jamf

Education Compliance for Beginners

How to build a K-12 compliance plan that protects students, teachers and communities

The modern K-12 compliance landscape

In any industry, device and network security compliance can be a complex beast. Industry standards change as device capabilities expand—and as laws or best practices transform.

K-12 environments compound these complexities.

Discover:

- **How to keep up with ever-changing education compliance requirements**
- **Why a strategic approach to compliance infrastructure matters**
- **How to build sustainable compliance practices**

This document is for informational purposes only and does not constitute legal advice. Compliance requirements vary by jurisdiction and institution. Schools and districts should consult qualified legal counsel to determine their specific compliance obligations.

Unique K-12 compliance challenges

Like their corporate counterparts, schools must secure the wide variety of devices and users that connect to school networks and keep them secure from cyber attacks.

Unlike corporate settings, schools must allow for very open and simple communication with parents and the public — all of whom are using devices that your district doesn't control.

This creates a broad and vulnerable attack surface. Add the budget constraints that many schools and districts face, and it's easy to see how security compliance is a constant challenge.

School device and network users are also unique.

The starkest difference between corporations and schools is this: schools serve a truly daunting diversity of users, including teachers and administrators, school and district staff, and perhaps the most challenging: children.

Children are curious. Children need compelling, interactive learning tools. They need to gain the skills to become responsible digital citizens, and they need to share what they have learned with their teachers, families and peers.

The curiosity of children is boundless.

That's why school IT must enable some boundaries for them. Their job: to keep children safe from phishing attempts, malware and dangerous or inappropriate content — without slowing down day-to-day learning and teaching.

Additionally, schools must balance cybersecurity practices with student privacy concerns. And for some of the most vulnerable students, such as LGBTQIA+ children, violating their privacy can be extremely dangerous for their mental health and physical safety.

Intersecting standards and requirements

Education environments worldwide find themselves under close scrutiny and enormous pressure coming from multiple directions:

1. **National and international legislation**
2. **Regional laws and standards**
3. **Educational oversight bodies**

In the EU, the General Data Protection Regulation (GDPR) protects student data, for instance, and in the UK it's the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Child-specific laws and regulations also come into play, such as the US's Children Internet Protection Act.

In addition, schools often have requirements that can affect data, network and device security such as the US's Americans with Disabilities Act.

And don't forget the bodies that certify levels of security compliance that schools want to meet, such as StateRAMP and FedRAMP, two security levels that are often required by governmental organizations that schools wish to interface with.

The digital transformation challenge

A huge shift has occurred nearly overnight in K-12 classrooms around the world, brought about by both the COVID-19 pandemic and a sharply increased focus on school security.

Schools going through a digital transformation make the following changes:

Shift from paper-based to digital learning environments

Follow increased data collection and storage requirements

Consider remote and hybrid learning and their effects on compliance

Common compliance themes across frameworks

In addition to these myriad differences in compliance for schools and districts from their corporate counterparts, schools must also adhere to requirements and best practices regarding:

- Data protection and privacy
- Device and network security
- Access control and authentication
- Incident response and breach notification
- Audit trails and reporting

K-12 cyberattacks are widespread

Unfortunately, schools and districts are an attractive target for cybercriminals.

The data that schools carry, including social security numbers and other identifiers, is lucrative. In addition, some school districts keep parents' credit cards on file for school lunches and fees — which is fast money.

This is a widespread phenomenon; in the UK's Cyber security breaches survey 2025, 44% of primary schools and 60% of secondary schools identified breaches or attacks that year.

The cost of non-compliance

Many schools and districts have paid that cost. Some have been forced to pay ransoms, some have been sued by parents for leaked data, some have made headlines for their lack of ability to protect their networks and data or to properly report breaches.

Financial penalties and legal consequences

As mentioned above, schools, districts and even vendors that fail to follow strict security compliance and data protection policies have found themselves in financial and legal trouble.

They find themselves paying exorbitant ransoms, breaking federal or international student privacy laws and getting sued by parents.

A recent vendor attack

In 2024, a widely used student information system (SIS) and education technology platform paid $2.85 million in ransom to a hacker who threatened to release student data if it wasn't paid.

