



# Considerations for a holistic approach to digital and physical security

## Best practices for implementing technology for safer schools

To perform their best, students—and educators—need to feel safe, both physically and digitally. Yet the risks to educators and students are becoming more complex. Technology plays a critical role as schools address these evolving security challenges: from understanding who is on campus or targeting students online, to responding to medical issues, natural disasters, or acts of violence.

Equally challenging is ensuring safety without making the school community feel afraid. Security technology should be ubiquitous and invisible—except to those who need to monitor and manage it. Like a light switch, faucet, or wireless network connectivity, it should just work. When this technology is combined with school policies and procedures—from establishing which door to enter to assuring acceptable use of online resources — you can build a coordinated and comprehensive response and prevention system.

When considering holistic approaches for school security, it's important to think about behavioral counseling, personnel and resource allocation, drill and training schedules, compliance, physical hardening of facilities, and policies and procedures. Integrated technology solutions serve to make these critical elements even more effective.

This guide focuses on the technology that can help make schools safer, including access control, video surveillance, collaboration, notification, and cybersecurity. It suggests questions to ask, provides processes to consider, and outlines action points you can follow as you prepare your school to respond to cyber and physical threats. (Please note: This guide is not designed to replace a state-mandated school safety plan.)

## Access Control



Do we have integrated controls to manage access to networks, doors, gates, and parking facilities?

True access control spans the lifecycle of a day. For example, you know where a student or educator should be at any given time, and you should expect this same level of information about anyone who visits your school. Ideally, you have established and validated procedures in place to identify visitors and authorize access before they enter, and consistent procedures to maintain awareness of where they travel within the campus.

In fact, these safety mechanisms should operate around the clock. With automation and notification capabilities, they should protect the building and valuable school resources even after the school day ends.

The same is true of your cyber environment. By managing the distinct access privileges granted to educators, staff, students, and visitors, you can help protect valuable data from threats that may emerge from within your environment.



Are access controls fully integrated with video surveillance systems and communications/alert systems?



Are video surveillance systems triggered if a door, gate, or parking facility is accessed inappropriately?



Does the system notify appropriate personnel of a breach? Can personnel monitor and manage the system remotely, including from a mobile device?

The integration of access control systems with other technology, including video surveillance, collaboration, and notification systems, enables seamless and consistent monitoring and management. For example, access control systems should include alarms/alerts so that there is an audible signal and/or visible light, and appropriate personnel are notified when an entry point is accessed without authorization.

### Other considerations



Do access control systems have time stamp and event trigger actuation?



Are sensors, sirens, and lights in place to alert in the event of an emergency?



Do we have a plan for maintaining access control systems and ensuring that authorizations are kept up to date?

### Actions

- Restrict access to as few entry points as possible and expand the number of entry points only if access can be monitored/controlled by personnel and/or technology.
- Limit visitor access during the school day, and when possible, establish connections with local law enforcement to ensure you have the most up-to-date information on restricted individuals.

## Video Surveillance



Can we validate that video surveillance is in place in all appropriate locations across campus? Are video surveillance systems fully integrated with access controls and communications/alert systems? Are video surveillance systems monitored? If yes, how?

Video surveillance is an integral part of security and safety, with cameras acting as digital witnesses, spanning and assessing more area than is humanly possible. Despite this potential, video is most often accessed reactively, during evidence gathering and investigation after an event. Yet, modern video surveillance systems have the capability to use analytics, or software systems, to detect anomalies, adverse behaviors, and unexpected objects or people in places they shouldn't be. Once a potential problem is detected, an integrated video surveillance system can send a notification to school administration or resource officers as appropriate so that information can be used proactively to aid in response. This ensures video surveillance works as more than just an investigative tool and operates in a proactive and preventive way.



How are data and analytics from video surveillance systems shared with school resource personnel and first responders/law enforcement? How long is surveillance information stored and maintained?



