

A Synectics Guide To

Effective Campus Security and Operations



**Best Practices for Schools,
Colleges, and Universities**

SYNECTICS

Contents

What's the best way to keep students, staff, and facilities safe and secure while optimising your operations? This guide takes an in-depth look at technologies that will help schools, colleges, and universities answer this question. And how these can be adopted as part of a unified security and operations management solution. One that will improve risk detection and incident response – from everyday scenarios to emergency situations.

- 04** Current Trends and Challenges
- 06** Unify Your Security Monitoring and Control
- 10** Optimise Your Solution
- 12** Secure Perimeters, Parking, and Grounds
- 16** Verify and Locate Visitors, Students, and Staff
- 20** Keep Students and Staff Safe
- 22** Investigate Incidents Quickly
- 26** Manage and Improve Emergency Response Scenarios
- 30** Manage Multiple Sites and Mobile Services
- 32** Protect Privacy and Data







Current Trends and Challenges

Before looking more closely at what's possible, it's useful to understand some of the challenges and developments currently affecting education providers.

1 Crime on campus

Campus crime at all levels of education continues to be an issue. Theft, alcohol-related offences, sexual assault and harassment, drug offences, and physical violence are among the most common on-campus offences. In the three years prior to 2025, nearly 100,000 violent incidents were reported in UK schools, including cases involving weapons such as knives and firearms¹.

2 Reputation matters

Safety matters to potential candidates. In the US, The Clery Act² mandates that colleges disclose campus crime statistics to ensure prospective students and their families can make informed decisions. Prioritising safety and security is a way to stand out from the crowd. Many UK university league tables also include clear sections on crime rates on campus.

3 Focus on student well-being

Keeping students safe is not just about protecting them from security risks. Mental health in particular is a big issue. 42% of UK university students³ have reported experiencing serious personal, emotional, behavioural, or mental health problems necessitating professional help. Anxiety affects 55% of US students, depression 41%, and 13% have seriously considered suicide⁴ in the past year.

4 Cyber risk threat

Cyber risk in education is a growing concern – in fact research suggests that education is the fourth most targeted industry for this type of crime⁵. A massive 97% of higher education institutions in the UK reported a breach or cyber incidents in 2023/24⁶. In the US, the Highline Public School District in Washington State was closed for two days in 2024, after a ransomware affected nearly 93,000 students' data.

1 <https://www.sacpa.org.uk/2025/04/03/the-alarming-increase-in-violent-incidents-within-uk-classrooms/>

2 <https://www.clerycenter.org/the-clery-act>

3 <https://happiful.com/student-mental-health-struggles-rise-report>

4 <https://www.uhc.com/content/dam/uhcdotcom/en/HealthAndWellness/PDF/UHC-White-Paper-Student-Behavioral-Health-Report-May-2024.pdf>

5 <https://firmussec.com/attackers-school-day-cyberattacks-on-the-education-industry/#:~:text=A%20Top%20Target%20for%20Cyberattacks&text=Research%20conducted%20by%20Sophos%20in,%25%20of%20the%20cases%2C%20respectively.>

6 <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024-education-institutions-annex>



Unify Your Security Monitoring and Control

Keeping campuses safe, secure, and operating as efficiently as possible against this backdrop is crucial – especially given their high foot traffic, and diverse population of students, staff, and visitors.

With multiple entry points, large outdoor areas, and buildings spread across multiple locations, maintaining consistent security coverage is both necessary and difficult. Additionally, campuses must balance safety with accessibility, ensuring a welcoming environment without creating a sense of restriction. Factoring in off-campus facilities, such as school bus services, increases the challenge further still.

It's an operations brief that requires a mix of security, emergency, and safety technologies to track and respond to threats.





Choosing the right systems

A number of factors will influence decisions about which individual systems and technologies to adopt. These decisions are typically shaped by three factors: legal mandates, the scale of the estate, and available resources.

1. Mandated systems and capabilities

Some specific systems and capabilities are mandated by law. The nature of these will vary based on location. In the US, for example, schools in some states are required to have panic alarms linked to local law enforcement. Other states have specific regulations concerning classroom lockdown capabilities.

While not a legal entity, the Partner Alliance for Safer Schools (PASS) in the US provides a detailed framework for assessing the required K-12 security components.

2. Size of estate

Typically, more people equal more risk. As such, larger educators will have more complex requirements that will need to be reflected in the systems adopted. In the UK, for example, the newly introduced Terrorism (Protection of Premises) Bill, also known as 'Martyr's Law', applies a tiered set of security requirements to publicly accessible facilities based on capacity, including those within the education sector. The vast majority of UK universities will need to adopt the enhanced tier due to their large student populations and extensive campus estate.

3. Available resources

Annual security budget, the size of an educator's security team and the number of security officers employed are important factors that may dictate the type of cameras adopted, level of automation required, and priorities for new technologies adopted.

Connect your data

Whichever individual systems you choose, monitoring them independently is time consuming and potentially risky. When you have a siloed view of any particular incident, there's a danger that things 'fall through the cracks.'

