

A Practical Guide to

Evaluating EdTech Vendors' Data

Security & Data Management

Contents

- Introduction.....3
- Why Protecting Student Data Matters.....4
- How Schools Can Evaluate EdTech Vendors’ Data Security and Data Management5
 - Independent Security Certification.....5
 - Education-Sector Assurance Frameworks and State-Level Approvals.....5
 - Transparent Data Management and Privacy Alignment6
 - Responsible AI Oversight.....6
- How Security Controls Work Together.....8
 - Infrastructure, Data Residency and Performance9
 - Technical Safeguards.....9
 - Governance and Independent Verification9
- The Security Stack in Practice: A Case Study 10
- Buyer’s Checklist: Evaluating EdTech Vendors’ Data Security and Data Management12
- Conclusion.....13

Introduction

Digital learning platforms are now embedded in the daily operation of schools across Australia and New Zealand. Assessment, communication, reporting and learning support are increasingly delivered through connected digital systems, many of which incorporate cloud infrastructure and emerging AI capabilities. With this growing reliance on digital platforms comes an important governance responsibility: ensuring that the tools used in classrooms manage student data responsibly.

Digital learning platforms often process sensitive information relating to minors, including personal identifiers, learning progress data and wellbeing-related information. Schools remain accountable for protecting this data even when it is handled by third-party vendors. As a result, selecting technology providers now requires a level of due diligence that extends beyond functionality and classroom usability. This includes understanding what data is collected, where data is stored, how it is protected, how long it is retained, and whether security controls have been independently assessed.

This practical guide is designed to support school boards, principals and IT leaders through that evaluation process. It outlines the key security and compliance indicators schools should look for when assessing EdTech vendors and their digital learning platforms, including independent certifications, education-specific assessment frameworks, data management practices, responsible AI oversight, and appropriate technical controls and infrastructure.

It also demonstrates how these principles can be implemented in practice within an education platform, providing a practical reference point for school leaders conducting vendor due diligence. A structured checklist is included to help schools apply these considerations in a consistent and practical way when evaluating potential providers.

Creating a safe digital learning environment requires the same level of care and oversight that schools apply to physical learning environments: ensuring that the tools used in classrooms support teaching and learning while responsibly protecting students.

Why Protecting Student Data Matters

As schools adopt digital learning tools, the amount of student information processed through online platforms has increased significantly. Digital systems now support assessment, reporting, communication and personalised learning, meaning that student records often include a wide range of personal and educational data.

This information can include student identifiers, learning progress data, demographic details and, in some cases, wellbeing or support information. Because these records relate to minors, they require careful handling and appropriate safeguards.

Across Australia and New Zealand, regulators have emphasised that organisations responsible for personal information must take reasonable steps to ensure it is protected from misuse, loss or unauthorised access. These obligations apply to schools as well as to the third-party technology providers that process student data on their behalf.

At the same time as the education sector has increased its reliance on EdTech vendors and their digital platforms, the sector has also experienced a steady rise in cybersecurity incidents. Reports from the Australian Cyber Security Centre consistently identify education and training among the sectors affected by cybercrime activity. In New Zealand, national cybersecurity reporting has similarly highlighted the growing importance of data protection across public services, including education.

“Schools are among the most targeted organisations; the education sector tops the most targeted industry according to several reports.”



New Zealand Ministry of Education News,
Cyber Smart Week: Safer Logins, Safer Schools, 17 October 2025

When student data is compromised, the impact can extend beyond the immediate technical incident. Schools may experience operational disruption while systems are investigated or restored, and they may need to notify affected families and regulators. Exposure of sensitive student information can also raise safeguarding and privacy concerns, particularly when records relate to minors. In some cases, the effects may persist over time, as personal identifiers such as names, dates of birth or contact details can remain usable long after the initial incident.

For school leaders, these outcomes reinforce why careful selection and oversight of third-party vendors and digital learning platforms is an important governance responsibility.

How Schools Can Evaluate EdTech Vendors' Data Security and Data Management

When evaluating EdTech providers, school leaders and IT teams do not need to conduct their own cybersecurity audits. Instead, several widely recognised indicators can help schools determine whether a vendor manages student data in a structured and accountable way.

These indicators include independent certification, education-sector assurance frameworks, clear data governance practices, and responsible oversight of emerging technologies such as artificial intelligence.