The very next year, the same hacker began approaching individual school districts that used their software with similar demands.

Reputational damage and community trust

Schools can lose a lot of community trust from funders, parents and local businesses, especially when they don't have clear rules on how to inform the public about breaches.

A recent district attack

After a 2023 ransomware attack, an urban US school district did not inform the public that hackers were demanding money and threatening to release extremely sensitive data if they weren't paid. The district did not pay, and the information was released to the public. Even then, they waited for months to notify specific students affected. The public outrage impacted the district's reputation.

People are, naturally, sensitive to their students' privacy, and without clear guidelines, schools and districts can find themselves in a tailspin as they receive different and sometimes contradictory advice from multiple directions. When school officials act in a non-consistent manner, the public often assumes the worst.

A recent school closing

In January 2026, a cyberattack on a secondary school in the UK completely closed down the school for a week. It rendered "the school's entire IT system non-functional, including telephone, email, Google Classroom, school management systems and Microsoft SharePoint."

Operational disruptions and resource allocation

The intent of cyberattacks may ultimately be profit, but the way they go about it can disrupt school systems in a myriad of ways, resulting in:

- **Paycheck disbursement slowdowns**
- **Tardy grade reports**
- **Complete closures of schools for days at a time**

Now that you understand these risks, let's explore the foundational elements that create a robust compliance plan.

Four core compliance pillars in K-12 education

1. Student data privacy

What is student data?

Understanding what constitutes student (or even teacher or parent) data is the first step in creating policies and procedures to protect this data. This data is comprised of, but not limited to:

- Names, birthdays, street addresses and personal email addresses
- Parent names, workplace information and credit card numbers
- Learning data such as test scores and grades
- Health, behavior and attendance records

Data minimization principles

Minimizing what data you collect and how long you keep it can go a long way in keeping student data private. Collect only what is necessary for functions to take place and only keep it for the time it is needed. Hackers can't access information that you don't have!

Allow only those who actually need it to access the specific data they require. Limited access creates a smaller attack surface.

Set consent and notification requirements. Ensure that you practice transparency in communicating what data you request and why, as well as where it is stored and for how long. This will go a long way toward community trust.

Thoroughly manage third-party vendors such as testing or educational software companies**.** Check their compliance with safety and privacy protocols. Set policies and workflows to ensure that you know exactly what data you allow them to access, how it will be used, and what vendors will do with that data. This can prevent the most common type of attack: third-party breaches.

Four core compliance pillars in K-12 education

2.