The importance of a collaborative relationship between a school and first responders/law enforcement cannot be overstated. It's clear that video provides valuable evidentiary data, but it's equally critical that these agencies can access video systems remotely during an event to ensure they provide the appropriate response.

### Actions

- Ensure all areas of a facility are covered. Gaps in security can be quickly discovered, leaving room for exploitation. Importantly, placing video surveillance technology in parking lots and garages, as well as at school entrances, can allow for early detection of a potential event, giving everyone more time to react and make more informed decisions.
- Consider adding video analytics capabilities to your video surveillance systems. With these capabilities, traditional cameras become valuable sensors that work proactively.
- Ensure that video surveillance systems are integrated with notification tools so that as events are detected, the video streams can be shared in real-time and alerts can be sent immediately to appropriate personnel as defined in the policies you've established.




## Collaboration

-  Are all collaboration resources (voice, video, text) accessible to essential stakeholders?
-  Are guidelines in place to ensure appropriate school and community personnel have access to collaboration resources? How do we ensure that our contact lists are kept up to date?


Through the effective use of collaboration resources, everyone within a school community, as well as multiple agencies (even those at great distances away), can be connected to school resources and to each other. Achieving this degree of accessibility requires careful planning to ensure adequate levels of security and privacy, but once complete can support vital partnerships, which can play a significant role before, during, and after an event.


Importantly, collaboration technology already deployed in schools for use in teaching and learning can also be used for security purposes, expanding the value of your technology investment. Through a private, secure collaboration platform, all stakeholders can meet routinely to share safety and security plans, concerns, and recommendations. And they can be prepared to collaborate and respond in the case of a security event.

-  Are collaboration technologies fully integrated with access controls and video surveillance systems?

Fully integrated systems mean that school community personnel, first responders, and others have access to comprehensive information needed to make a decision in an emergency. Or to decide there is no emergency at all.

### Other considerations

-  Can we establish secure online spaces to communicate instantly with appropriate personnel about hazards or security-related concerns?

-  Can we use data and analytics mined from social media and public records to identify and remediate threats?

### Actions

- Use collaboration technology in an integrated way to share critical information in real time, allowing multiple agencies to coordinate incident response easily.
- Consider other applications for collaboration spaces to help protect the school community. Using collaboration tools—especially when counselor-to-student ratios are high—can enable proactive intervention and provide additional resources to help students in need or at risk. For example, create a safe online space to connect at-risk students with resources that aren't available on campus and enable them to engage online. Or, establish a process through which students can use collaboration resources to anonymously report potential threats or hazards that might otherwise escape the notice of school personnel.



## Notification



In case of an event, can we ensure that appropriate personnel are advised quickly about the situation and informed of their required actions based on their role?

The most effective notification system is designed to reach all audiences, from students and families to first responders and community officials. You should ensure that notifications can be sent to distinct groups based on role. These notifications should advise recipients of the steps they should take in response to the alert.

It's also important that notifications are accessible across devices and applications, including mobile and desktop devices, desk phones, digital signage, intelligent whiteboards, and social media, to reach the broadest possible audience.



Is notification technology integrated with other security tools (access control, video surveillance, and collaboration) as needed?

The integration of notification technology with other security tools ensures that school community personnel, first responders, and others have access to the same information in case of an event. If, for example, a school is evacuated because of a fire alarm, an educator could receive a notification advising whether the evacuation is a drill or emergency and can access daily school attendance data to ensure that all her students are accounted for.

### Actions

- Streamline access to simplify use of the notification system in an emergency; remove multiple logins and manual messaging that can lengthen response time.
- Based on role, ensure that recipients are advised how to respond when they receive an alert.



## Cybersecurity



Do we provide a secure teaching and learning environment without impacting privacy or productivity?



Can we monitor and control access to ensure that only authorized users use the network? Do we have visibility into systems and processes to identify threats?