Consolidating the management of multiple systems into a unified security and operations management platform is a practical solution. As well as delivering a 360° view of incidents that would not be possible when monitoring systems separately, it saves busy, resource-tight teams considerable time, improving efficiency and productivity.

Here are some examples of third-party data sources that can be integrated:

Security	Education	Emergency	Society
Cameras	Visitor management systems	Fire and smoke alarms	Social media
Perimeter detection	Mass notification systems	Chemical detection	Weather warnings
Facial recognition	School bus surveillance and telematics	Noise (e.g. gunshot) monitors	Major event alerts
Loitering and crowd detection	Vape detection	Emergency help points, duress (panic) alarms	Traffic reports
Object detection and recognition	Student/Staff ID systems	Lighting (e.g. evacuation guidance)	Tip lines
License plate recognition	HR systems	Sprinkler systems	
Watch lists	Approved guardian lists	Third-party watch lists	
Other AI and video analytics	Dispatch		
Metal detectors			

Top Tips When Choosing Your Platform:

1. Check for ONVIF Compliance:

ONVIF is a global and open industry forum focused on standardising communication between IP-based physical security products to achieve interoperability between equipment.

2. Ask About Legacy Tech:

If a platform is described as open architecture, it should integrate with any third-party system. But make sure this applies to legacy technology – including analogue cameras, if you have them. This means systems can be cost-effectively scaled and updated in line with budgets without having to rip out and replace existing infrastructure.



Optimise Your Solution

With your unified platform, you will be able to understand threat scenarios, detect and prioritise concerns, and efficiently respond to safety and security issues on campus.

For this to be as effective as possible, four specific integrations and system features are recommended.

1. Mapping made for complex campus layouts

School, college, and university campuses have complex layouts, can involve multiple sites, and are often located in the heart of urban environments. To detect and respond to incidents effectively, certain mapping capabilities are essential.

Choose a solution that supports the integration of geo-spatial mapping, such as OpenStreetMap, and locally hosted maps, including CAD maps and floor plans. Your solution should present camera information and integrated device data as 'glanceable' interactive icons and category clusters. This will allow your security team to zoom out or drill down to monitor and coordinate responses effectively, equipped with locational data that adds context, such as hot spots and incident heat-mapping.

2. Analytics-driven intelligence

By integrating AI-based video analytics tools into your platform, you will be able to create customised rules and thresholds which can then be applied to all captured data to raise real-time alerts whenever specific criteria are met. This supports proactive risk detection (risks that operators might otherwise miss) and enables much faster footage review for real-time and post-event investigation.

In the US, being able to share critical information about facilities, including mapping, is PASS-recommended best practice for some institutions.

Question: Do I have to have specific cameras to benefit from AI and analytics?

No. Most security and operations management platforms now offer built-in analytics and AI tools or integrate with third-party analytics software. Using cameras with 'edge-based analytics' capabilities can help reduce server and network infrastructure requirements. However, cameras with higher resolution (4K and above) are advisable where detail is critical to risk detection.



3. Workflows and automation

When alerts are triggered (including those linked to analytics), workflows pair the risk identified with corresponding action by delivering on-screen instructions that guide operators through the most appropriate next steps. All in line with your institution's Standard Operating Procedures (SOPs). Workflows can also automate specific response protocols for even greater efficiency and consistency.

4. Remote access to information

Remote access solutions allow authorised people outside the control room to securely access important information relevant to their duties and roles – from teachers, support staff, maintenance and grounds teams, to security guards and external personnel, including law enforcement and emergency responders.

There are two main types of remote solutions to be aware of:

What	How It Works	Perfect For
Secure web access	These solutions use a WebRTC (Web Real-Time Communications) application to enable communication between devices, mean that authorised users can securely access data and key system functionality from authenticated mobile devices connected to the web.	Internal info sharing Individuals and teams can view live footage, recorded footage, receive alarms, and access reports based on specific job role and clearance level.
Cloud-based sharing	Incident lockers and digital evidence management capabilities held in the cloud offer a fast and secure mechanism for sharing video footage and critical data.	External info sharing This solution doesn't give system access but does allow authorised users to receive and send data in real time via devices connected to the cloud.

ASK: Your surveillance provider may offer dedicated mobile app capabilities to support specific remote access functionality and task assignment and completion reporting capabilities.

Secure Perimeters, Parking, and Grounds



Effective, multi-tiered security starts outside. Identify and respond to security risks beyond the front door.

Parking areas and campus grounds can often be overlooked in security planning, yet they are critical zones where students, staff, visitors, and property assets are potentially vulnerable.

Incidents such as theft, attacks, anti-social behaviour, and unauthorised access frequently occur in these peripheral areas. What's more, detecting risks and suspicious events here can often prevent small events from becoming major incidents.

Detect suspicious vehicles and behaviours

High-definition cameras integrated into the security and operations management platform can monitor parking lots, drop-off zones, and open spaces 24/7.

