior to updates being made to the Privacy Policy and Terms and Conditions (please specify minimum timeframe) **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)** D. None of the above (#T1)	
PR17#	Does the Privacy Policy or other published document describe all of the service's sub processors including information on: • The name of the sub processor and its organisation; • Contact information of the sub processor (e.g. website URL, email address); • The data types disclosed to the sub processor including the purpose of the sub processor; • The lawful basis for processing the data where applicable; • Countries where data may be processed in or stored.	1 & 2	**A. Yes - All of the above (T1) (please provide link)** B. **Yes - Some of the above including name of the sub processor, data types disclosed, and location of processing (T2) (please provide link)** C. No (#T1, #T2)	
PR18	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	A. Yes (Please specify) **B. No (T1, T2)**	
PR19	Does the organisation or service share, publish, or provide access to any personal information or aggregated/de-identified user data to third parties for advertising, market research, profiling, or similar purposes?	1 & 2	A. No personal information or aggregated/de-identified data is shared, published, or provided to third parties for these purposes	

			B. Aggregated or de-identified user data may be shared with third parties (no personal information is shared) (please specify) C. Personal information may be shared with third parties for advertising, market research, profiling, or similar purposes (please specify) D. Both personal information and aggregated/de-identified data may be shared with third parties for these purposes (please specify)	
PR20	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. No (T1, T2)**	

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
PF1	When using the service, are any users exposed to advertising, marketing and/or offers?	All	A. Yes **B. No (T1, T2)**	
PF2	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?	**1 & 2**	A. No **B. Yes, please provide details (T1, T2)** **C. N/A (T1, T2)**	
PF3	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 **C. Profile is generated but only visible to user (e.g., visibility is restricted by default) (T1, T2)** **D. No user profile is generated (T1, T2)**	
PF4	Select all functionality available within the service.	All	Informational only, used to generate subsequent questions. A. Forms, surveys and eSignatures B. Online meetings, video conferencing, audio conferencing C. Remote access tools D. Screen Sharing and/or Screen recording E. Chat / Instant Messaging F. Commenting and communities/forum G. Quiz, poll, flashcard creation and/or distribution H. File download, including executable, developer tools, images etc. I. Direct email J. File upload and storage, and file sharing and collaboration K. Content creation and collaboration L. Content libraries M. Notifications and alerts N. Online learning activities, assessments and/or games O. Administrative support services and records management P. Data distribution, data broker, integration platforms as a service Q. Authentication as a service and identity providers	

			R. Data aggregation, analytics, insights and reporting S. Assessment or collection of health and well-being information including socio-emotional factors (e.g., physical and mental health, well-being, behaviour) T. Other (please specify) U. None of the above	
PF5	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	
PF6#	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)	
PF7#	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)	
PF8#	In relation to the screen sharing and/or screen recording functionality available within the service, select all that apply.		A. Use of screen sharing functionality is disabled by default B. Screen sharing and/or screen recording can be disabled by an administrator or moderator C. Screen sharing sessions and/or screen recording are initiated and/or accepted by the user who is sharing their screen D. Screen sharing and/or screen recording sessions are not logged (#T1, #T2) E. Screen recordings can be shared with other users on the service	
PF9A	How does your service moderate chats/messages for inappropriate content? (Select all that apply)		A. The service moderates chat/messages using a profanity filter B. The service moderates chat/instant messaging and reserves the right to remove	

			posts and/or users that breach the Terms of Use C. Users can report chat/instant messaging that breaches the Terms of Use D. Other (please specify) E. None of the above	
PF9B	Can non-account holders chat and communicate with account holders (i.e., no log in is required to participate in chat/messaging)?		A. Yes **B. No (T1, T2)**	
PF9C	What controls are in place to restrict communication and access to other users?		A. Communication can be limited to restricted groups only (e.g., class, year level) B. Chat/instant messaging is visible to an administrator (e.g., teacher) in real time C. Chat/instant messaging can be disabled by an administrator or moderator D. Other (please specify) E. None of the above	
PF9D#	Are audit logs of chat/instant messaging available including all of the following information: • account identifier of the sender and recipient; • timestamp of the message or event, and • whether the message was removed (if applicable).		**A. Yes (T1, T2)** B. No (T1#, T2#)	
PF10A	How does your service moderate your commenting and communities/forums functionality for inappropriate content? (Select all that apply)		A. The service applies a profanity filter prior to publishing B. The service moderates comments and reserves the right to remove posts and/or users that breach the Terms of Use C. Users can report comments that breach the service's Terms of Use D. Comments must be approved by an administrator or the service prior to publishing E. Other (please specify) F. None of the above	

PF10B	Can non-account holders can post comments and communicate with account holders (i.e., no log in is required to post or reply to comments in communities/forums):		A. Yes **B. No (T1, T2)**	
PF10C	What controls are in place to restrict communication and access to other users?		A. Commenting can be disabled by an administrator/moderator B. 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) C. Users can upload files or share projects or files in forums/communities D. Other (please specify) E. None of the above	
PF10D#	Are audit logs for commenting and/or community forums available including all of the following information: • account identifier of the sender and recipient; • timestamp of the post or event, and • whether the post was removed (if applicable)		**A. Yes (T1, T2)** B. No (T1#, T2#)	
PF11	In relation to the quiz, poll and flashcard functionality, select which features are offered within the service. Select all that apply.		A. Quizzes - service provider generated, non-editable B. Polls - service provider generated, non-editable 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	
PF12	(Question removed from 2021.1)			
PF13	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	
PF14	(Question removed from 2023.1)			
PF15	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	
PF16	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	
PF17	In relation to the file upload and sharing functionality available within the service, select all that apply.		A. Users can download files uploaded to the service by other users B. Authors have control over who can view and/or edit their files C. Administrators (e.g., teachers) can restrict who can view and/or edit users' files D. Administrators can disable file sharing E. None of the above	

			F. Not applicable – file sharing is not supported	
PF18	(Question removed from 2023.1)			
PF19	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	
PF20	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	
PF21	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 E. Search results that are not filtered based on user characteristics (e.g., age, year level, user type etc.) F. None of the above	
PF22	Who can publish content to content libraries within this service (i.e., users or service provider); and		A. Service provider generated content with moderation	

