95% of schools may not be POPI Act compliant

Schools are increasingly embracing the digital universe and now the Covid-19 pandemic has stratospherically accelerated the adoption of online communication and digital strategies for South African schools. Out of pure necessity, as school gates shut in March, many schools made the agile pivot to online education, as well as intensive online communication with learners and parents alike.

Source: pixabay.com

But dangerous risks are emerging as schools take this online leap and parents should be sure to ask important questions, such as:

Is personal information held by the school safe?

Schools hold a vast amount of private information on their learners and their families. This can include anything from their home address, parents' occupations, work name and address, ID numbers, bank account details for debit orders, the number, age and name of children in the family, closest relatives, telephone numbers, health conditions and more.

Secondly, ***Do schools have the systems in place and defence mechanisms to keep learners' and parents' details secure?***

Thirdly, ***Are schools abiding by the laws which require them to protect our privacy, such as the Protection of***

Personal Information Act (POPIA)?

Some experts have warned that up to 95% of schools may not be POPIA compliant.

Willem Kitshoff, CEO of the d6 Group, a South African online school management platform - used by more than 2,500 schools around the country, says that not all schools are harnessing smart technology – which is leading to increasing concerns about data security.

“There are so many advantages to the adoption of online strategies and the increasing use of digital platforms to improve a wide range of relationships within school communities. But school communities comprise real people, with real rights - who also need to be protected online. So it’s essential to balance speed, efficiency and ease-of-communicating with very best security and privacy protocols.”

Ross Saunders, a specialist in data privacy and cybersecurity, explained some risks to parents and learners.

> *“Information that is insecurely stored carries a tremendous risk of being leaked out. Once information is leaked, it’s like toothpaste from a tube. Risks to the person who the data belongs to would likely be identity theft, fraudulent transactions, and extortion.”*

For schools, Saunders advised, there are further potential concerns: “Risks to the school would most certainly be reputational damage, but under POPIA there would likely be an inclusion of fines, civil liability (being sued) or both. Schools can also be held to ransom for the information they hold, should a ransomware attack occur due to insecure practices.”

What should parents and schools do?

“Parents should be asking questions around the security of platforms in use by the school, as well as any other manual processes within the school. Parents should hold schools accountable for the way the school stores, processes, and retains information and individuals have the right under POPIA to request a breakdown of what information a school holds about them and their children, and schools are obliged to provide the information,” advises Saunders.

“Schools, in turn, should only keep the minimum information required to fulfil their obligations, and ensure that this information is stored securely whether it’s in electronic or physical form.”

On the management front, many School Governing Bodies (SGBs) take on much of the responsibility for deciding what systems their schools adopt. Saunders explained: “Part of the law is to ensure that security safeguards are in place when it comes to data. The SGB should focus on the school’s policies and procedures, ensuring that secure practices are in use and that privacy is front-of-mind.”

“Cybersecurity and network security are critical for electronic data, while access control and physical security measures need to also be addressed for hard-copy information. SGB’s need to review the processes and any data transfers, satisfying themselves that security and privacy has been considered within a school’s day-to-day operations.”

Kitshoff says both schools and parents are well-advised to interrogate the systems in place at their own school, to ensure they protect and comply.

“d6 has developed a range of digital services for schools that are all highly secure and fully POPIA compliant. We realised the vital need to protect all of the information that schools hold and our fully integrated school administration system, financial management facility, digital and online communication platforms, as well as the d6 cashless services are all rigorously maintained with security in mind and the protection of information.”

Kitshoff ended with this assurance: “The digital school revolution is inevitable and exciting. These important issues around

data protections may look complicated, but in partnership with the right experts, schools can walk a healthy line between expanding their online presence fast, while still maintaining strict, careful curatorship of every piece of information in their care.”