State Privacy Office
September Privacy Tip

Back to the Classroom: Student Data Security Tips to Remember

A new semester has started, and students of all ages are back in class, either in person or through remote learning.

If there is anything the last few years have taught the educational system, it is that technology can be both a great blessing and a great curse. For many schools, since the pandemic meant expanding their digital attack surface overnight. Suddenly, students, teachers, and administrators were accessing data and communicating from hundreds or potentially thousands of home networks.

What Schools Can Do:

Schools are in a vulnerable position, as they handle large amounts of private information for students. Beyond merely grades and test scores, schools maintain medical records, addresses and sensitive data such as social security numbers, financial documents, and potentially legal records and releases. Schools *must* take steps to secure this data to protect their students.

- Train staff and teachers to identify phishing emails, suspicious links, and other social engineering tactics. Ensure that all members of the organization know who to contact when they receive suspicious communications.
- Craft a clear protocol for dealing with data security, breaches, and cyber threats. This should include a Mobile Device Use Policy that addresses school-owned devices, as well as teachers' personal devices they use for work.
- Regularly update authorization lists and know which people and what devices have access to secure networks or resources.
- Use an encrypted email service for school communication.
- Allocate funds to enable IT personnel to take the proper steps to protect the school's networks and servers.

What IT Departments Can Do:

School IT departments must appropriately use the means at their disposal to execute a data defense strategy. When limited by time and resources, it can be helpful to use vetted solutions that streamline or automate security processes.

- Encrypt all servers and devices that have access to school and student data.

- Update and patch software and programs on school devices regularly.
- Monitor for suspicious activity by utilizing an Intrusion Detection System (IDS) and a device location tracking service.
- Use an MDM or endpoint security software that allows IT administrators to protect devices remotely by locking or wiping the device.

What Parents and Teachers Can Do:

Software solutions and strong device security policies provide a reasonable defense against threat actors. However, they cannot fully address the human element of digital risk. Parent and teacher involvement is crucial. An understanding of modern cybersecurity practices is the keystone of effective data and privacy protection.

- Individuals should maintain good password hygiene. This includes using strong and unique passwords, changing them regularly, and not storing them in plain text.
- Update personal devices and antivirus software regularly.
- Maintain a secure home office or remote learning environment for your children.
- If you must travel with your devices for work, or have children who will be attending school remotely, endeavor to keep the devices secured and out of sight when not in active use to limit the chance that an unauthorized user will access them.
- Most importantly, teach children healthy cybersecurity habits and emphasize the importance of digital privacy.

Schools, teachers, and parents have a responsibility to educate children and keep them safe. Knowledge is power, and the more active a role that students take in maintaining their own data security, the safer they will be not only for their academic careers, but for the rest of their lives.

Note: *Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.*