

# Back-to-School Cybersecurity Checklist for K-12 IT Leaders

## 1. Secure Your EdTech Integrations

- ☐ Maintain a live inventory of all connected apps
- ☐ Remove unused or unapproved tools
- ☐ Establish a vetting process for new integrations

## 2. Strengthen Defenses Against Phishing & Credential Theft

- ☐ Conduct regular, safe phishing simulations
- ☐ Provide ongoing, scenario-based staff training
- ☐ Set up multi-factor authentication (MFA) for critical systems

## 3. Close Device Security Gaps

- ☐ Require minimum security standards for all devices, including BYOD
- ☐ Automate updates on district-issued devices
- ☐ Schedule routine vulnerability scans

## 4. Monitor Vendors & Eliminate Shadow IT

- ☐ Centralize vendor management and app approvals
- ☐ Monitor all third-party connections through one platform
- ☐ Disable access for vendors who no longer meet security standards




## 5. Control AI Tool Use & Data Sharing

- ☐ Vet all AI tools for privacy compliance before classroom use
- ☐ Set clear rules for what data can be entered into AI systems
- ☐ Provide staff guidance on safe, approved AI practices

SchoolDay helps K-12 schools check these boxes faster. [Learn how we can help your school.](#)



SchoolDay is on a mission to help reduce data sprawl, protect student privacy, and enhance data security in the education sector.

 [schoolday.com](https://schoolday.com)  [info@schoolday.com](mailto:info@schoolday.com)  +1 888 557 6085