Safeguarding Student Data for the Future

Keeping the Education Industry Available

Contents

Safeguarding Student Data for the Future

Keeping the Education Industry Available

Digital transformation has significantly impacted the education industry, opening new learning possibilities to students and streamlining admin processes for teachers and principals. Students now have access to an abundance of online information, and the adoption of cloud technologies means that schools no longer face the challenge of access to information. E-learning is encouraged through Microsoft Office 365 and Google Classrooms, staff are taking digital roles; creating paperless classrooms, writing reports and marking students work through programs such as SchoolPro and Kiddom.

However, the adoption of new technologies does not come without its challenges. Australian schools are facing new complexities when it comes to safeguarding the personal data for both staff and students.

IT professionals in schools are now faced with the prospect of exponential data growth, understanding how to manage it, where to store it, what to keep and what to destroy all whilst adhering to privacy and data compliance regulations specific to each state. Tangentially, they also are tasked with communicating a school's Availability needs to principals, school boards or parents in order to ensure appropriate budget and resource is allocated to adequately protect the school.

This report aims to explore the issues faced by IT professionals in schools around Australia and New Zealand when it comes to keeping data available. It will unpack the challenges that come with making data available in schools, improving student outcomes, remaining compliant, and keeping students safe and secure.

Improving student experience

Continual advances in technology are changing the way students need to learn, connect and interact. STEM (Science, Technology, Engineering & Mathematics) is providing a foundation for students to succeed at school and beyond.

Schools are adopting a paperless classroom approach and relying on tablets and online classrooms to empower students to achieve more. Qualitative and quantitative data can help educators to identify pinch points in a student's learning, observe patterns of progress or stagnancy across subjects and as such, empower teachers to make changes at a classroom level to improve student outcomes.

Comparing student performance or growth data across years or between classes allows teachers to observe differences in practice — if all the information was collected in the same way each time. For example, the data may indicate that students in one class understand a topic more thoroughly than another. This allows teachers to work collaboratively and share best-practice principles across lessons to create a more consistent learning experience that improves results.

Backing up students work

Student data is being collected all the time and it's not just to adhere to legislative obligations, it can also be used to improve the overall student experience. Captured data will not be beneficial if it is not used. Data collected on students, staff and teachers may be highly personal or sensitive. This could include student performance data, demographic characteristics, or responses to surveys. Schools should operate openly and transparently by informing all participants on how the data will be collected, how it may be used and who will have access to it.

For schools using Microsoft Office 365, there is a general misconception that Microsoft is responsible for the backup and retention of their data. Put simply, Microsoft is not the data owner. Microsoft Office 365 will provide best attempts to recover from an incident (disruption or data loss), but data ownership and the liability of recovering from data-loss sits with the institution collecting the data, such as schools.

Microsoft Office 365 offers geo-redundancy, which is often mistaken for backup. Backup takes place when a historical copy of data is made and then stored in several locations, so if data is lost, accidentally deleted or maliciously attacked, for example, there will be an easily accessible copy elsewhere. Geo-redundancy on the other hand, only protects against site or hardware failure, so if there is some type of infrastructure crash or outage, students can continue to use the program.

In the event of a malicious attack, human error or even natural disaster, schools need to make sure data is protected. For students, working on major group assignments and teachers working on perfecting curriculums in collaboration platforms like SharePoint, the loss of data is not an option. Ultimately, schools need to ensure that staff, and in some cases students, have access to, and control over, their data. By providing critical functionality such as the ability to retain data, quickly restore mailboxes, messages and documents and retain data on premise, backups can ensure schools continue to operate efficiently whilst providing peace of mind to students and staff that their work, data and personal information is safe and recoverable.

Compliance — adhering to legal obligations

A number of IT professionals in schools are not aware of the legislative requirements behind data protection and record keeping. As record keeping becomes increasingly digital, this should be a main priority. Aside from suffering reputational damage for the deliberate destruction of documents, a school's officers could be found criminally liable for such actions. Under the Crimes Act 1914 (Cth) and corresponding State legislation, it's an offence to intentionally destroy documents that a person knows are, or may be, required as evidence in a judicial proceeding in order to prevent them being used in a court proceeding. [1]

There is also a huge grey area in understanding what is considered to be 'destroying documents' with no clear guidelines available to help IT managers navigate this issue. For example, the average length of time from data compromise to discovery is over 140 days, yet Microsoft's default settings mean data is permanently deleted between 30-90 days. It then becomes the school's responsibility to ensure this data is backed up and recoverable.