	is content subject to moderation to ensure users are not exposed to information, including images, video, text and/or recordings, which may be deemed: • Offensive by a reasonable member of the school community (e.g., nudity, pornography, graphic content, profanity, racist, sexist etc. and/or • Inappropriate for users under 18 years? Moderation may include: • The service reserves the right to remove content that breaches the Terms of Use • The service applies a profanity filter • The service has an implemented assurance procedure to ensure content conforms to quality standards prior to publication • Users can report content that breaches the Terms of Use Select all that apply.		B. Service provider generated content without moderation C. User generated content with moderation D. User generated content without moderation	
PF23	In relation to the notification and alert functionality available within the service, select all that apply.		A. Notifications and alerts can be one-way (broadcast) B. Notifications and alerts can be two-way e.g., parents/recipients can respond to notifications and alerts C. Notifications can be via email D. Notifications can be via SMS E. Notifications can be via push notifications F. Notifications and alerts can be disabled by an administrator/moderator G. For each notification and/or alert, the school and/or users can specify and/or limit the audience 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	
PF24	(Question removed from 2021.1)			
PF25	In relation to the online learning activities, assessment and/or game functionality available within the service, select all that apply.		A. The service provides standardised testing B. The teacher or user can create their own online learning activities and/or games. C. Answers can include pre-defined response options (e.g., multiple choice, Likert scales etc.) D. Answers are numerical free text fields (e.g., 0-9) E. Answers are short response free text fields (e.g., typing, equations, units of measurement, spelling and vocabulary) F. Answers can include long response free text fields (e.g., sentences, paragraphs, essays etc.) G. Answers can include file uploads (e.g. uploading a word document, image file etc) H. Data analysis, analytics and/or reporting is generated I. Data analytics and/or reporting can be sent to parents via the service. J. Answers can include audio or video (e.g. capture from the microphone or camera) K. Notes or comments can be made against a response, learning activity, assessment and/or game	
PF26	Select the response option which best describes the publication of results on the service. Results are considered to be published if they are visible to anyone other than the owner of the results.		A. Student results can be published on the service but privacy settings cannot be applied. B. Student results can be published on the service and privacy settings can be applied. C. Student results cannot be published.	
PF27	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	
PF28	What names do you, as the service provider, give to the various modules available within the service?		*Informational question- used to inform QA and data assets disclosed to service.*	
PF29	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 purpose? Please indicate whether this data field is mandatory or optional.		For each indicate mandatory, optional or not collected: 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	
PF30	When a school uses this service, what additional information (beyond what's required to set up an account) may be collected about students, staff, or parents? This question is only about school use, exclude any data collected during personal use by parents. For each data asset, please specify whether it relates to student, staff, or parent. Select N/A if no data is 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	
PF31	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)	
PF37	In relation to the assessment or collection of health and well-being information through functionality available within the service, select all that apply:		A. Online forms – service provider generated, non-editable B. Surveys – service provider generated, non-editable C. Quizzes – service provider generated, non-editable D. Polls – service provider generated, non-editable E. Learning activities and/or game-based assessment F. Diagnostic and/or standardised testing G. Online forms – customisable / user generated H. Surveys – customisable / user generated I. Quizzes – customisable / user generated J. Polls – customisable / user generated K. Learning activities and/or game-based assessment – customisable / user generated N. Data analysis, analytics and/or reporting is generated for users based on their responses	

			P. Well-being data analytics and/or reporting can be sent to parents via the service.	
PF37A	Does the service have in-built monitoring and/or reporting tools for schools to identify respondents who may require follow up or additional support?		A. In-built monitoring and/or reporting tools identify respondents who may require follow-up or additional support - (please specify) B. No in-built monitoring and/or reporting tools are provided to identify respondents who may require follow-up or additional support.	
PF38	In relation to the response options available within the service to assess or collect health and well-being information, select all that apply:		A. Responses can include pre-defined response options (e.g., multiple choice, Likert scales etc.) B. Responses are numerical free text fields (e.g., 0-9) C. Responses are short response free text fields (e.g., typing, equations, units of measurement, spelling, and vocabulary) D. Responses can include long response free text fields (e.g., sentences, paragraphs, essays etc.) E. Users can request further assistance or to talk to someone. F. Users can request further assistance or to talk to someone and this automatically notifies the school-nominated staff member. G. Users are de-identified and response data is aggregated/summarised so users and respondent data and reports are anonymous. H. Response data is aggregated/summarised so respondent data and reports do not identify the user. I. Respondent data and reports identify individuals for the purpose of monitoring, action and follow-up. J. Other	

PF39	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 **C. Yes – All of the above (T1, T2)**	QPP11/IPP4 NZISM 16.6.7 NZISM 16.6.10
PF51	In relation to file upload functionality within the service, are the principles and techniques from the OWASP followed?		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 **E. Yes - All of the principles and techniques are followed (T1, T2)**	
PF52	Does the service automatically remove or sanitise potentially sensitive metadata (such as EXIF geolocation, device identifiers, and timestamps) from user-uploaded files?		A. Yes – All identifying or sensitive metadata is automatically removed or sanitised on upload. B. Partially – Sensitive metadata (such as geolocation) is removed, but non-identifying metadata needed for functionality is retained. (please specify) C. No – Metadata is retained only where the user uploading has provided explicit, informed consent for a feature that requires it. (please specify) D. No – Metadata is retained because it is technically required for core service functionality and cannot be removed. (please specify) E. N/A – The service does not accept user-uploaded files.	

PF53	Does the service offer support for passwordless authentication or biometric authentication?		A. Yes (please specify) B. No	
PF54	Can authentication flows be customised?		A. Yes (please specify) B. No	
PF55	Does the service provide audit logs for authentication events?		A. Yes B. No	
PF56	Are security questions customisable by the organisation or predefined?		Free text	
Data integration, aggregation, data broker, data hub, data distribution hub control questions (PF32, PF33, PF35, PF36, PF40-PF50)				
PF32	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. No (T1, T2)**	
PF33	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: • the purpose for data sharing; • the scope of data to be shared (e.g., academic results); • the scale of data sharing (e.g., current student records only, or a specific year level); • the security and privacy controls in place in recipient systems; and • ownership of data. Furthermore, data agreements are updated to reflect changes in any of the above?		A. No B. Yes - Some of the above but data agreements not updated C. Yes - Some of the above with data agreements updated **D. Yes (T1, T2)**	
PF34	Retired			
PF35	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:		Select all that apply: **A. Data sharing can be controlled by the customer (school, school system or jurisdiction) (T1, T2)**	

			B. Data sharing can be controlled by the data aggregator (service being assessed) C. Data sharing can be controlled by the data recipient	
PF36#	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)?		**A. Data aggregator notifies customer as soon as possible after discovery and provides all relevant details (T1, T2).** B. Data aggregator notifies customer without commitment to timeframe and/or details not provided. C. Third party service notifies customer as soon as possible after discovery and provides all relevant details. D. Third party service notifies customer without commitment to timeframe and/or details not provided. E. Unknown (#T1, #T2) F. No notification of customer occurs (#T1, #T2)	
PF40	Does your service offer enterprise level controls (for example schools that belong to an owning higher authority (e.g. a Department or Education Authority))?		A. No B. Yes – two or more levels (e.g. school level controls and Departmental controls) **C. Yes – two or more levels with Departmental controls overriding school level controls (T1, T2)**	
PF41	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?		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 **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)	
PF42	Does your service offer the ability for the customer to restrict which recipient systems are available for integration?		A. No B. Yes - Recipient systems can be defined by the school only **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)**	
PF43	Can the customer of your service restrict the data elements/fields that are shared with each individual recipient system?		A. No **B. Yes (please specify) (T1, T2)**	
PF44	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?		A. No **B. Yes (T1, T2)**	
PF45	Does your service require customers to regularly reauthorize all recipient and integrating systems and perform a review of all data elements/fields shared?		A. No **B. Yes (please describe the process including frequency) (T1, T2)**	
PF46	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?		A. No B. Yes - filtering can be applied only **after** source data is consumed by your service. Filtered records are then not shared with recipient systems (please describe) **C. Yes - filtering can be applied prior to data being consumed by your service (T1, T2) (please describe)** D. Yes – other (please describe)	