Access management essentials

Role-based access principles

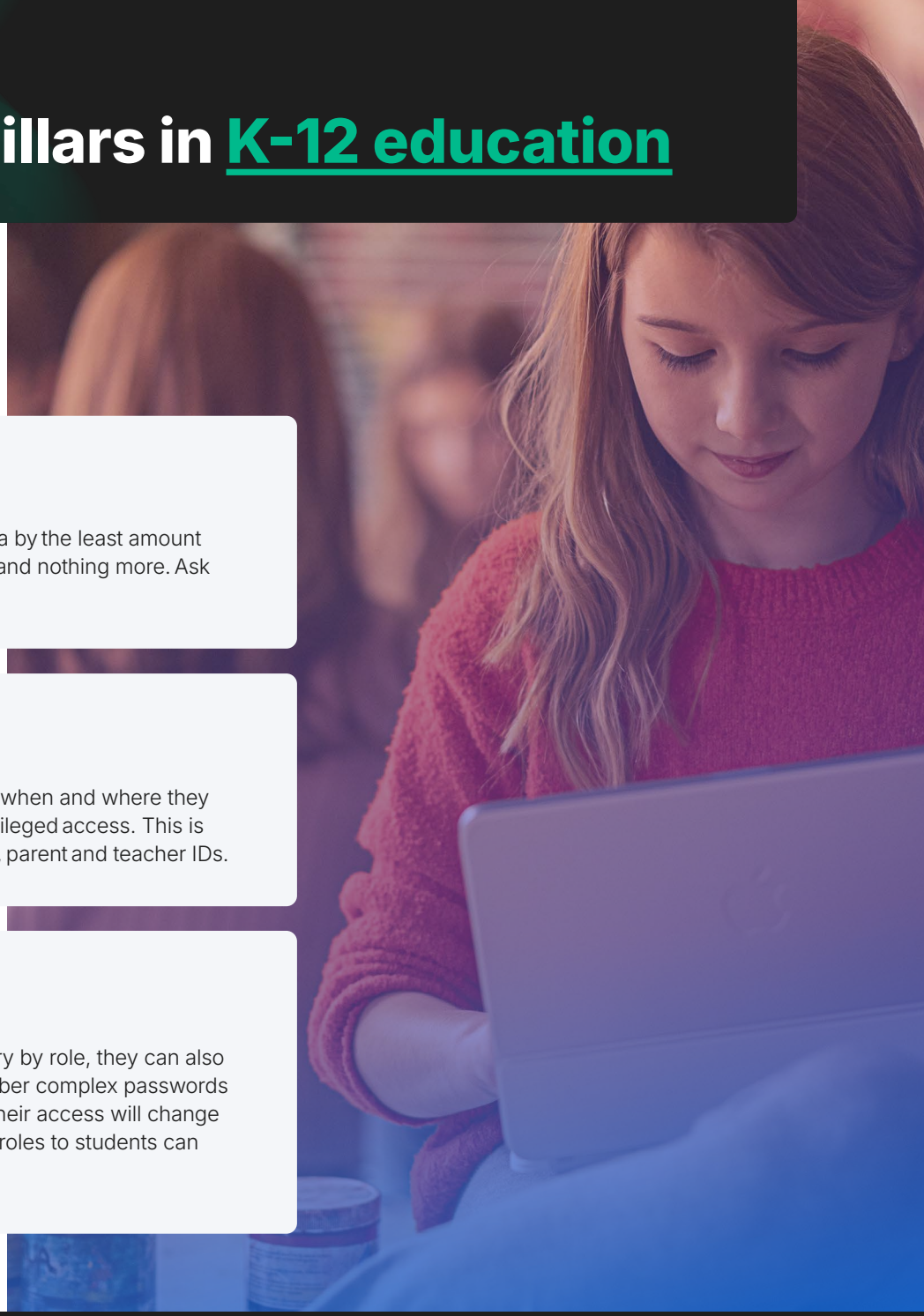
As noted before, it is vital to manage access to networks and data by the least amount of access a person requires: offer what they need to do their job and nothing more. Ask yourself: Who should have access to what and when?

Enforcing role-based access

Ensure that you have a way to privilege access controls for staff when and where they need it — and to securely limit guests and visitors to the least privileged access. This is often best controlled when these privileges are linked to student, parent and teacher IDs.

Age-based flexibility

Keep in mind that as access and authentication requirements vary by role, they can also vary by age. Younger learners may not have the ability to remember complex passwords while older students will. And, of course, as each student ages their access will change based on new curriculum. Assigning grade-based or age-based roles to students can save you a lot of hassle in the long run.



Four core compliance pillars in K-12 education

3.

Security infrastructure requirements

Setting clear security infrastructure requirements and using vigorous endpoint protection strategies can mean the difference between a partial breach and a full one, between a compromised device and a safe one.

Endpoint protection strategies

Ensure that you have endpoint protection in place that offers:

- Automated threat prevention and remediation
- On-device analysis and proactive reporting
- Automated data policy enforcement

As important as the features themselves: ensure that implementing your solution doesn't compromise security, privacy or performance.

Network segmentation considerations

One of the best ways to prevent a partial breach from becoming a district-wide one is to segment your networks based on who is using the network or what part of the organization the network serves. You could have, for example: admin and teacher networks, student networks and guest networks.

Continued...

Four core compliance pillars in K-12 education

3. Security infrastructure requirements

Encryption standards and implementation

Take a close look at what encryption and implementation strategies your various governing bodies require — as well as what best practices you can implement:

- Strong encryption algorithms
- Secure key management
- Data encryption when stored and in transit

Regular security assessments

As student populations shift and ed tech tools evolve, you'll need to ensure that you have regularly scheduled security assessments. This security upkeep is absolutely essential to continued compliance.