The following sections outline the practical indicators schools can look for when assessing digital learning platforms.

Independent Security Certification

One of the clearest indicators of a mature security program is independent certification against recognised information security standards.

The most widely recognised of these is ISO/IEC 27001, an international standard for information security management systems. Rather than focusing on a single technical control, ISO 27001 requires organisations to implement a structured governance framework for managing information security risks.

To achieve certification, organisations must:

- identify and assess information security risks
- implement documented security controls
- maintain internal audit and governance processes
- undergo independent third-party certification audits.

Certification is not permanent. Organisations must undergo regular surveillance and recertification audits to maintain compliance.

For schools evaluating technology providers, ISO 27001 certification provides an important form of external validation. It demonstrates that information security practices have been independently assessed and are managed through a structured, ongoing risk management process rather than informal internal policies.

Education-Sector Assurance Frameworks and State-Level Approvals

In Australia and New Zealand, the Safer Technologies 4 Schools (ST4S) framework provides an education-specific process for assessing digital products used in schools.

ST4S evaluates technology providers against criteria relevant to school environments, including privacy alignment, authentication practices and data protection safeguards. ST4S provides an assessment and attestation framework designed to streamline vendor risk evaluation for schools and education departments.

Technology providers that successfully complete this process may be listed within the ST4S Product Catalogue and may participate in the ST4S Product Badge Program, indicating that a product has undergone ST4S assessment.

For school leaders and IT teams, the ST4S platform provides a practical tool for verifying vendor claims. Schools can visit st4s.edu.au to:

- search the ST4S Product Catalogue to confirm whether a vendor has been assessed
- verify whether a product holds an ST4S badge
- review the Excluded or High-Risk lists maintained by the framework.

In addition to ST4S, some Australian state education departments conduct their own compliance and security reviews of digital learning platforms. Approval within these systems can provide additional assurance that a product has been evaluated against state-level privacy, security and governance requirements.

For example, digital platforms approved for use within the New South Wales and Queensland government school systems have undergone formal review processes aligned with departmental security and data governance standards. For schools operating within those jurisdictions, such approvals can provide an additional layer of validation when assessing potential vendors.

Transparent Data Management and Privacy Alignment

Another indicator of a responsible EdTech provider is clear and structured data management.

Digital learning platforms routinely process personal information relating to students, which means vendors must identify what and how information is collected, stored and managed over time. Organisations with mature data governance practices typically document how data is handled throughout its lifecycle, including collection, storage, retention and deletion.

A key sign of this maturity is the application of data minimisation principles. In practice, data minimisation means collecting only the information necessary to support the educational purpose of the platform and avoiding the storage of unnecessary or excessive data. This reduces both privacy risk and the potential impact of any future security incident. For schools, this means understanding what data is collected, why it is required, and whether clear retention and deletion policies are in place.

Some providers align their privacy practices with internationally recognised regulatory frameworks such as the General Data Protection Regulation (GDPR) of the European Union. While GDPR is a European law, its principles around lawful processing, transparency, data minimisation and individual data rights have influenced privacy best practice globally.

For schools evaluating vendors, alignment with GDPR principles can provide additional assurance that student data is handled within a structured and well-defined privacy framework.

Responsible AI Oversight

As artificial intelligence (AI) becomes more common in digital learning platforms, responsible oversight of AI systems is emerging as another indicator of vendor maturity.

AI-enabled features can analyse student responses, generate feedback or support personalised learning pathways. When these systems process student information, organisations must ensure that AI functionality operates within the same security, privacy and governance controls that apply to the rest of the platform.

Increasingly, organisations demonstrate this commitment through formal AI governance policies or participation in recognised industry initiatives. One example is the Cloud Security Alliance's AI Trustworthy Pledge, an industry-led commitment designed to promote responsible and secure development of AI systems.

Signatories to the pledge commit to developing AI technologies in line with principles such as transparency, accountability, data protection and risk management. The initiative encourages organisations to embed security and privacy safeguards into AI systems, implement governance oversight for AI development, and ensure that AI-enabled features are deployed in ways that protect sensitive information.

Emerging frameworks are also beginning to formalise AI-specific assessment in education contexts. For example, the recent introduction of an AI module within the ST4S framework highlights a growing focus on evaluating how AI-enabled tools process, store and govern student data within school environments.

