Defending your data

NICK BARBAGIANNOPOULOS, DIGITAL AUTOMATION & SOLUTIONS MANAGER FOR RICOH AUSTRALIA, ADDRESSES WHAT THE NOTIFIABLE DATA BREACHES SCHEME MEANS FOR SCHOOLS – AND WHAT THEY NEED TO DO ABOUT IT.

Australia's new Notifiable Data Breaches (NDB) regulations came into effect on February 22, however many schools are still struggling to come to terms with the implications.

Designed to ensure better protection of personal data held by private and public-sector organisations, the regulations lay down clear guidelines for what must happen in the case of a data breach. If the data loss could result in serious harm for the individuals involved, those individuals must be notified as soon as the breach is uncovered.

The new laws have significant implications for schools as they regularly collect and store large amounts of personal information relating to both students and staff. Collected in both printed and electronic form, this data could include everything from contact details and banking information to photos, videos and medical records.

It might be tempting to think that breaches of such information can only occur through hacking or cyberattacks against a school's IT infrastructure, but this is far from the case. It's much more common for breaches to happen as a result of human errors or a failure to follow information handling policies.

For example, a breach that meets the NDB criteria could be the loss or theft of a laptop on which is stored the personal information of a teacher or group of students. Alternatively, it might be as simple as personal information being inadvertently provided to the wrong person, or student records being stolen from an unsecured waste paper bin.

Once a school becomes aware that a breach has occurred, a detailed statement must be prepared for any people affected. This statement must set out a description of the breach that the school believes has happened, the nature of the information lost, and recommendations about the steps the affected individuals should take.

Failure to comply with the new NDB rules can be costly for a school. Monetary penalties will apply and are up to $360,000 for individuals and $1.8 million for organisations. Clearly, if a school should fail to meet its obligations, the impact to its annual budget could be significant.

HOW TECHNOLOGY CAN HELP

Ricoh has been a trusted technology partner in the education sector for many years. Working closely with schools across Australia, the company has a clear understanding of the issues they face and the most appropriate technology solutions they can adopt.

When it comes to compliance with the NDB regulations, Ricoh has a range of solutions that can ensure schools are best placed to meet their obligations. These include:

• Digital automation:

While computers have changed the way schools operate, there is often still a heavy reliance on paper documents. Everything from student files and academic results to budgets and financial records are regularly stored in paper form.

Ricoh offers a robust, easy-to-use document and records management platform that can assist a school migrate its printed data into the digital realm. Documents can be efficiently scanned, categorised and stored on dedicated servers located on the school campus. For additional security, this data can also be backed up to a cloud platform to ensure nothing is lost should problems occur in the local infrastructure.

From an NDB perspective, shifting stored information from paper to digital form reduces the chance of it being accessed inappropriately or falling into the wrong hands. Records can be stored securely based on state-based regulations, further improving the level of data security within the school.

• Secure printing:

Even if a school is successful in migrating its data stores to a digital platform, there will continue to be a need to print some documents. Student records might be needed for a planning session or financial charts required for a management meeting.

To ensure printed documents are only accessible by the person who creates them, Ricoh offers a 'follow-me' print solution. Users send a document to a nearby printer, but it is not actually produced until that user enters a code into the device or swipes their access pass.

This means the user must be at the device for the document to be printed, thereby reducing the chance that sensitive information be left in the output tray or collected with other printed output. In this, way the security of information on paper throughout the school can be significantly improved.

Embedded Security

Managing devices can be a time-consuming activity for school IT departments. Indeed, the networked nature of school IT infrastructures can make them vulnerable to attack and compromise.

As data moves through the network, it is possible for a knowledgeable hacker to intercept raw data streams, files and passwords. Indeed, data sent in a print stream can be exploited if unencrypted and captured in transit.

Ricoh uses a number of techniques to help protect against threats, including authentication, end-to-end encryption of print and scan files, encryption of data on servers and segregation of administrator duties. Ricoh's multi-function devices also use a digital signature to judge firmware validity. In addition, a range of security services and managed services can also monitor, optimise and effectively manage document and information security.

• Secure administrative processes:

Schools regularly request and obtain sensitive personal data relating to students from parents. This could be anything from updates on medical conditions to details of extra-curricular activities and events.

To allow this data to be collected, processed and stored securely, Ricoh offers an internet-based portal platform. Parents can enter required information via the portal which is connected directly to the school's central administration infrastructure.

In this way, data relating to everything from student enrolment applications to permission forms and incident reports can all be retained in digital form and stored securely behind the school's firewall. This significantly reduces the chances of a data breach that would invoke the penalties associated with the NDB regulations. Also, it can help to remove a number of currently paper-based processes and improve overall administrative efficiency.

• Secure IT infrastructure:

Modern schools are heavily reliant on both wired and wireless networks to allow staff and student to access the applications and data they need on a daily basis. With the number of cyberattacks on the rise, ensuring this infrastructure is secure at all times has never been more important.

Ricoh works with schools to consult, design, build and manage IT infrastructures that meet their needs for performance and flexibility while also being secure. Teachers can use the network to access curriculum details, create lesson plans and connect with their peers. Equipped with mobile devices, students can access academic materials, complete tests and interact with other students.

Cloud-based solutions can also be added to the mix. Rather than having to establish, manage and maintain growing racks of server and storage infrastructure, a school can instead purchase capacity from a cloud provider. Then, using the high-speed networks, teachers and students can securely access resources on any device and from any location.

When considering the NDB regulations, it becomes clear that maintaining security of this infrastructure has never been more important. Ricoh can work with schools to manage school networks to ensure data is only accessed by authorised parties. Should an incident occur, the school can be immediately notified.

By adopting these types of solutions, a school can be confident it has the systems and processes in place to reduce the likelihood of suffering a notifiable data breach and the implications this can have. Attention can instead remain on the most important facet of any educational institution: the students.

Article published in **Education Matters Secondary** (May 2018)