This will give you the chance to:

- Incorporate new and emerging technologies
- Create policies to meet any changes to internal or outside compliance requirements and best practices
- Check for any reporting blank spots or new reporting needs
- Evaluate your vendors and how they suit any new or expanded needs

Four core compliance pillars in K-12 education

4. Documentation and audit preparedness

Preparing for audits can seem like a chore. However, proper audit preparedness can not only save you time in the long run when audits are required but also keep your networks and data more secure.

Here's how to approach it:

Key data categories to manage and report on

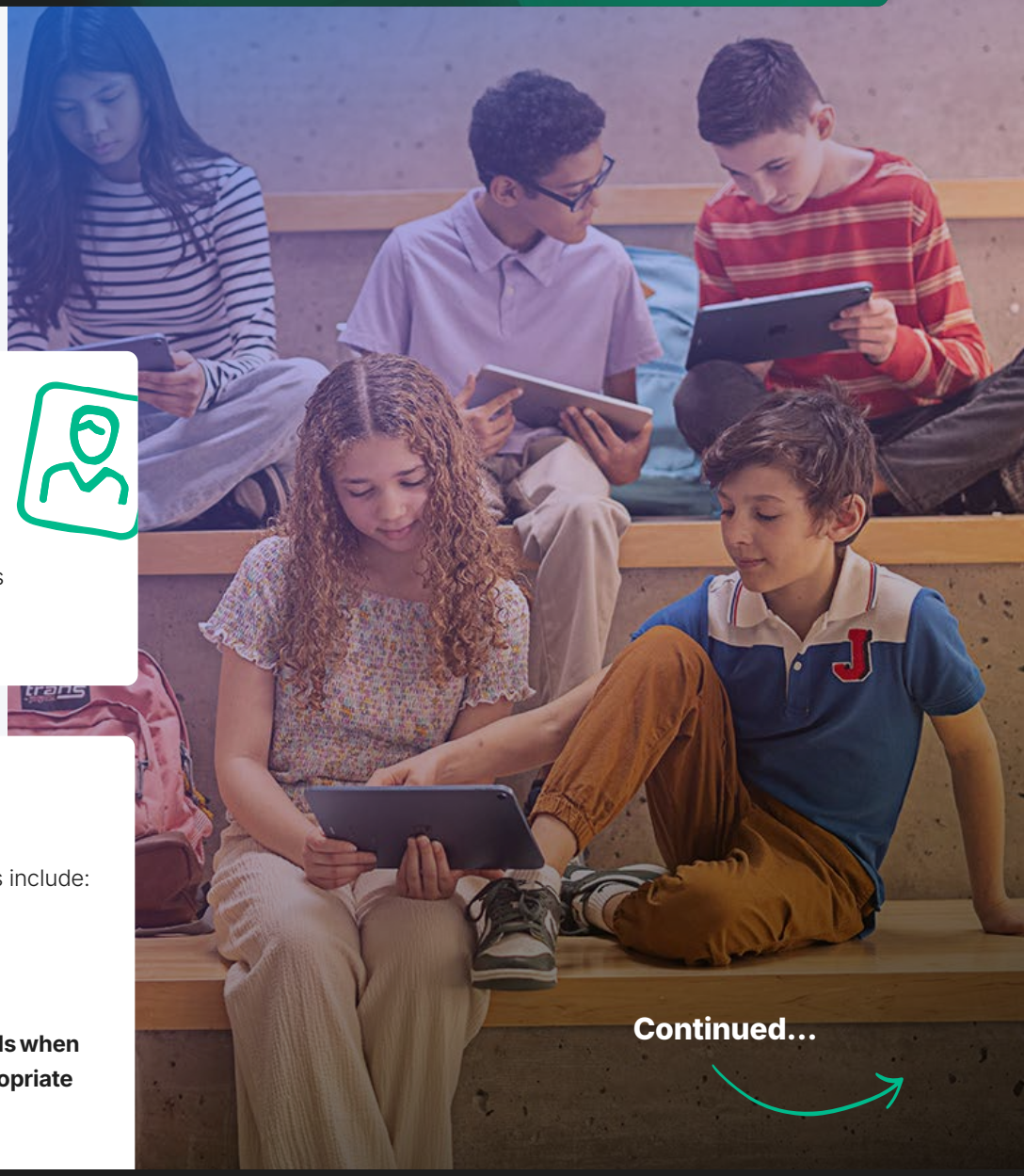
Keep in mind the three large groupings of data you'll need to track:

Student data: attendance, grades and behavior records
Operational data: IT asset reporting, network configurations and security logs
Legal data: Compliance documents, vendor contracts and audit reports

Essential record-keeping practices

Ensure that you maintain secure, centralized and compliant data. Key practices include:

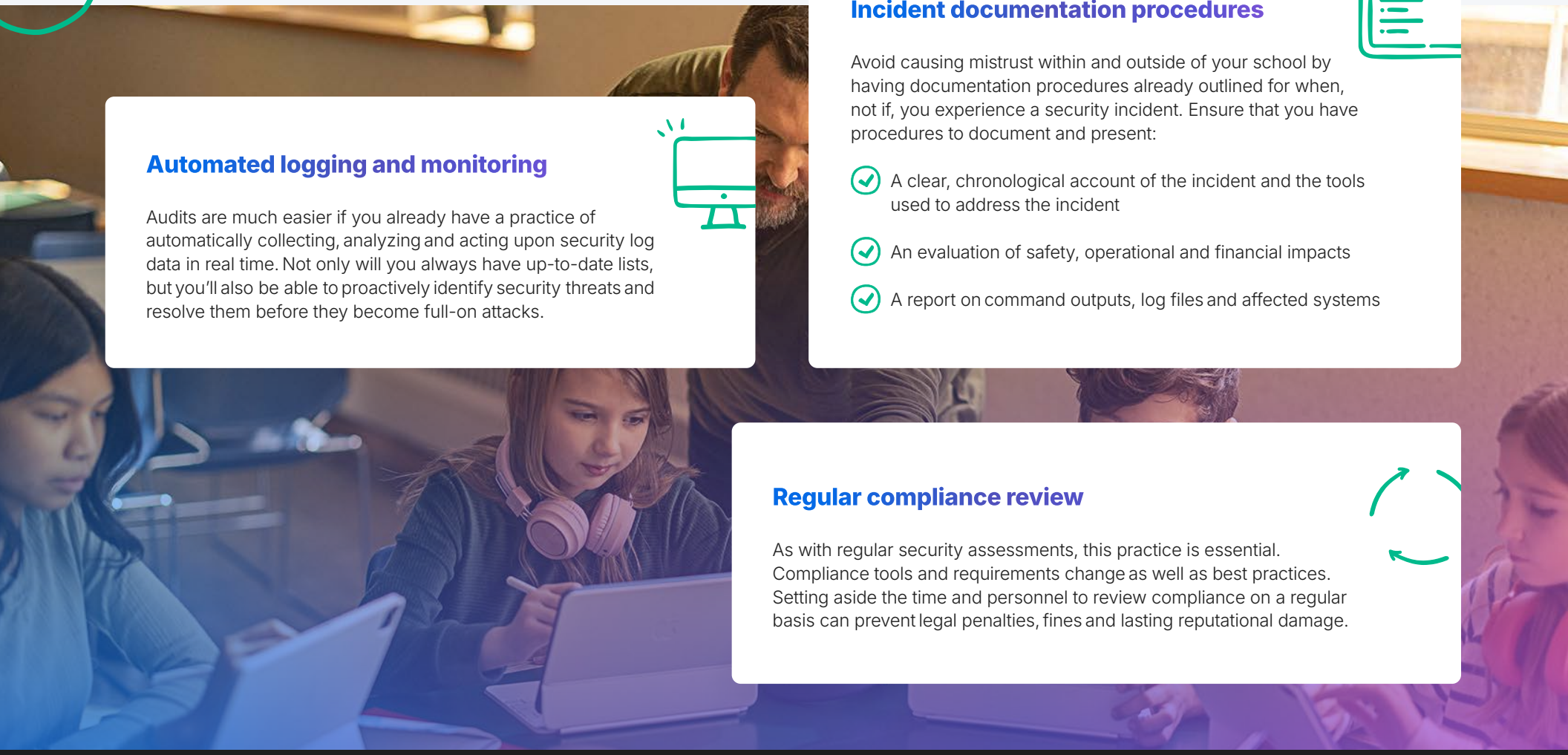
- **Using a Student Information System (SIS)**
- **Managing hardware/ software inventory**
- **Digitizing records when and where appropriate**



Continued...