For schools evaluating digital platforms, public participation in recognised industry initiatives indicates that an organisation has committed to structured oversight of AI development and to aligning its practices with emerging global expectations for responsible AI use.

How to Evaluate an EdTech Provider's Data Security and Data Management

Independent indicators schools can use to assess whether a digital learning provider manages student data responsibly.

Indicator	What it is	How schools can verify it	What it means for schools
ISO/IEC 27001 Certification	An international standard for information security management systems requiring organisations to systematically manage and monitor information security risks.	Published certification statements (e.g. website or trust centre) and a current ISO certificate issued by an accredited body.	Provides assurance that the organisation manages student data through structured security governance and independently audited controls.
ST4S Assessment (Safer Technologies 4 Schools)	An education-sector framework that evaluates digital learning tools against privacy, security and data protection expectations relevant to schools in Australia and New Zealand.	Vendors listed in the ST4S Product Catalogue and participation in the ST4S Product Badge Program. Schools can verify products via st4s.edu.au .	Helps school leaders quickly confirm that a platform has undergone sector-specific review, reducing the burden of conducting individual vendor risk assessments.
State Education Department Approvals (e.g. NSW, QLD)	These assessments typically evaluate privacy practices, security controls and alignment with departmental data governance requirements.	Referenced on vendor website or procurement documentation. Schools can also confirm approval through their state department's approved supplier lists or procurement frameworks.	Shows the platform has passed formal review against state requirements. Even outside those states, it signals the provider has met compliance standards used by some of Australia's largest education systems.
Privacy Governance & GDPR Alignment	Structured policies governing how personal information is collected, used, stored and deleted, often aligned with internationally recognised privacy regulations such as the EU's GDPR.	Public privacy policies, documented data governance practices and alignment with recognised regulatory principles.	Provides transparency around how student data is handled throughout its lifecycle and supports responsible data management over time.
Responsible AI Governance (e.g. CSA AI Trustworthy Pledge)	Organisational commitments to develop and manage AI systems using principles such as transparency, accountability, data protection and risk management.	Public commitment to initiatives such as the Cloud Security Alliance AI Trustworthy Pledge and documented AI governance policies.	Signals that AI-enabled features are developed within a structured governance framework that protects student information.