PF47	When a customer withdraws data sharing approval for a recipient system what action does your service take?		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. All of the above (T1, T2)** E. None of the above.	
PF48	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?		A. No **B. Yes. Please specify which systems and data are supported for write-back from your service. (T1, T2)**	
PF49	Prior to onboarding a recipient system to your service, what due diligence checks and verifications are performed by your organisation on recipient systems?		A. Security check performed or evidence of security maturity obtained (please specify including details of any industry standard or other certifications) B. Privacy check performed or evidence of privacy maturity obtained (please specify including details of any industry standard or other certifications) C. Security and privacy requirements are detailed in contracts between the service's organisation and the recipient system **D. All of the above (T1, T2)** E. None of the above.	
PF50	Are ongoing checks and monitoring performed by your organisation on the service's recipient systems to ensure compliance with security and privacy requirements?		**A. Yes (please detail and specify frequency) (T1, T2)** B. No	

6.4 Criteria – Interoperability

6.4.1 Interoperability – Data Standards

#	Question	Tier	Response options
DS4	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
DS5	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
DS6	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
INT5	Please select from the following integrations or connections that are available within the service.	1 & 2	A. Native (vendor-provided) integrations B. Marketplace / Partner-built integrations 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. Data standards-based integration (e.g. LISS, SIF) H. Other (please specify) I. None of the above
INT6	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
INT7#	In relation to **native and partner built connections or integrations**, are agreements in place between the organisation and all 3rd party services being connected or integrated with and do these agreements cover: • the purpose for data sharing; • the scope of data to be shared (e.g. academic results); • the scale of data sharing (e.g. current student records only, or a specific year level); • the security and privacy controls in place in recipient systems; and • ownership of data. Furthermore, data agreements are updated to reflect changes in any of the above?	1 & 2	**A. Yes (please specify) (T1, T2)** B. No (#T1, #T2)
INT8	In relation to **partner built connections or integrations**, what due diligence checks and verifications are performed by your organisation prior to the connection or integration being made available to users?	1 & 2	A. Security check performed or evidence of security maturity obtained (please specify including details of any industry standard or other certifications) B. Privacy check performed or evidence of privacy maturity obtained (please specify including details of any industry standard or other certifications) C. Security and privacy requirements are detailed in contracts with the organisation that develops and manages the integration or connection **D. All of the above (T1, T2)** E. None of the above.
INT9	In relation to **partner built connections or integrations**, does your organisation conduct ongoing monitoring to ensure compliance with your privacy and security requirements (e.g. developer guidelines, platform rules etc).	1 & 2	**A. Yes (please specify) (T1, T2)** B. No
INT10	In relation to **native and partner built connections or integrations**, does your service require the user to re-authorise or reconfirm integrations are still valid on a periodic basis?	1 & 2	**A. Yes (please specify timeframe) (T1, T2)** B. No
INT11	In relation to **native and partner built connections or integrations**, does the service provide privacy controls	1 & 2	**A. Yes (please specify) (T1, T2)** B. No

	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).		C. N/A – integration is "consume-only", returns data to the same user, or transfers no personal data
INT12	Question retired 2025		

6.5 Criteria – Safety

#	Question	Tier	Response options
SFP1	Does the organisation regularly review and incorporate the Safety by Design principles into the product design and throughout operation of the service?	1 & 2	**A. Yes (T1, T2)** B. No
SC1	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	**A. Yes - Published on the website (please provide a link) (T1, T2)** **B. Yes - Provided to users prior to usage of the service (please specify) (T1, T2)** C. No
SC1A	If students use or interact with the service, is the acceptable usage policy written in child friendly language?	1 & 2	A. No **B. Yes (T1, T2)** C. N/A - Students do not use or interact with the service
SC1B	Please provide details on how to access the service's acceptable usage policies, weblinks and any other relevant materials.	1 & 2	
SC2	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 **C. Yes - includes all of the above (T1, T2)**
SC3#	Does the organisation have processes in place to identify, respond to, or disclose any known instances of child-safety-related misconduct or offences involving its staff or contractors?	1 & 2	A. No (#T1, #T2) **B. Yes (T1, T2)**
SC4	Does the organisation that provides the product or service ensure all of its staff/contractors: • Receive induction regarding the importance of child safety;		A. No B. Yes - some of the above **C. Yes - all of the above (T1, T2)**

	• Are appropriately supervised to ensure they are behaving in a child safe way when supporting schools; • Receive training that acknowledges student diversity; • Consider diversity (gender-diversity, religious beliefs, indigenous cultural safety, etc) in the product design?		
SC5	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 **C. Yes - Please specify**
SC6	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
AP0	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
AP1#	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 (#T1, #T2) **B. Yes - meets all of the requirements above but conducted less frequently (T2)** C. **Yes - meets all requirements above (T1, T2)**
AP2#	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	1 & 2	**A. Yes - security testing fully satisfies the guidance provided in an industry standard framework (please specify framework) (T1, T2)** B. Yes - security testing partially satisfies the guidance provided in an industry standard framework (please specify framework)

	Applications, the OWASP Mobile Application Security Testing Guide)?		C. No (#T1, #T2)
MA1	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)
MA1A	Apple App Store URL, Google Play Store URL, Other Android marketplace URL	1 & 2	
MA2	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)
MA3	Does the mobile app only request permissions that are necessary for the app to function for its expected purpose?	1 & 2	**A. Yes (T1, T2)** B. No
BE1	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)
BE2	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
BE3	Does the browser extension only request permissions that are necessary for it to function for its expected purpose?	1 & 2	**A. Yes (T1, T2)** 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 requirements for the AI Module is listed separately within the AI Module section of this guide.

#	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.

6.9 Artificial Intelligence (AI Module)

A hash (#) indicates a control is critical for compliance, or if not complied with will result in a high risk outcome for the criteria and the overall outcome on the report.

6.9.1 AI – General

Q	Question	Tier	Response options	Standard / References
AI_G1#	Please select if AI is used for any of the use cases or applications as described below (e.g. the ST4S AI Exclusion List): • Processes personal information (e.g. receives student names, gender, racial/ethnic origin or other personal information including sensitive information) • Processes data that may be used to create profiles of individuals or groups that are used to further develop the model or other purposes not within the primary interest of the school • Processing biometrics, human attributes, motions, metrics or attributes whether physical or mental (e.g. facial recognition and scanning, eye tracking, detecting movement, determining or predicting emotions, student disability, learning difficulties etc.) • Student monitoring, behaviour management and observation services • Administrative support and decision making (e.g. automatically vetting enrolment or scholarship applications, complaint handling, disciplinary action etc) • Note taking (e.g., voice recording, speech recognition to-text transcribing, etc) • Utilising NSFW[2] AI models, producing or outputting NSFW content or any other content that may be deemed offensive by a reasonable member of the school community	All	A. Yes (please specify) B. No	

	• Applications or services which process health and wellbeing data (e.g. physical or mental health, fitness, meditation, food consumption, body metrics etc)
	• Prohibited uses as defined under the EU AI Act
	• Any application of AI that may be considered by the ST4S Team, a ST4S Working Group member or a reasonable member of the school community to be:
	  ○ Invasive
	  ○ Unethical
	  ○ Pose a risk to safety, human rights or privacy
	  ○ Not be within the best interests of the student and/or school
	• Processing files, media or content that is not manually uploaded by the user but rather provided via an integration or consistent connection to file libraries, directories, file and media hosting services etc (e.g. via API, FTP etc)			