Four core compliance pillars in K-12 education

4. Documentation and audit preparedness



Automated logging and monitoring

Audits are much easier if you already have a practice of automatically collecting, analyzing and acting upon security log data in real time. Not only will you always have up-to-date lists, but you'll also be able to proactively identify security threats and resolve them before they become full-on attacks.

Incident documentation procedures

Avoid causing mistrust within and outside of your school by having documentation procedures already outlined for when, not if, you experience a security incident. Ensure that you have procedures to document and present:

- A clear, chronological account of the incident and the tools used to address the incident
- An evaluation of safety, operational and financial impacts
- A report on command outputs, log files and affected systems

Regular compliance review

As with regular security assessments, this practice is essential. Compliance tools and requirements change as well as best practices. Setting aside the time and personnel to review compliance on a regular basis can prevent legal penalties, fines and lasting reputational damage.

COMPLIANCE READINESS ASSESSMENT

Are you ready?

A self-assessment checklist

This constantly evolving, rigorous and complex process can seem overwhelming. Checklists are an excellent preparedness practice so that your team will miss nothing.

TECHNOLOGY INFRASTRUCTURE READINESS

Do you have the following in place?

- [ ] A device inventory and management system
- [ ] Centralized identity and access management
- [ ] Network segmentation between student and administrative systems
- [ ] Endpoint protection deployed across all devices
- [ ] Data encryption at rest and in transit
- [ ] Automated backup and recovery procedures
- [ ] Security monitoring and alerting capabilities

POLICY AND GOVERNANCE READINESS

Have you documented or established:

- [ ] Comprehensive acceptable use policies
- [ ] Data retention and disposal policies
- [ ] Incident response procedures
- [ ] Staff training programs
- [ ] Vendor management and due diligence processes
- [ ] A regular policy review and update schedule

OPERATIONAL READINESS

Have you:

- [ ] Designated a compliance officer or team
- [ ] Conducted regular security assessments
- [ ] Enabled audit trail capabilities
- [ ] Established breach notification procedures
- [ ] Set parent and student communication protocols
- [ ] Enabled documentation and record-keeping systems

VENDOR AND THIRD-PARTY READINESS

Have you put the following in place?

- [ ] Data processing agreements with all vendors
- [ ] A security certification verification process
- [ ] Regular vendor security assessments
- [ ] Clear data sharing and access controls
- [ ] Vendor incident notification requirements

How Jamf for K-12 supports compliance

While Jamf for K-12 doesn't automate and ensure your school's compliance itself, it provides essential infrastructure that supports your overall compliance strategy with:

Device management and security:

- Centralized device enrollment and configuration
- Automated security policy enforcement
- Remote device management and protection
- Comprehensive device inventory and reporting

Scalable management:

- Consistent policy application across all devices
- Efficient management of large device deployments
- Scalable policy deployment across large device fleets
- Support for diverse learning environments (1:1, shared devices, BYOD)

Access control and authentication:

- Integration with identity providers for Single Sign-on (SSO)
- Role-based access management
- Role-based app and content restrictions
- Secure authentication across devices and platforms

Integration capabilities

- Works with existing school information systems
- Supports third-party educational applications
- Integrates with network infrastructure
- Connects with identity and access management solutions

The Jamf platform serves as a foundational layer that helps districts build the reliable, secure and manageable technology environment that compliance frameworks need.

Our automations and capabilities allow your team to focus on policy, training and strategic compliance initiatives rather than day-to-day device management challenges.

Compliance in K-12 is never done.

It's a continuous practice that evolves alongside your technology, your student population, and the regulatory landscape.

The good news is that you don't have to build that foundation alone.

Jamf for K-12 gives your team the tools to manage devices, enforce policies and maintain the kind of secure, auditable environment that compliance demands. That means less time spent on infrastructure and more time on the work that truly matters.

Request a free trial

jamf