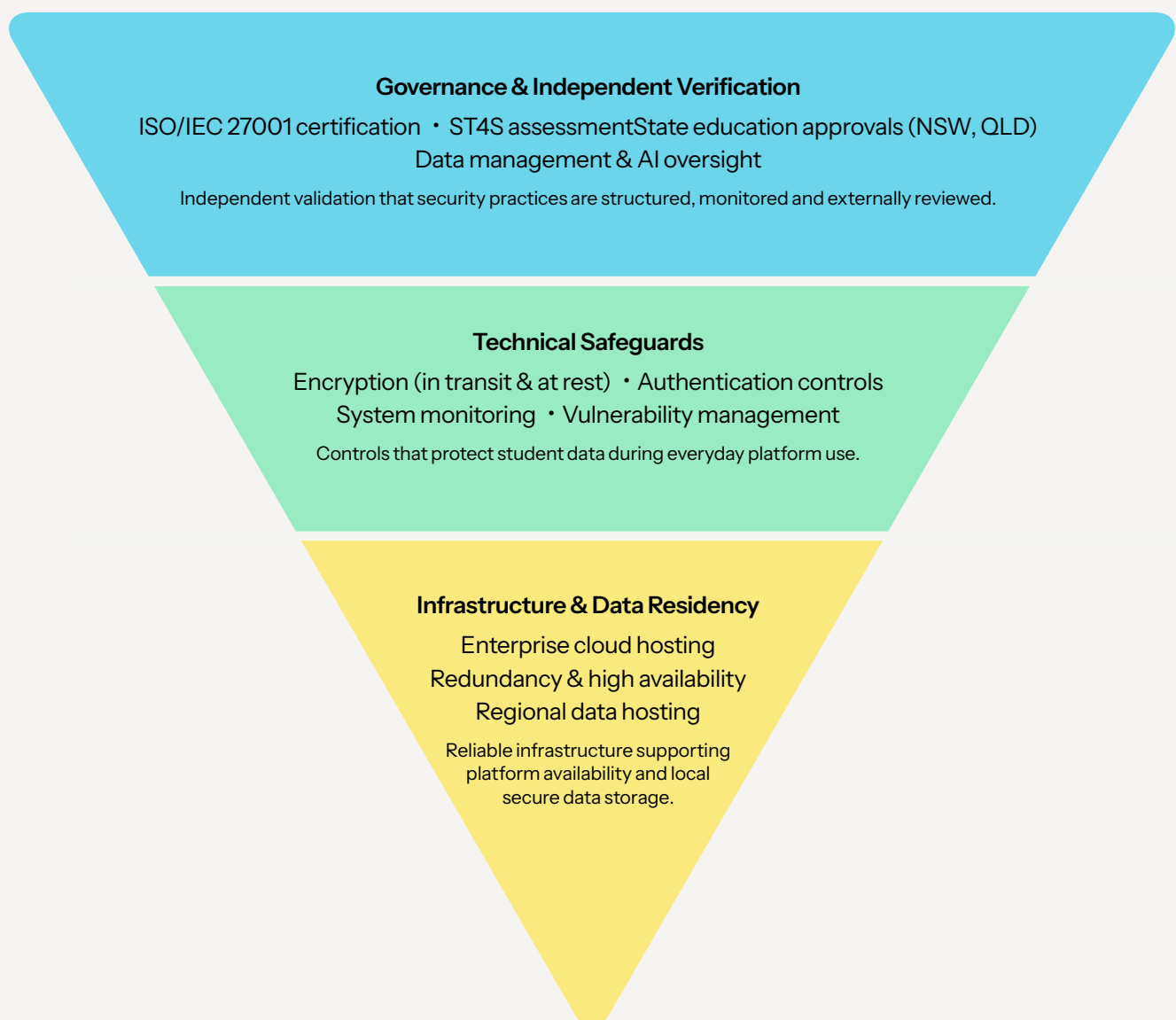
How Security Controls Work Together

In addition to independent validation and education sector assessments, schools should also consider how a platform's security controls operate in practice.

Mature technology providers typically implement security through multiple layers of protection, rather than relying on a single safeguard. This layered approach ensures that if one control fails or is bypassed, other protections remain in place.

A useful way to understand this model is through a simplified 'security stack', which illustrates how infrastructure, technical safeguards and the aforementioned independent verifications work together to protect student data.

The Security Stack: How Responsible Platforms Protect Student Data



Infrastructure, Data Residency and Performance

Many modern education platforms are hosted in secure cloud environments. This means data is stored in professionally managed, highly secure data centres rather than on individual school servers. These environments include physical security controls, system redundancy and continuous monitoring designed to support reliability and resilience.

This infrastructure supports not only secure data storage, but also consistent performance under varying levels of demand. In school environments, where platform usage can increase significantly during assessment periods, reporting cycles or system-wide events, the ability to scale without disruption is an important aspect of operational resilience.

For example, one platform (Education Perfect) supports more than 800,000 unique monthly users while maintaining 99.98% uptime. During the COVID-19 pandemic, when platform usage increased significantly, system performance and availability were maintained without changes to security controls. Schools should expect performance and security to operate together rather than as a trade-off.

Clear data hosting arrangements are also an important consideration. Understanding where student data is stored helps schools confirm that platforms align with regional privacy expectations and data governance requirements.

Performance Metrics Panel: Secure Performance at Scale

99.98%

uptime

800,000+

unique monthly
users

700%

usage increase managed during
COVID-19

Technical Safeguards

Above infrastructure sit technical safeguards. These include encryption, secure authentication, system monitoring and secure development practices.

Encryption protects information both while it is being transmitted, for example when a student submits work from a device, and while it is stored within databases. Secure authentication helps ensure that only authorised users can access information. Automated monitoring tools scan for vulnerabilities before they can be exploited.

Governance and Independent Verification

At the highest layer sit the governance and verification mechanisms discussed in Section 3, including independent security certification, sector assessment frameworks, documented data governance policies and AI oversight.

For schools evaluating EdTech platforms, the presence of these layered controls indicates that student data protection has been designed into the platform architecture rather than added as an afterthought.

The Security Stack in Practice: A Case Study

The previous sections outline key independent indicators that schools can use to evaluate whether an EdTech provider manages student data responsibly, along with how layered security controls work together in practice.

The following graphic provides a practical example of how infrastructure, technical safeguards and governance mechanisms operate together to protect student information in a school environment.

