Cybersecurity Practices for Schools

FIVE PRIORITIES to Establish a Culture of Digital Responsibility & Safety

As technology becomes an integral part of education, schools are increasingly vulnerable to cyber threats. Cyberattacks on educational institutions can compromise sensitive student information, disrupt learning, and strain resources. Here are the top five cybersecurity priorities that every educational organization should consider to expand their culture of digital responsibility and safety.

1

MULTI-FACTOR AUTHENTICATION (MFA)

Reduce the chances of unauthorized access, protecting school networks from hackers even if passwords are compromised.

With the rise of cyberattacks like phishing, relying solely on passwords is no longer sufficient to protect school data. Multi-Factor Authentication (MFA) adds an extra layer of security by requiring users to verify their identity through two or more authentication methods—typically something they know (password), something they have (a device or token), or something they are (fingerprint or face recognition).

Practices:

- Start by enabling MFA for critical systems such as email, learning management systems (LMS), and student information systems (SIS).
- Encourage staff and students to activate MFA on personal devices and school accounts.
- Partner with your IT team to simplify the MFA setup process and provide support for troubleshooting.

2

AWARENESS TRAINING FOR STAFF AND STUDENTS

When staff and students are aware of potential risks, they can actively participate in securing the school's digital environment.

Humans are often the weakest link in cybersecurity. Phishing scams, malware, and ransomware are usually triggered by someone unknowingly clicking on a malicious link. Continuous cybersecurity awareness training ensures that staff and students can recognize these threats and know how to respond.

Practices:

- Conduct regular workshops and training sessions on cybersecurity best practices, focusing on email security, social media risks, and safe internet usage.
- Integrate cybersecurity topics into the digital curriculum for students.
- Use phishing simulations to test staff and students' awareness levels and adjust training based on results.

3

ASSET MANAGEMENT

Organizations can identify and address vulnerabilities in their systems, preventing unauthorized access to critical resources.

Schools often have a wide range of digital assets, including computers, tablets, servers, and software. Without a clear inventory, it's difficult to monitor what needs protection, leaving gaps that cybercriminals can exploit.

Practices:

- Create an up-to-date inventory of all school-owned hardware, software, and data.
- Ensure that all devices are properly maintained, receive security patches, and are monitored for vulnerabilities.
- Assign responsibility for managing these assets to specific IT staff, ensuring accountability and oversight.
- Create role-based access to data based on the principles of least privilege.

4

CONTINGENCY MANAGEMENT PLANNING

Ensure that your school can quickly recover from cyber incidents with minimal disruption to operations, safeguarding students' education and personal data.

Cyberattacks and data breaches can happen despite your best efforts. A robust contingency management plan prepares your school to respond quickly and minimize the impact of an attack.

Practices:

- Develop a detailed incident response plan that outlines the steps to take in the event of a cyberattack, including roles and responsibilities for key personnel.
- Establish protocols for communication with staff, students, and parents if a breach occurs.
- Ensure your plan includes a strategy for data backup and recovery to minimize downtime and data loss.

5

CONTINGENCY MANAGEMENT TESTING

Highlight any weaknesses in the response plan, allowing for continuous improvement.

A plan is only effective if it works in practice. Regularly testing your contingency management plan ensures that your team knows how to execute it under real-world conditions.

Practice:

- Conduct regular cybersecurity drills, simulating different attack scenarios such as ransomware, data breaches, or denial-of-service (DoS) attacks.
- Involve staff, IT teams, and administrators in these tests to ensure everyone is familiar with their roles.
- After each drill, conduct an after-action review and refine the contingency plans based on what worked and what didn't.

DR. ANDREA TEJEDOR
BLUUM EDUCATIONAL STRAGEGIST

"As cyber threats evolve, school leaders must be ***proactive*** *in safeguarding sensitive data and ensuring that students, staff, and the broader school community remain safe online. By prioritizing cybersecurity, school leaders can prevent disruptions, protect valuable information, and create a* ***secure learning environment for all."***

Learn more about Bluum's Research and Planning Services.
Education@bluum.com

bluum™