AI_G1A#	Are AI features or functions designed to receive or process personal information?	All	A. Yes B. No	
AI_G1B	Can the AI features and functionalities be disabled by a school or administrator user for all other users?	All	A. Yes B. No C. No, but schools can request this	
AI_G2	Please select from the following which best describes AI features or functions within the service:	All	A. Automated grading and feedback systems B. AI-driven curriculum design and optimisation C. Anonymised Analytics and Reporting D. Analytics and Reporting with Personal Information E. Educational chat bots F. Non-educational chat bots G. Generation of learning resources and content H. Language processing for plagiarism detection I. AI-assisted research and data analysis tools J. Text translation	

			K. Image, video or audio generation L. Other (please specify)	
AI_G3	Please describe how the service utilises AI features and functionality	All	Free text field	
AI_G4	What type of users have access to AI functionality within the service? Select all that apply:	All	A. Students B. Parents C. Teachers D. Admins E. Other (please specify)	
AI_G5	For your products AI solution, select from the following options which best describes the AI solutions or models in use.	All	A. Ready-made AI solution or foundational model from another provider (e.g. OpenAI, Gemini etc) with no changes B. Another provider's AI solution or foundational model with customisations (e.g. to better fit the services needs such as with custom GPTs or extended data sets) C. Utilises an AI solution or foundational model developed internally within your organisation. D. Other (please specify)	
AI_G5A	Can you describe how your AI model is integrated with or dependent on the foundation model? And how does it contribute to the EdTech's system functionality?	All	Free text (Must include hyperlink to foundation model terms page)	
AI_G5B	Which foundation model 'Terms' apply to you (the Vendor) from the foundation model you used to develop your model? *For example, with OpenAI, it can be either 'Plugins and Actions Terms' or 'Business Terms' for non-individual use. Please provide a hyperlink to the applicable terms. If multiple models are in use, please list all terms as they apply.*	All	A. Free text (Must include hyperlink to foundation model terms page)	
AI_G6	Please list all AI models used by your product and advise if access is provided via a third party platform e.g. Anthropic Claude via AWS Bedrock	All	Free text field	

AI_G7	What type of model is the AI solution or model used in your application built on?	All	A. Generative AI model B. Predictive AI model C. Transfer learning model D. Semi-supervised learning model E. Unsupervised learning model F. Reinforcement learning model G. Meta-learning model H. Other (please specify)	
AI_G8	Does the organisation's current insurance policy cover incidents and breaches directly related to the deployment or operation of AI technologies, including but not limited to data privacy violations, unintended operational behaviours, or AI system failures? Please provide details on the scope of coverage.	All	A. Yes (please specify) B. No	
AI_G9	What sources of information or data sets does the AI solution consume or interact with? Select all that apply:	All	A. Information or data sets uploaded or entered by an end-user B. Information or data sets created from your organisation's existing information C. Information or data sets created by a third party D. Real-time information or data sets including data feeds E. Other (Please specify)	

6.9.2 AI – Hosting

Q	Question	Tier	Response options	Standard / References
AI_H1	In which countries are the AI solutions or models used in your product hosted (including inference endpoints and related services)?	All	Multi Choice - Country List	
AI_H2#	Will end users be informed of any relocation or expansion, such as a change of country, involving the AI model and the infrastructure or services used to host it?	All	A. No B. Yes (specify average notification lead time)	

6.9.3 AI – Logging

Q	Question	Tier	Response options	Standard / References

AI_L1	Does the system log user inputs and outputs to the AI model, including the following information: • Date and time of the request or event • User ID associated with the account • Session information • Contents of the request and corresponding output • Error messages or exceptions • Metadata or contextual information	All	A. All of the above B. Some of the above (please specify) C. None of the above	
A1_L1A	How long are these logs retained for and are they deleted or anonymised?	All	A. Logs are deleted after the session is ended by the user (e.g. the user closes the chat with the AI) B. Logs are deleted after a period of time (specify timeframe) C. Logs are anonymised after the session is ended by the user (e.g. the user closes the chat with the AI) D. Logs are anonymised after a period of time (specify timeframe) E. Other (please specify) F. None of the above	
A1_L1B	Is there a function within the service to export these logs?	All	A. Yes (please specify) B. No	
AI_L2	Does your organisation enforce logging and monitoring to detect anomalies or malicious activity associated with the AI system. These could be to detect: • any change in behaviour or performance that may indicate a compromise or data drift • ensure compliance obligations are met and to aid investigation and remediation efforts in the event of an incident • Log and monitor the network and endpoints that host your AI system to detect attempts to access, modify or copy system data • sign of automated prompt injection attacks	All	A. Yes B. No	

6.9.4 AI – Access

Q	Question	Tier	Response options	Standard / References
AI_A1	Does the solution have controls (i.e. role based access) to restrict access to certain users (e.g. students or teachers) from accessing or interacting with AI features or functionality?	All	A. Yes (please describe) B. No	

6.9.5 AI – Human Resources

Q	Question	Tier	Response options	Standard / References
AI_HR1#	Is training and education provided to all persons involved in the design, evaluation, development, and support of AI solutions or models on the following topics: • Ethical AI, covering aspects such as fairness, transparency, and bias mitigation. • User-centric design principles for enhancing usability and user experience. • Compliance awareness, including understanding regulations and legislative requirements relevant to AI implementation. • Privacy best practices and requirements for protecting user data and ensuring compliance with privacy regulations. • Cybersecurity training to mitigate risks and ensure the security of AI systems. • Education on online safety to promote awareness and responsible use of AI technologies.	All	A. All of the above B. Most of the above C. No or only some of the above	

6.9.6 AI – Technical and Testing Controls

Q	Question	Tier	Response options	Standard / References
AI_T1#	Does your organisation have a responsible AI framework and ethics policy which includes at a minimum: 1. Governance: • Principles and Values: Establish clear principles like fairness, transparency, and accountability that guide AI development and use.	All	A. Yes (please specify) B. No	