Can we protect school resources, student data, and intellectual property from cyber threats? If a cyber attack does occur, can we respond quickly to stop threats before they affect our network or student and faculty devices?



Do we safeguard students and other users from personal attacks online, such as cyber bullying?

In schools, cyber and physical threats converge. Violence at school is overwhelmingly associated with pre- and post-event digital messaging and communication, and bullying takes place both in school and online. A coordinated and comprehensive response to all types of threats is critical.

### Other considerations



Can we assure compliance with legal requirements, such as FERPA, CIPA, and HIPAA?

Cybersecurity in schools plays two aligned roles: to protect a school's systems and data from intrusion and attack, from both internal and external threats, and to detect cyber events—from harassment of an individual student to threats against a school's infrastructure—when they do occur.

Schools and the data they hold—from personal information to intellectual property—are a tempting target for cyber thieves who seek to access and use the data, or those who hope to gain by infiltrating systems and holding them hostage. The risk is twofold: Technology can be used to commit crime, or the technology, like malware, becomes part of the crime. The most secure schools have a digital perimeter protecting the entire environment.

### Actions

- Ensure that no initiative is completed without sign-off from the cyber review team. Every project, from HVAC updates to access control, and from school bus telemetry to remote learning, has digital components, which can be surprisingly vulnerable. Cybersecurity must be considered with each initiative.
- Ensure the teams charged with physical security and cybersecurity coordinate activities for a consistent response to threats of all types.



## What to do next

Educators understand the value of a plan and the importance of a plan in achieving a successful outcome. A safer school initiative begins with this same approach: a vision of what you hope to achieve and a determination of the clear steps you need to take to get there.

The “human” element is critical. No environment can be safe without a committed community in place to make change happen. But technology can support these efforts, and an integrated system—that includes access control, video surveillance, collaboration, notification, and cybersecurity—can help ensure an intentional and coordinated response to any type of event.

Contact us at [cisco.com/go/education](https://cisco.com/go/education) to learn more.



## Safer Schools Readiness Checklist

### Access Control

✓ Restrict access to as few entry points as possible and expand the number of entry points only if access can be monitored/controlled by personnel and/or technology.

✓ Limit visitor access during the school day, and when possible, establish connections with local law enforcement to ensure you have the most up-to-date information on restricted individuals.

### Video Surveillance

✓ Ensure all areas of a facility are covered. Gaps in security can be quickly discovered, leaving room for exploitation. Importantly, placing video surveillance technology in parking lots and garages, as well as at school entrances, can allow for early detection of a potential event, giving everyone more time to react and make more informed decisions.

✓ Consider adding video analytics capabilities to your video surveillance systems. With these capabilities, traditional cameras become valuable sensors that work proactively.

✓ Ensure that video surveillance systems are integrated with notification tools so that as events are detected, the video streams can be shared in real-time and alerts can be sent immediately to appropriate personnel as defined in the policies you've established.

### Collaboration

✓ Use collaboration technology in an integrated way to share critical information in real time, allowing multiple agencies to coordinate incident response easily.

✓ Consider other applications for collaboration spaces to help protect the school community. Using collaboration tools—especially when counselor-to-student ratios are high—can enable proactive intervention and provide additional resources to help students in need or at risk.





## Notification



Streamline access to simplify use of the notification system in an emergency; remove multiple logins and manual messaging that can lengthen response time.



Based on role, ensure that recipients are advised how to respond when they receive an alert.

## Cybersecurity



Ensure that no initiative is complete without sign-off from the cyber review team. Every project, from HVAC updates to access control, and from school bus telemetry to remote learning, has digital components, which can be surprisingly vulnerable. Cybersecurity must be considered with each initiative.



Ensure the teams charged with physical security and cybersecurity coordinate activities for a consistent response to threats of all types.



**Learn More**

For more information please visit:  
[cisco.com/go/education](https://www.cisco.com/go/education)