The suggested retention periods of student data will vary from state-to-state and is dependent on what type of data a school is collecting. As an example; in Victoria, schools are only required to hold information regarding a student's medical details and parental

information for one year after a student leaves that school. Contrastingly in ACT and NSW, the same data is held onto for seven years or until a student reaches the age of 25 — whichever is later.

In New Zealand, there is a requirement to keep enrolment records & daily attendance registers for seven years but records around withdrawal registers, punishment records (eg: suspension or expulsion) and significant awards or honours are to be kept indefinitely.

Non-government schools are not tied to the same regulations as government schools and have the autonomy to create, manage and implement their own regulations around data retention. This can be challenging for some schools but the general recommendation from governments is for non-government schools to use the state policies as a strong guideline.

Data retention used to be more complicated than it currently is, with schools having to house all relevant information on paper records and in boxes on site. Today, thanks to significant developments in digital technology, public school records around Australia & New Zealand are being recorded quickly, easily and with lesser risk of loss or misplacement. For schools choosing the digital solution, it is important to ask if these records require a back-up or to be kept available. In an instance where a school data centre might catch on fire or be destroyed in a natural disaster, schools need to ensure they're equipped with the technology that can recover this data.

Protecting students

In 2012, the Australian Government issued the Royal Commission into Institutional Responses to Child Sexual Abuse. The commission was the longest running in history, running for eight years and delved into purported instances of child abuse within the Catholic Church and other institutions over years.

The report heard the testimonies of more than 8,000 survivors of child sex abuse. Just months after the Australian Royal Commission issued its final report, New Zealand announced its own investigations into child sex abuse in state care and faith-based institutions. Though the investigations have been delayed, they're scheduled to begin this year.

In Australia it is worth pointing out that regulations have been temporarily tightened in light of the Royal Commission. As a result of this, the Australian government issued a disposal freeze on student data and information in 2013. The freeze is still in action and will be until the Government announces otherwise. The purpose of the records disposal freeze is to assist in the identification of Commonwealth records that are likely to be required by the Royal Commission. To put it simply, the disposal freeze suspends the National Archives of Australia's permission to destroy any relevant records that could otherwise be legally destroyed under current records authorities.

The freeze includes a very in depth and varied set of data formats including: paper, tapes, audio and visual recordings, photos, digital records, emails, word documents, shared workspaces, local and personal drives, thumb drives and laptops or other devices. The freeze also covers databases, digital business, case management and workflow systems. Even SMS, social media posts and personal notebooks. It is now a legal requirement for all records in digital formats, including information in databases and other digital business systems, to be maintained with all the necessary metadata to support retrieval and access to authentic and reliable information.

Case study quotes

"Having Availability is paramount not only to student's learning but also in regard to administrative support, payroll, finance and alumni services. We found, with Veeam® Backup Essentials™, we could consolidate our disaster recovery and availability of resources under the one umbrella."

Yugon Chobanoff
ICT Operations Manager
John XXIII College

"With Veeam, the certainty that data is being backed up and restored gives us a critical assurance of visibility and reliability. If we were to lose anything, that would be a major drama for the community of teachers, students, parents and alumni that we serve. But with Veeam we just don't have that kind of Availability nightmare. It provides us good visibility and reports that we can feel comfortable. If anything pops up we get the alerts, know what the problem is and what to do to fix it. And if we can't fix it, we can rely on the 24/7/365 support from Veeam."

Winston Mattson
Director of Systems & Infrastructure
Ivanhoe Grammar School

About Veeam Software

Veeam is the leader in Backup solutions that deliver Cloud Data Management™ in schools around Australia and New Zealand. Veeam Availability Platform™ is the most complete backup solution for helping schools on the journey to achieving success in the Five Stages of Cloud Data Management. Veeam has 343,000+ customers worldwide, including 82% of the Fortune 500 and 67% of the Global 2,000, with customer satisfaction scores at 3.5x the industry average, the highest in the industry. Veeam's global ecosystem includes 64,000 channel partners; Cisco, HPE, NetApp and Lenovo as exclusive resellers; and 22,500+ cloud and service providers. Headquartered in Baar, Switzerland, Veeam has offices in more than 30 countries. To learn more, visit https://www.veeam.com or follow Veeam on Twitter @veeam.

For more information on how you can keep your school available and protected, please reach out to your Veeam Account Manager or https://www.veeam.com/contacts.html

VEEAM

Cloud Data

Backup for what's next

5 Stages of Cloud Data Management –
start your journey today!