	• Roles and Responsibilities: Define roles and responsibilities for all stakeholders involved in the AI lifecycle, from developers to users. • Risk Management: Implement processes to identify, assess, and mitigate potential risks associated with AI systems, including bias, security vulnerabilities, and societal impact. 2. Design and Development: • Human-Centered Design: Focus on designing AI systems that meet human needs, prioritize well-being, and are inclusive. • Data Management: Ensure responsible data collection, storage, and usage practices that respect privacy regulations and minimize bias. • Algorithmic Transparency and Explainability: Promote transparency in how AI systems make decisions, allowing users to understand the reasoning behind outputs. 3. Testing and Deployment: • Testing and Validation: Implement rigorous testing procedures to ensure AI systems perform as expected, are reliable, and avoid unintended consequences. • Monitoring and Auditing: Continuously monitor deployed AI systems to identify potential issues, biases, or performance degradation. • Human Oversight: Maintain human oversight throughout the AI lifecycle for responsible decision-making and intervention when necessary. 4. Communication and Stakeholder Engagement: • Transparency with Users: Clearly communicate how AI systems work, their limitations, and how user data is used. • Stakeholder Engagement: Engage stakeholders like policymakers, regulators, and the public in			

	discussions about responsible AI development and deployment. 5. Accountability and Continual Improvement: • Accountability Mechanisms: Establish clear accountability for potential harms caused by AI systems. • Continual Learning and Improvement: Continuously learn from data, feedback, and real-world deployment to improve AI systems and address emerging issues.			
AI_T2#	Does your organisation conduct security testing and assessments of AI systems and their features/functionality, which encompass the following key areas: • Penetration and jailbreak testing • Vulnerability scanning • Testing of access control mechanisms	All	A. Yes (Please specify the frequency and timeframe) B. No	
AI_T3#	Does your organisation conduct privacy testing and assessments of AI systems and their features/functionality, which encompass the following key areas: • Data minimization testing • Data anonymization testing • User control testing • Compliance testing (Please specify the frequency and timeframe)	All	A. No B. Yes (every 6 months or less) C. Yes (between every 6 - 12 months) D. Yes (more than every 12 months)	
AI_T4#	Does your organisation conduct safety testing and assessments of AI systems and their features/functionality, which encompass the following key areas: • Bias and fairness analysis • Explainability verification	All	A. Yes (Please specify the frequency and timeframe) B. No	

	• Edge case validation • Content and interaction integrity checks • Testing for inappropriate content creation, responses or other harmful[1] interactions			
AI_T5#	Does your organisation implement the guidance of the OWASP Machine Learning Security Top 10 or equivalent? Reference Link: https://owasp.org/www-project-machine-learning-security-top-10/	All	A. Yes - All guidance is implemented B. Yes - Most of the guidance is implemented C. None or only some of the guidance is implemented	
AI_T6#	Does the organisation implement the guidance from the OWASP AI Security and Privacy Guide (or equivalent guidance)? Reference: https://owaspai.org/	All	A. Yes - all of the guidance is followed B. Yes - some of the guidance is followed C. No	
AI_T7#	Are there controls in place during the release of updates to AI systems, features/functions and models which include: • Transparent documentation to end users on how the AI functions, limitations, what is it sourcing data from etc • Clearly identifying and warning users of new AI systems, models and features/functions etc • Allowing users to opt-in and opt-out of new AI systems, models, features/functions etc • AI models are clearly versioned and this is communicated to end users • Users understand the limitations of the models use (e.g. disclaimer notices) • A published history of change logs for end users to observe and inspect changes to the AI that may differ from its previous use • Users are notified when changes to AI systems, models and features/functions occur.	All	A. Yes - All of the above B. Yes - Most of the above C. No or only some of the above	

AI_T8#	If information is collected from users for training or developing AI/ML models, what processes are in place to verify information is complete, accurate and suitable to be incorporated into training?	All	A. No processes are in place to verify information or it is not completed routinely B. Information is verified manually for training per a standard process C. Information is automatically verified (e.g. using another AI model to verify information for quality and assurance) D. A combination of manual human and automatic verification processes are followed E. Other (please specify) F. N/A - Information is not collected from users for training or developing AI/ML models	
AI_T9#	Is there a full and complete record of the training data you have supplied, and the processes and artefacts involved in the production/development/fine-tuning of the AI model?	All	A. Yes B. No	
AI_T10#	Is personal information used throughout the testing and development lifecycle of features, functions or models of the AI solution? (e.g. when testing AI features or functions, executing test cases etc)	All	A. Personal information is deidentified, and consent has been obtained B. Personal information is deidentified, and consent has not been obtained C. Personal information is not deidentified, and consent has been obtained D. Personal information is not deidentified, and consent has not been obtained E. Personal information is not used throughout the testing and development lifecycle	
AI_T11	During the AI model's testing and training lifecycle, do you engage external auditors to verify that the outputs are minimally affected by misinformation and bias?	All	A. Yes (please specify) B. No	

6.9.7 AI – Incidents

Q	Question	Tier	Response options	Standard / References

AI_I1	Have any of the AI systems, features, functions and models been involved in any of the following:
	
	• A security incident or breach
	• A privacy incident or breach
	• Producing biased results
	• Producing harmful[1] or inappropriate content such as:
	  ○ NSFW or adult content
	  ○ Deepfakes
	  ○ Harmful responses such as explicit descriptions of suicide or self-harm methods
	  ○ Other content or responses that may be deemed offensive or harmful to young people or a reasonable member of the school community.
		All	A. No (T1, T2)
			B. Yes – less than 12 months ago (please specify)
			C. Yes – greater than 12 months ago (T1, T2) (please specify)	

AI_I2#	Does your organisation have a documented process for identifying, investigating, and reporting on AI incidents, including those related to security incidents/breaches, privacy breaches/incidents, bias, or harmful content generation?	All	A. Yes B. No	

6.9.8 AI – Data Deletion and Retention

Q	Question	Tier	Response options	Standard / References
AI_D1	If a user withdraws consent of their data being included in the AI solution or model is the user data deleted and the model retrained?	All	A. User data is deleted and the model is retrained B. User data is deleted and the model is not retrained C. User data is never used to train the AI model	
AI_D1A	How long after deletion is the model retrained?	All	A. retrained within 3 months B. retrained within 6 months C. retrained within 12 months D. retrained after 12 months or longer	

6.9.9 AI – Governance

Q	Question	Tier	Response options	Standard / References

AI_GO1#	Does the organisation designate a dedicated role, distinct from development and product ownership, responsible for AI safety (e.g. AI Officer, AI Safety Officer or Ethics etc), and does this role include the following responsibilities: • Risk identification and assessment of AI systems. • Developing safety guidelines and mitigations for AI development and use. • Staying up-to-date on AI safety research and best practices. • Monitoring and auditing AI systems after deployment. • Advocacy and communication regarding responsible AI development. • Data governance. • Handling feedback and complaints (e.g. feedback from end users)	All	A. Yes, with all the specified responsibilities B. Yes, with most of the specified responsibilities C. No or only some of the specified responsibilities	
AI_GO2	In the context of AI: with regards to any third-party providers that make up the solution, or provide service to you, does your organisation: • have an inventory of all third-party service providers; • regularly assess and manage the risks associated with these third-party providers; and • ensure contractual agreements require third-party providers to comply with information security, privacy policies, and regulatory obligations.	All	A. Yes (please specify) B. No	

6.9.10 AI – Privacy

Q	Question	Tier	Response options	Standard / References
AI_PA1	Is data entered into the model also saved for training purposes or is it discarded? (e.g. Are all inputs of a student discarded or are inputs also saved into the model to retrain and improve?)	All	A. Inputs are retained for the purposes of retraining and model development - By Default	

			B. Inputs are retained for the purposes of retraining and model development - If Opted In C. Inputs are discarded D. Other (please describe)	
AI_PA2#	If the AI solutions or models are trained across user data (including where de-identified, content and media created etc) is explicit consent obtained from the user?	All	A. Yes (please specify how consent is obtained from the user) B. No C. Not applicable - user data is not used for training purposes	