Education Perfect's Security Stack

Governance & Verification	✓ Independent Certification ISO/IEC 27001:2022 certified. Independently audited information security management system with ongoing surveillance and recertification.	✓ Education-Sector Assessment ST4S listed and holds the ST4S product badge. Assessed against privacy and security criteria relevant to Australian and New Zealand school environments.	✓ State-Level Validation Approved for use in NSW and QLD government school systems. Meets state-specific privacy, security and data governance requirements.
Governance (Data & AI)	✓ Data Governance & Privacy Practices Structured data governance supported by documented policies, including data minimisation, data lifecycle management, controlled access and alignment with recognised privacy principles such as GDPR.	✓ Data Residency Student data for AU/NZ schools is hosted in Sydney. Provides clarity on where data is stored and supports regional privacy expectations.	✓ Responsible AI Governance Signatory to the Cloud Security Alliance AI Trustworthy Pledge. AI features developed within a framework emphasising transparency, accountability and data protection.
Infrastructure & Technical Controls	✓ Secure Cloud Infrastructure Hosted on enterprise-grade cloud infrastructure (Amazon Web Services - AWS) designed for reliability, monitoring and resilience.	✓ Redundancy & High Availability Built-in system redundancy supports continuity of learning during peak demand or unexpected disruption.	✓ Secure Access & Monitoring Controls Role-based access, system monitoring and vulnerability management protect data during everyday platform use

This can equally be illustrated from a teaching and learning perspective. The following diagram illustrates how student data is protected as it moves through the Education Perfect platform, from initial submission through to storage and controlled access.

The Education Perfect Student Data Journey



Student input: assessment submission or login

Data minimisation principles applied — only information required for the educational purpose is collected.



Encrypted data transfer

Protected while moving across networks



Regional cloud infrastructure (Sydney)

High-availability, redundancy and data hosted locally, supporting regional privacy requirements and data governance expectations



Encrypted at rest

Secure databases and backups



Role-based access controls

Data accessible only to authorised users



Buyer's Checklist: Evaluating EdTech Vendors' Data Security and Data Management

Selecting an EdTech provider requires more than reviewing features or classroom functionality. It involves assessing whether the platform can be trusted to manage student data in a secure, compliant and well-governed way.

The following checklist is designed to support that process, providing a structured set of criteria that school leaders, boards and IT teams can use to assess EdTech vendors. It brings together the key considerations outlined above: independent verification, technical safeguards, and infrastructure along with the practical questions schools should ask when evaluating digital learning platforms.

Schools should expect clear, evidence-based answers.

Schools should prioritise independently verifiable evidence over vendor claims.

EdTech Buyer's Checklist

Independent Validation

- Is the provider independently certified to ISO/IEC 27001 or an equivalent internationally recognised standard and can this be verified through a current certificate?
- Has the provider been assessed through education-specific assurance frameworks, such as ST4S, and can its status be confirmed via the ST4S Product Catalogue?
- Is the platform formally approved within relevant state education systems (e.g. NSW, QLD)?

Data Management & Privacy

- What student data is collected and is it limited to what is necessary for the educational purpose (data minimisation)?
- Is there a clearly documented data lifecycle policy, including how data is stored, retained and deleted?
- Where is student data hosted and processed, and does this align with regional data residency expectations?
- Does the provider demonstrate alignment with recognised privacy frameworks (e.g. GDPR principles)?

AI Oversight

- Are AI features within the provider's existing security and privacy framework?

- How are student inputs used within AI systems and are they excluded from training external or public models?
- Does the provider have a documented AI policy?
- Has the provider committed to recognised AI governance principles (e.g. industry or government frameworks)?

Infrastructure & Performance

- Is the platform hosted on enterprise-grade cloud infrastructure with built-in redundancy and high availability?
- What is the platform's historical uptime, and can this be evidenced?
- Can the provider demonstrate reliable performance during peak usage periods (e.g. assessments, reporting cycles)?
- Is there evidence that security controls operate effectively at scale, without degradation of performance?

