

Data Protection Checklist for Schools

Enable secure, compliant communications between teachers, parents, and students to improve collaboration and support digital learning initiatives.



Advances in technology have begun to transform education, allowing educators to implement distance learning initiatives that extend the reach of their curriculum beyond the physical classroom. Digital tools allow teachers to tailor learning to students' personal needs, improve reporting on student progress, and provide better transparency to all stakeholders, especially parents. The benefits extend to internal operations within educational agencies and institutions as well, improving productivity and efficiency. As collaboration between faculty, administrators, and staff become more seamless, school services improve.

While these trends bring significant opportunities for student learning and development, they also carry significant risks. Cloud environments that support eLearning initiatives and digital communications between faculty, students, and parents leave sensitive data at risk of exposure, raising concerns regarding privacy and regulatory compliance.

Most Common Types of Sensitive Data within Schools

- Personally identifiable information (PII).
- Protected health information (PHI), such as immunization records and student prescriptions.
- Individualized educational plan (IEP).
- Transcripts and report cards.

Compliance Concerns

- Health Insurance Portability and Accountability Act (HIPAA).
- Federal Education Rights and Privacy Act (FERPA).

Did You Know?

For education institutions, miscellaneous errors (such as accidentally sharing sensitive data with unintended recipients) and web application attacks (most commonly targeting email) are the top two causes of data breaches.



SOURCE: [Verizon's 2019 Data Breach Investigation Report](#)

Trusted by Educational Institutions and 5,000+ Organizations Worldwide



Data Protection Checklist for Schools

Based on security and privacy best practices, this checklist should be used to build or update a data security program that meets the demands of today's K-12 schools and higher education institutions.

- ✓ **Encrypt Data** — The best approach to safeguard students' PII and PHI is to encrypt it, ensuring compliance and critically protecting your institution in the event of a breach.
- ✓ **Automate Security** — Where applicable, apply rules across all departments and employees to ensure all student data is secure in both emails and documents.
- ✓ **Simplify Workflows** — Add an easy-to-use layer of encryption to the school's existing email and file applications, such as G Suite, without requiring new applications or logins.
- ✓ **Boost User Adoption** — Increase adoption of security technology through training and security awareness programs. Source easy-to-use security solutions that staff will want to use.
- ✓ **Ensure Compliance** — Meet current and future federal and state data privacy regulations for student data to avoid non-compliance penalties.
- ✓ **Maintain Control** — Deliver persistent data-centric protection, and stay in control of your students' data no matter where it is shared, by revoking or expiring access, controlling forwarding, and watermarking documents.
- ✓ **Enable Collaboration** — Keep student data secure and private while allowing safe collaboration with other parties.
- ✓ **Enhance Visibility** — Gain access to read receipts and granular tracking to determine who's seen your data, as well as where and when, to support compliance audits.

Protect and Share Sensitive Student Data with Virtru

Virtru helps educational institutions modernize their security to keep up with digital learning initiatives and privacy regulations by ensuring sensitive data is protected and under your control at all times. Integrated with the applications you already use like Gmail, Google Drive, and Microsoft Outlook, Virtru gives educational organizations the ability to share sensitive data with ease, while keeping student records and sensitive communications private and compliant.



Contact us to learn more about using Virtru within your organization.
virtru.com/contact-us

At Virtru, we empower organizations to unlock the power of data while maintaining control, everywhere it's stored and shared. Our portfolio of solutions and tools—built on our open data protection platform—governs data throughout its lifecycle. More than 5,000 organizations trust Virtru for data security and privacy protection. For more information, visit virtru.com or follow us on Twitter at @virtruprivacy.