6.9.11 AI – Privacy General and Terms

Q	Question	Tier	Response options	Standard / References
AI_PR1#	Are users opted-out by default of having user data and any other related information (including where de-identified, aggregated, etc.) being provided to AI?	All	Rows: A. Used for AI Usage Analytics B. Stored for Personalization by the AI C. Used for Training, Developing and Improving AI Models Options: • Opt-Out by Default • Opt-in by default • Not Applicable	
AI_PR2#	Does the service offer users control over their data with easily accessible privacy settings to manage consent and preferences on how user data is to be used with AI systems, models and features/functionality (including for model training purposes)?	All	A. Yes (please specify) B. No C. Not applicable - user data is not used with AI systems, models, features/functionality, or for training purposes	
AI_PR3#	Is there an easily accessible statement (Privacy Policy, Privacy Statement, Privacy Notice, Data Protection Policy, User/Customer Data Policy, etc) that informs individuals about the use and collection of their personal information or any other related data (e.g. including where de-identified, aggregated or otherwise) for use in AI (ML, LM, LLM) and does the statement outline the following in a clear and transparent manner:	All	A. Yes (please specify) B. No	

	• what personal data will be collected • the purposes for processing personal data • the retention periods for personal data • who the data is shared with • the individual's right to access, rectify or stop the use of their personal data • how to withdraw consent, Additionally, is this information provided in a reasonable timeframe, such as before an individual registers or their information is disclosed to AI systems and models?			
AI_PR4#	Has your organisation established a consent management process to manage user consent for their information being used for AI purposes, including providing and withdrawing consent?	All	A. No B. Yes (please specify) (T1, T2) C. Not applicable - user data is not used with AI systems, models, features/functionality, or for training purposes	
AI_PR5	Do you regularly review your processing, documentation and privacy information to check that your purposes have not evolved over time beyond those you originally specified? (e.g. function creep)	All	A. Yes - On a quarterly or more frequent basis (specify timeframe) B. Yes - Less frequently (specify timeframe) C. No	
AI_PR6#	Can users adjust settings to prevent information, including prompts shared with the AI models, from being shared with third parties?	All	A. Yes (please specify) B. No C. N/A - Information and prompts are not shared with third parties	
AI_PR7	Does the vendor indemnify the jurisdiction and users (e.g. staff, teachers and students) in respect of copyright or moral rights infringements that occur in connection with the use of the AI system, and if so, are there any caps or limitations on those indemnities?		A. Yes (please specify) B. No	
AI_PR8	Does the vendor give warranties that the use of the AI model or system will not infringe copyright or moral rights, and if so, are there any caps or limitations on those warranties?		A. Yes (please specify) B. No	

6.9.12 AI – Product Functionality

Q	Question	Tier	Response options	Standard / References

AI_PF1#	Do users receive a notification or a disclosure notice informing them when they are engaging with an AI system or when the content they are interacting with has been generated by an AI system? E.G> Chat bots clearly identify themselves as being an AI chat bot, charts and graphs produced by an AI system are clearly labelled as being AI generated.	All	A. Yes (please specify) B. No	
AI_PF1A#	Does the notification or disclosure notice include disclaimers indicating that the AI system may produce responses or outputs that could be inaccurate and contain biases?	All	A. Yes (T1, T2) B. No	
AI_PF2	What type of content can be generated or outputted by the AI systems or models?	All	A. Images B. Videos C. Text e.g. blog posts, social media posts, newsletters, presentations D. Audio or music E. Quizzes F. Emails G. Infographics H. Code, scripts or other web development content I. Other (please specify)	
AI_PF3	Can users input their own content, media or other assets in to be modified or edited using AI tools/functionality? (e.g. not using text prompts to output images but building upon already existing images)	All	A. Yes (please specify) B. No	
AI_PF4#	Within the service, are there easily accessible tools for users to provide feedback on AI features, such as: • Commenting on the accuracy of a response or output of the AI (e.g., thumbs up/down) • Reporting harmful[1] or inappropriate content (e.g., biased outputs, harmful digital communications, misinformation)	All	A. Yes (please specify) B. No	

	• Providing general feedback in relation to a particular AI feature • Additionally, can users provide other relevant feedback to improve the AI's performance?			
AI_PF5#	What methods are enabled for users to report AI-generated content that may be harmful or breaches the terms of service?	All	A. Form B. Direct email to the service provider C. Chat D. Other (please specify) E. None of the above	
AI_PF6	How does the service provider handle reported content during the investigation process? (e.g., is it removed from user view, taken down from the public site, etc.) Please specify the timeframes for investigating and taking action (e.g., censoring or removing content, etc.)	All	Free text field	
AI_PF7	Are users able to disable AI chat or prompt history?	All	A. Yes - All user types (please describe) B. Yes - But only user types with certain access privileges, i.e., administrative access (please describe) C. No D. N/A - No prompt or chat history is available	
AI_PF8#	Are there controls to warn, restrict or prevent personal information from being disclosed to the AI model? Select all that apply:	All	A. Automatic safeguards block users from inputting personal information. B. Intermediary filtering systems are in place to remove personal information before it reaches the AI model C. Manual review processes are established to check and prevent personal information disclosure. D. Warnings or prompts remind users not to share personal information E. Other (please specify) F. No controls are available	

AI_PF8A	Please further describe the controls in place to warn, restrict or prevent personal information from being disclosed to the AI model.	All	Free text field	
AI_PF9#	Does your organisation provide consumers (end-users) with guidance on: • Understanding how the AI system works • Using the AI system effectively for desired outcomes • Using the AI system responsibly and safely. • Identifying and addressing biases and addressing ethical issues to ensure safe and responsible usage • Protecting user privacy and obtaining consent. • Complying with regulations and legal obligations where applicable • How to provide feedback, report errors and concerns	All	A. All of the above B. Most of the above C. None or only some of the above	

6.9.13 AI – Safety

Q	Question	Tier	Response options	Standard / References
AI_SF1	Does your organisation publish help material on how to safely utilise AI functions and features within the service that is: • Easily accessible to the student or young person (e.g. an easy to find help button in the chat bot or on the application), and • Written in child friendly language	All	A. Yes (please specify) B. No	
AI_SF2	Does the organisation consider and apply Safety by Design principles within the AI components of the service?	All	A. Yes (please describe) B. No	
AI_SF2A	Please describe	All	Free Text	
AI_SF3	Does the organisation incorporate appropriate safeguards to reduce and mitigate the potential misuse of AI features and functionality?	All	A. Yes (please describe) B. No	
AI_SF3A	Please describe	All	Free Text	
AI_SF4#	Do you have a process in place to recognise and filter out and remove illegal, harmful[1] or inappropriate content	All	A. Yes (please describe) B. No	

