Data Protection Checklist for K-12 Schools

Enable secure, compliant communications between teachers, admins, parents, and students to protect student privacy.

Now more than ever, K-12 educators have access to digital tools and platforms to tailor learning to students' personal needs, improve reporting on student progress, and provide better transparency to parents and school administrators.

As collaboration becomes more seamless between faculty, administrators, and staff, students benefit. But, when schools don't have the right tools in place to safeguard students' data, it's the students who suffer the consequences.

It's essential for K-12 teachers, staff, and admins to protect students' privacy and digital identity, while still being able to share important communications and records with guardians and administrators.

Most Common Types of Sensitive Data within Schools

- **Personally identifiable information (PII)**, like address and family information
- **Protected health information (PHI)**, such as immunization records, health conditions, and student prescriptions
- **Individualized educational plans (IEPs)**, which contain both PII and PHI for students. IEPs are frequently shared externally with parents and guardians via email.
- **Transcripts and report cards**, which contain private information about students' academic performance.

Did You Know?

35 states have passed data privacy laws to supplement FERPA. One of the most notable examples is New York Ed Law 2-D, which requires school districts to designate a Data Protection Officer and adopt the NIST Cybersecurity Framework.

Compliance Concerns

HIPAA
(Health Insurance Portability and Accountability Act)

FERPA
(Federal Education Rights and Privacy Act)

State Privacy Laws
(such as New York Ed Law 2-D)

Newfield Central School District · ICSD Iron County School District · az.gov State of Arizona · Spackenkill Union Free School District

©Virtru Corporation. All rights reserved.

Data Protection Checklist for K-12 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 Sensitive Data Wherever It's Stored or Shared** — The best way to protect students' PII and PHI from bad actors and third parties is through end-to-end encryption. This supports a broad range of state and federal compliance regulations.
- **Control Access to Private Student Information** — When student data needs to be shared externally, make sure you stay in control: Only grant access to those with a need to know, and select tools that allow you to revoke or expire access, restrict forwarding, and watermark sensitive files.
- **Automate Security** — Teachers and admins are extremely busy, so make data security effortless. Where applicable, apply automatic Security Rules across all departments and employees to ensure student data is protected in emails and files, even when teachers move quickly.
- **Make Data Sharing Easy** — When teachers and admins need to share information with parents and guardians, they need a low-barrier way to securely communicate sensitive information. Use easy tools that complement your school's existing email and file apps, such as Google Workspace or Microsoft Outlook, without requiring new accounts and passwords.
- **Remember the Recipients** — If you're sharing secure information with government agencies, or with parents and guardians, you need to make sure that your encryption software still makes information accessible. That means choosing security tools with an easy recipient experience that doesn't require them to create new accounts and passwords (which they probably won't remember) just to access one file.
- **Monitor Evolving Compliance Regulations** — Meet current and future federal and state data privacy regulations for student data to avoid non-compliance penalties. These regulations are ever-evolving, so it's important to collaborate with other districts within your state to ensure you're up to speed on any changes.
- **Enhance Visibility** — Gain access to read receipts and granular tracking to determine who's accessed sensitive data, as well as where and when, to support compliance audits.

Easily Protect and Share Sensitive Data with Virtru

Virtru helps educational institutions modernize their security to keep pace with digital learning initiatives and privacy regulations. Virtru equips teachers and faculty to share information with parents, colleagues, and government agencies without losing control over the sensitive data they've been trusted to protect. Integrated with the applications you already use like Gmail, Google Drive, and Microsoft Outlook, Virtru gives schools the ability to share sensitive data with ease, while keeping student records and sensitive communications private and compliant.

virtru

Ready to Learn More?

Visit virtru.com/education to get started.

©Virtru Corporation. All rights reserved.