PowerSchool

DIGITAL CHECKLIST:

How is Your District's Data Protection Culture?

ASSESS YOU CULTURE OF DATA PROTECTION WITH YOUR KEY STAKEHOLDERS BY ASKING THESE QUESTIONS

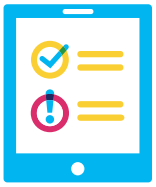
Data security is a white-hot topic, and for good reason. Cybersecurity threats and attacks have skyrocketed with the shift to online teaching, learning, and operations. The results can be disrupted operations, harm to students and staff, and compromised IT infrastructure.

With a significant increase in online users, devices, and potential openings for attacks, it's critical to get everyone on the same page to ensure your highest level of security. To get there sustainably, you need a **culture of data protection**. Tech leaders can shore up internal systems and infrastructure, but creating a culture—with students, parents, teachers, administrators, and IT staff all dedicated to one goal—ensures your data security into the future.

A solid culture is built on:

Continual education

Secure tools and infrastructure



Smart planning

Train your users to boost your human firewall, provide best practices and secure edtech products, and create a plan for handling attacks when they occur.

Use this helpful guide to assess your data protection culture and to see where you need to boost your efforts.

Start with a Security Audit

Build your culture of data protection on a solid foundation. Your IT department should assess your system and best practices every 6 months.

OUR SCHOOL OR DISTRICT:

- ☐ Completes a third-party security audit every 6 months to examine current processes, procedures, and infrastructure
- ☐ Knows how our technology infrastructure is laid out, including the physical and virtual resources that support the flow and storage of data
- ☐ Has a holistic view of vulnerabilities, with a complete understanding of which improvements need to be made, and a plan to complete them
- ☐ Educates our schools and district on training needs and IT infrastructure resiliency

0 **/4 Number of Boxes Checked**

LEARN MORE: Is Your District Ready for Cybersecurity Threats? >

Training for School and District Personnel, Students, and Families

Investments in training your "human firewall," or users, can keep security fresh in their minds and greatly reduce the chance of having a security incident.

OUR SCHOOL OR DISTRICT:

- ☐ Trains everyone on basics:
  - **Common threats:** social, hacking, and malware
  - **Best practices:** password management
  - **Phishing:** training courses and simulations, including an age-appropriate definition of attacks and scams so they'll know how to handle suspicious email or online messages
  - **Rules for accessing confidential work** on unsecured networks (with public Wi-Fi access)
  - **Reporting:** How to report a security threat
- ☐ Teaches good digital citizenship—offering practical guidelines and policies, including the importance, best practices, and examples of being responsible with software, devices, and platforms
- ☐ Has defined "personal information," instructing students not to share it online without asking a parent first
- ☐ Offers multiple ways to learn cybersecurity, through courses and resources like email newsletters and lunchroom posters
- ☐ Continues to teach through repetition, reminders, and patience

0 **/5 Number of Boxes Checked**

LEARN MORE: Learn How Cybersecurity Awareness Training Can Protect Your School District >

Preparing for What to Do When Attacks Happen

Create culture within your IT team and expanded incident response team by preparing an action plan. Make sure it's communicated out to stakeholders before attacks take place.

OUR SCHOOL OR DISTRICT:

- ☐ Communicates how to report cybersecurity attacks. An example is for phishing attempts—you can create a dedicated email address to forward suspected phishing attacks
- ☐ Has a transparent response process to attacks involving students: what are your immediate and long-term steps when you are attacked to minimize risk to students?
- ☐ Anticipates the unexpected with a clear plan in place: an example is using the PICERL process (Preparation, Identification, Containment, Eradication, Recovery, and Lessons) as a best practice to prepare for each step of any security risk. Here's an example:
  - **Preparation:** Training for key response team members and establishing a "war room" in case of threats. Have in place out-of-band communication strategies and standardized tools which are ready for use during an incident.
  - **Identification:** Procedures for logging, reporting, and validating events, collecting evidence, and ways to properly declare and classify an incident.
  - **Containment:** Short-term and long-term containment strategies, including guidance on determining the risk of continued operations. Have details guiding integration with the business change control process.
  - **Eradication:** Position your team to determine the root cause and symptoms of any incident and how to improve defenses, with directions on performing vulnerability analysis.
  - **Recovery:** Prepared to move forward based on the findings from the eradication activities. Recovery activities also incorporate monitoring and validating systems to ensure that the incident has been fully remediated and that there are no further indications of infection within the environment.
  - **Lessons Learned:** Once an issue is resolved, review the response activities with your Incident Response Team to identify and notate what worked well and what went wrong.
- ☐ Practices and tests the plan regularly

0 /4 Number of Boxes Checked

LEARN MORE: K-12 Data Security Tips from a CISO >

ON-DEMAND WEBINAR

Understand Cybersecurity Threats

Hear more from PowerSchool's Chief Information Security Officer and Microsoft Experts in this webinar, K-12 Education Cybersecurity Threats and What We Can Do About Them.

WATCH NOW

Ensuring Privacy Policies & FERPA compliance

You can strengthen your culture of data security with strict adherence to privacy and FERPA compliance, which also involves partnering with best-in-class edtech vendors that align with your policies.

OUR SCHOOL OR DISTRICT:

- ☐ Has a policy for vetting edtech tools, including against FERPA requirements. Before teachers use an application, online platform, or educational website, it should be vetted and approved by the school district.
- ☐ Has policies for partnering with vendors that provide role-based access to sensitive data
- ☐ Is transparent in communicating with parents and students about how we collect data to monitor student progress and health, in compliance with FERPA
- ☐ Communicates with teachers, students, and parents on how to conduct videoconferencing calls
- ☐ Uses tools from vendors that:
  1. Comply with FERPA, HIPPA, the Children's Online Privacy Protection Act, Breach Laws, Data Residency Laws, the Digital Millennium Copyright Law, and the Sarbanes-Oxley Act
  2. Sign the nation student privacy pledge
  3. Achieve ISO/IEC 27001:2013 Certification, renewed each year
  4. Comply with SOC2® (Security Operations Center) Examination
- ☐ Uses products that ensure data privacy and cybersecurity best practices, with strong security features such as multifactor authentication and data encryption

0 /6 Number of Boxes Checked

LEARN MORE: What to Do in Response to a Cybersecurity Incident >

0 Total Number of Boxes Checked

SEE YOUR RESULTS >

What's Your Culture of Data Security Score?

How many boxes did you check? 0

Look at the areas with lower scores to determine where to prioritize your next steps.

9 or less:

It's time for a cultural overhaul.

Your training and preparedness look to need some work.

10-14:

We suggest you look at improving your culture.

You could benefit from more training, communication, and best practices to ensure everyone is on the same page.

15-18:

You're on the right path, but there's some room for improvement.

While you've shown strong dedication to a shared culture of data protection, there are still areas that could be improved.

19:

Congratulations! Your culture of data security is in excellent shape.

While you can never ensure 100% data security, by building a rock-solid culture among your users, you are making your important information as protected as possible.

Power a Culture of Data Security

Schedule a customized demo to help meet your data privacy and protection needs.

Visit www.PowerSchool.com or call 1-877-873-1550

PowerSchool