Technical Safeguards

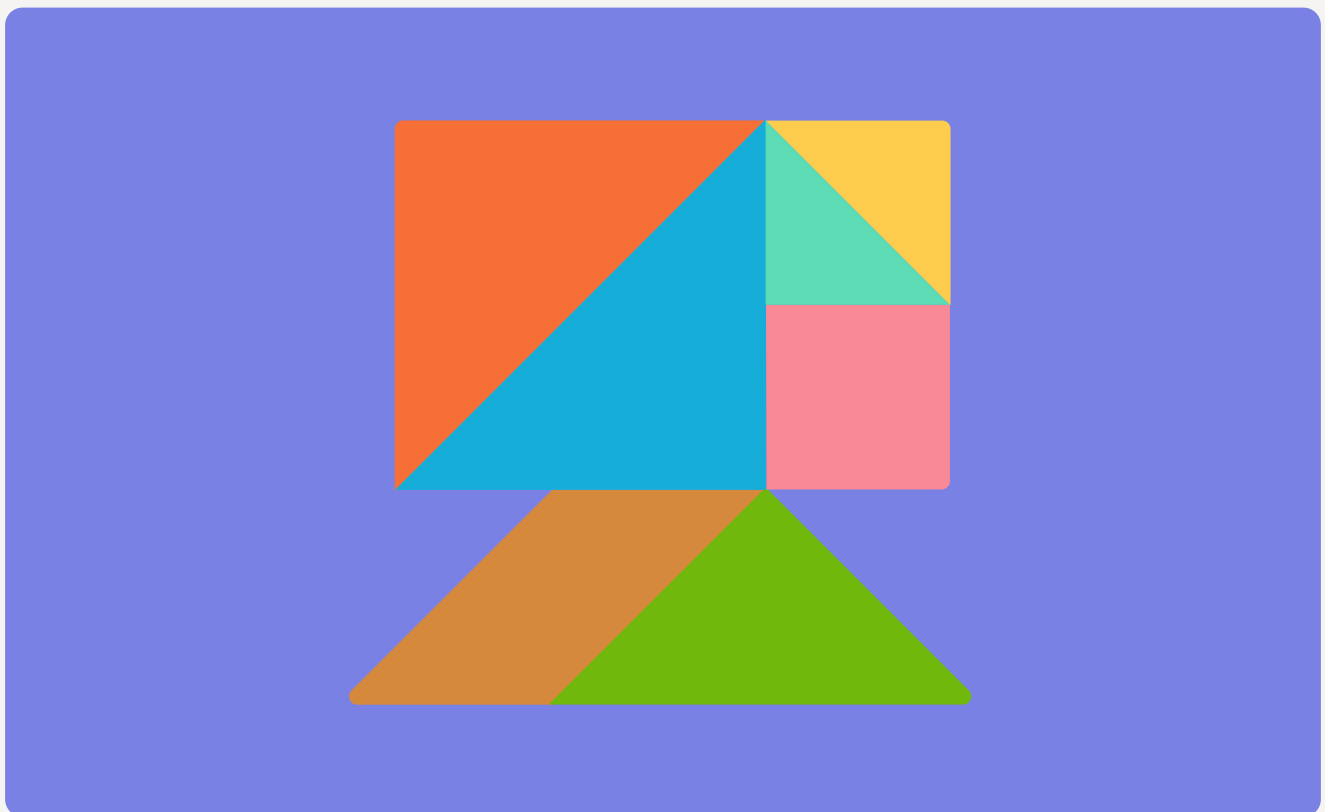
- Is data protected both in transit and at rest through encryption?
- Are role-based access controls and authentication mechanisms in place to restrict access to authorised users?
- Are monitoring, vulnerability management and incident response processes in place and documented?

Conclusion

As digital learning platforms become more embedded in teaching and assessment, the way schools evaluate technology providers is evolving. Alongside functionality and educational outcomes, there is an increasing expectation that platforms can demonstrate clear, verifiable approaches to managing student data.

In many ways, this is no different to how schools evaluate physical learning resources: considering not only their effectiveness, but their suitability, reliability and alignment with broader school responsibilities.

By focusing on independently verifiable indicators and asking the right questions, schools can make more informed decisions about the digital learning platforms they adopt, supporting effective learning outcomes while ensuring the responsible handling of student information.



Get in touch

🌐 educationperfect.com

f [educationperfectnz](https://www.facebook.com/educationperfectnz)

✂ [epforlearning](https://www.x.com/epforlearning)

in [educationperfect](https://www.linkedin.com/company/educationperfect)

@ [educationperfect](https://www.instagram.com/educationperfect)