	from AI models or their outputs? (Illegal or harmful content, such as CSEA material, image based abuse (IBA), harmful digital communications and abuse, or false, biased, harmful[1], or misleading information, or other unlawful material).			
AI_SF4A	Please describe	All	Free Text	
AI_SF5#	If students have access to the AI tool and are able to generate their own content does the service have real time detection tools to quarantine and alert administrators to inputs to the AI model which may be: • offensive and/or inappropriate • relating to self-harm or suicide • relating to drugs, alcohol or illicit substances • abuse including sexual abuse, physical or mental • unlawful activity		A. Yes - The user is alerted first and then asked if they would like to continue with the prompt as it will notify the school. Opportunity to withdraw the prompt. B. Yes - Alerts to the account holder immediately without warning to the student C. Other (please specify) D. No	
AI_SF6#	Are prompts filtered by default before being disclosed to the AI model to minimise or restrict harmful prompts, model manipulation or jailbreaking attempts?	All	A. Yes (please specify) B. No C. Not applicable - users cannot input content or prompts	
AI_SF6A	What type of content is flagged by the filter?	All	Select all that apply: A. Personally Identifiable Information (PII) B. Data Poisoning attacks C. Prompt injection D. Training attack E. Other (please specify)	
AI_SF7	Can school administrators enable chatbot message or session limits for their users?		A. Yes - please specify B. No	
AI_SF8	For any interactive AI feature (including chat, messaging, image or other media generation), does the service have a documented and implemented crisis response protocol that includes the following safeguards: 1. Crisis messaging and support signposting / On detection of high risk self harm or suicide content, the AI:		A. Yes, all safeguards are implemented and operating as described. B. Partially, some safeguards are implemented (please specify which). C. No, a crisis response protocol for self harm and suicide is not implemented.	

	• clearly states it cannot help with self harm or suicide requests • avoids providing methods, plans or instructions • presents clear, compassionate crisis messaging and prominently displays appropriate emergency and crisis support contacts for the user's country or school or tenant region, for example 000 and Lifeline 13 11 14 in Australia or local equivalents. 2. Crisis safe mode and content restriction / On high risk detection the AI moves into a restricted crisis safe mode that: • refuses or redirects further high risk prompts • limits responses to pre approved, clinically reviewed crisis safe scripts • maintains this state for a defined period, for example at least 30 minutes, rather than resuming normal conversation immediately. 3. AI disclosure and dependency mitigation \ The service helps prevent unhealthy reliance on the AI by: • clearly disclosing at the start of use, and at regular intervals, that the user is interacting with AI and not a human • issuing additional notifications or breaks after extended continuous use, for example at or before three hours of ongoing companion style use, and complying with any stricter local legal requirements. 4. Escalation and notification in education settings \ For school managed accounts, where permitted by law and school policy, high risk events such as explicit suicidal intent or concrete self harm plans:		D. Not applicable, the service does not provide interactive AI features to students or young people.	

	• are flagged as a high priority alert to authorised wellbeing or safeguarding staff only • are covered by a documented workflow that aims for human review and triage within 15 minutes of the alert, with clear roles, privacy safeguards and record keeping. 5. Clinical review and ongoing evaluation \ The crisis response protocol, prompts and AI behaviour: • are co designed or reviewed with qualified mental health professionals, with attention to youth specific guidance where relevant • are tested at least annually, and after any serious incident, using self harm and suicide test cases, with results used to improve detection, refusal and referral behaviour. 6. Other safeguards \ Other safeguards that reduce the risk of harm from self harm or suicide interactions with the AI (please describe).			

6.9.14 AI – 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
AI_EV1	Organisation's AI Ethics Policy and Responsible AI Framework	AI_T1
AI_EV2A	Security Testing (e.g. jail breaking / penetration testing)	AI_T2, AI_T3, AI_T4
AI_EV2B	Privacy Testing (e.g. testing for personal information, warnings and detection tools)	
AI_EV2C	Safety Testing (e.g. outputs of generated content is appropriate for audiences, checking for dangerous responses, NSFW content etc)	
AI_EV3	AI Incident Management Plan (for handlining security incidents/breaches, privacy breaches/incidents, bias reports harmful[1] content generation)	AI_I2
AI_EV4	Would you like to submit additional evidence?	AI_EV4

	Additional evidence can support us in understanding your AI systems, models and features/functionality. Examples of additional evidence might include: • Publications by your organisation on how models are developed and trained • High level system architecture and networking diagrams	
AI_EV5	Evidence of external auditors review on the AI model	AI_T11

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, 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. 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. Financial information covers individual, family, staff, student financial records, bank details, debts, debt reminders etc.	Sensitive information, including: **for students:** 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 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 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 **for job applicants, staff and contractors:** 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

1) Data		
Assessment Tier	**Data Definitions**	**Data examples**
	Identifiers covers government or other allocated identifiers which are possibly sensitive for the purposes of tracking an individual.	**Health information, including:** • 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 • for parents: history of genetic and familial disorders (including learning disabilities), miscellaneous sensitive information contained in a doctor or health report; and • for job applicants, staff members and contractors: medical condition affecting ability to perform work, health information, medical certificates and compensation claims. **Financial information including:** 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 **Identifiers includes:** 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.
Tier 2	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.	**for students:** 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

1) Data		
Assessment Tier	**Data Definitions**	**Data examples**
	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	**for parents:** 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 **for job applicants, staff and contractors:** 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.
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	Products which offer generic functionality in any of the following categories will be deemed as falling into tier 1: o Remote access Products in the following broad product categories will be deemed as tier 1: o Learning Management/ Student management and learning support systems e.g., student work, assessment, academic results, timetabling, pastoral care, communication;	Products which may contain, display or promote the following categories of information will be deemed as falling into tier 1: 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. 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)

	o School administration systems, including student records, attendance, data collection e.g., enrolment, consent management; o Financial management/ payment collection systems; o Behaviour management systems; o Teacher professional development tools/record keeping systems; o File storage e.g., iCloud, Dropbox, Google Drive; o Services with customisable functionality - site specific (including integration with enterprise solutions or additional third-party services); o Video or student diary or communication tools (parent, teacher, child); o Video capture/audio/webcam functions; o Services with multiple primary purposes/functionalities (e.g., combination of those listed in Tier 2)	
Tier 2	Products which offer functionality in any of the following categories will be deemed as falling into tier 2: o Chat/Instant or delayed messaging o Blogs o Email o Message boards o Screen sharing o Group calls o File sharing o Photo posting/sharing o Social media account sharing/integration (e.g., Facebook, Google) o Market places for the exchanges of goods/services	Products which may contain, display or promote the following categories of information will be deemed as falling into tier 2: o Political material o Sensitive topics which may cause offense in the community
Tier 3	N/A	N/A

Appendix B – Standards, Frameworks and References

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

* Standards and reference mapping last reviewed in June 2026

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. The technology providers we use to deliver the ST4S assessment process to you have achieved cybersecurity assessments or industry certifications such as ISO27001, SOC2 etc. You can find out more by visiting their website listing in the sub processors table below.

c. 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.
d. 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.
e. 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.
f. 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. Our preference is to select legal jurisdictions which have privacy and data protection laws that are comparable and/or provide stronger protections to personal information. Please refer to the sub-processor list in this guide for further information.
g. When providing documentation to us, you may distribute these via email however our preference (particularly for evidence documentation) is to utilise a direct upload to our questionnaire tool.
h. If you wish to provide limited access to documentation to us, you may discuss various options with your assessment officer. We may be able to review documentation and evidence with 'read-only' permissions on your cloud storage provider or access documentation from your trust portal or security centre. Should you wish to provide us to tools or services to access this information, it is your responsibility to ensure our access is setup correctly, securely, that you communicate credentials in an encrypted and secure manner to us, and that you appropriately handle our access or accounts by disabling access when the ST4S review or activity is completed.

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 this guide 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 (such as the Department of Education in a State/Territory within Australia) 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 such as improving the ST4S framework and its criteria.
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.

Appendix D – Changes since previous framework version

The following is a list of the key changes to the ST4S Criteria from V2024.1 to V2025.1. ST4S also maintains the previous release of the ST4S Supplier/Vendor Guide on our website.

Framework Version	Change	Description
V2026.1	New	Updates to the Full Assessment and AI Category introducing new criteria and wording adjustments based on feedback from the ST4S WG and Suppliers. New or changed criteria includes: H5, S1, S3, S4, S10, L1, A5, A6, A9, HR2, HR4, HR4A, T2, T4, T6, T6A, Q4, PR1C, PR2, PR17, PR19, PF37, PF37A, SC3, AI_G1, AI_G1B, AI_G6, AI_L1, AI_T3, AI_SF7, AI_SF8 Retired criteria: INF1
V2025.1	New	Updates to the Full Assessment and AI Category introducing new criteria and wording adjustments based on feedback from the ST4S WG and Suppliers. New or changed criteria includes: P2C, P3A, P3B, P8, P9, P10, P11, P12, P13, P14, H0, H2, H4, H6, S1, S2, S3, S6, S7, S8, S10, S12, L1, A0, A2, A3, A4, A8, A11, A12, A18, A19, HR2, T1, T2, T6A, T8A, Q2, I1, CC1, CC2, PA3, PR1, PR2, PR3, PR4, PR15, PR16, PR17, PF4, PF8, PF9, PF10, PF17, PF25, PF30, PF53, INT5, INT11, AI_H1, AI_GO2, AI_PR4, AI_PR7, AI_PR8 Retired criteria: P15, A14, INT12
V2024.1 AI Category (AI)	New	Updates to the AI Category introducing new criteria and wording adjustments based on feedback from the ST4S WG and Suppliers. New or changed criteria includes: AI_PF1A, AI_T9, AI_T10, AI_T11, AI_EV5, AI_G5A, AI_G5B, AI_SF6, AI_SF6A, AI_PR6
V2023.2 AI Category (AI)	New	Introduction of the AI Category noting multiple subcategories across security, privacy, safety, evidence etc.

Appendix E – ST4S Excluded List

The Safer Technologies for Schools (ST4S) assessment is focused on evaluating digital products and services that are essential for the educational environment, ensuring they meet high standards for security, privacy, and interoperability. There are some service categories or use cases that we do not assess.

The ST4S Excluded list is published on our website and may change from time to time. Please visit the link for the most recent version.

Appendix F – Definitions

Item	Definition
Harmful	Harmful is defined to include anything that is objectionable, illegal or unlawful, and restricted content made available to the wrong age group.
NSFW	Not Safe for Work is a general term used to describe any content that may be deemed inappropriate to create, view or access whilst in the workplace (and schools). NSFW content includes content that may be deemed inappropriate for younger audiences (e.g. persons under 18). Examples of NSFW content include nudity, excessively violent images, gore etc. NSFW content can also apply to text-based content. Examples may include AI services which may generate overly violent or sexual text stories or engage in conversation of this nature.

Appendix G – Supplier Code of Conduct

All suppliers participating in the ST4S assessment process must demonstrate due care and skill, remain transparent, adhere to the conditions within this guide, and refrain from misconduct. Misconduct matters may be referred to the ST4S WG and/or NEDAG, alongside relevant information such as correspondence or internal notes.

A decision as to what constitutes misconduct and whether an organisation or individual has engaged in misconduct is at the sole discretion of the ST4S Team. Examples are provided in this appendix.

Escalation Path and Resolutions

1. **Initial Decision**

The assigned assessment officer makes the initial decision. Decisions of risk levels and compliance and pre-defined within the ST4S framework. This includes the risk and treatment wording on reports and risk outcomes. Most cases are resolved by assessment officers. In the first instance, you should work with the assessment officer to resolve the matter and provide technical information to support their review.

1. **Initial Decision**
   The assigned assessment officer makes the initial decision. Decisions of risk levels and compliance and pre-defined within the ST4S framework. This includes the risk and treatment wording on reports and risk outcomes. Most cases are resolved by assessment officers. In the first instance, you should work with the assessment officer to resolve the matter and provide technical information to support their review
2. **Program Manager Review**
   If necessary, the decision is escalated to the ST4S Program Manager.
3. **Primary Member Review**
   If necessary, the matter is referred to the ST4S Working Group member who either assigned the most nominations to your assessment, referred or invited your organisation to participate in the ST4S assessment process (the primary member). In most cases, the primary member can resolve the matter. Their decision is final unless they choose to escalate the issue to the ST4S Working Group, however they are not required to.
4. **ST4S Working Group Review**
   If the matter is still unresolved, the primary member may choose to refer the matter to the ST4S Working for a final decision by majority vote.

Examples of Misconduct:

Misconduct includes, but is not limited to, the following:

1. **Plagiarism and Copyright Infringement**
   Using material belonging to another organisation or individual without proper authorisation. This includes on your website, privacy policy etc.
2. **Solicitation of Outcome**
   Attempting to influence an outcome whether by bribery, legal threats, bypassing the escalation process or other improper means.
3. **Bypassing Procedure or the Escalation Path**
   Lodging a complaint about the ST4S assessment process, outcome, or decisions to senior management at ESA instead of following the 'Escalation Path and Resolutions' process.
4. **Misleading or Deceptive Conduct**
   Providing false or misleading information during the assessment or related activities or making misleading representations.
5. **Being Uncooperative or Unprofessional**
   Being uncooperative throughout the assessment process or communicating in a manner we deem to be forceful, rude, inappropriate, aggressive, and/or unprofessional.
6. **Misrepresentation of ST4S Status**
   By act or omission, misleading others about your status within the ST4S assessment, membership to the ST4S Product Badge Program and any other related ST4S activities.
7. **Breaches of Terms and Conditions**

Violating any condition specified in this guide, the declaration you sign when completing an ST4S assessment or form, or any other instruction issued by the ST4S Team.

8. **Other Misconduct**
   Any other behaviour that the ST4S Team reasonably believes amounts to misconduct.

What is not misconduct

1. **Failing to Meet Criteria**
   Receiving one or more non-compliant items during the Readiness Check or Full Assessment and committing to either discussing further with us or withdrawing from the process as you may choose. Our goal is to help you achieve a compliant outcome. Please see the 'Support' section for more details.
2. **Requesting a Re-Review or Escalation**
   You may request a second opinion or escalate a decision if you disagree with an outcome (see 'Escalation Path and Resolutions'). A challenge must be accompanied with technical reasoning and explanation.
3. **Genuine and Honest Mistakes**
   Errors made in good faith, genuine misunderstandings, or providing incorrect information due to an honest misunderstanding or differing interpretation of the ST4S criteria.
4. **Fair Discussion and Debate**
   Expressing genuine disagreement with the criteria, provided you remain open to further discussion with the ST4S Team and provide reasoning.
5. **Constructive Critique and Feedback**
   Offering constructive feedback on the assessment process, criteria, or related ST4S activities.

If you have any concerns regarding the code, please contact the ST4S Team on our website or directly to our assessment mailbox.