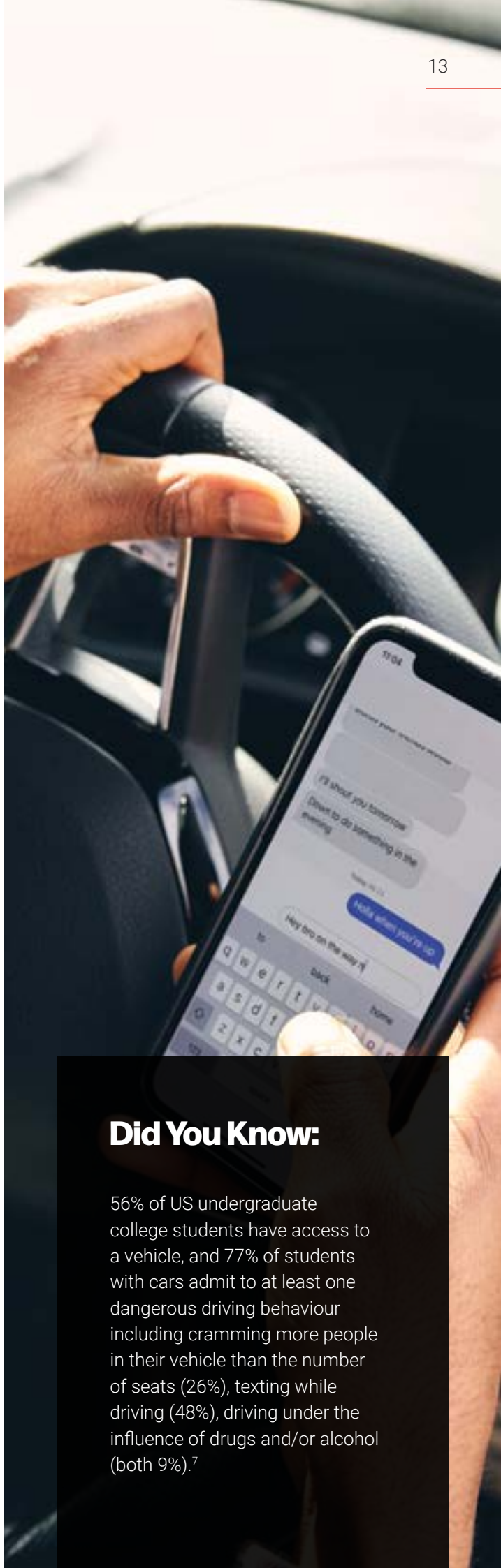
With AI-powered analytics, the system can automatically detect unusual or unwanted activity such as loitering near entrances or pick up points, erratic driving, tailgating, or movement in restricted areas. License plate recognition (LPR) further enables vehicle tracking and can be used to trigger real-time alerts against blocklisted plates.

Crowd formation is a useful AI tool for campus grounds. While often harmless, crowds can indicate an issue e.g. students gathering around a fight, anti-social behaviour or even a medical emergency unfolding.

Inform security teams and patrols

When an anomaly is detected, your unified platform can instantly alert campus security personnel. These alerts may include live video feeds, GPS coordinates, and suggested response protocols (workflows). Mobile dispatch solutions ensure patrol guards receive alerts on the go, via tablets or smartphones, allowing them to view live feeds and respond in real time.

⁷ [https://www.valuepenguin.com/college-students-cars-survey#:~:text=Most%20undergraduate%20students%20\(56%25\),16%25:%202011%20to%202013](https://www.valuepenguin.com/college-students-cars-survey#:~:text=Most%20undergraduate%20students%20(56%25),16%25:%202011%20to%202013)



Did You Know:

56% of US undergraduate college students have access to a vehicle, and 77% of students with cars admit to at least one dangerous driving behaviour including cramming more people in their vehicle than the number of seats (26%), texting while driving (48%), driving under the influence of drugs and/or alcohol (both 9%).⁷



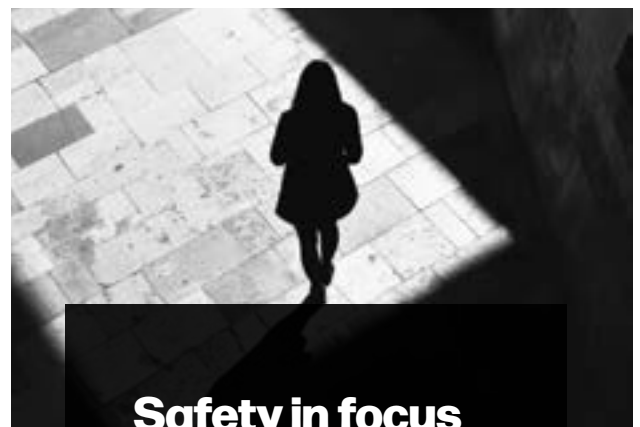
Control and monitor parking access

For gated and staff-only areas, your solution can manage access credentials, automatically open barriers for authorised vehicles, and deny entry to unauthorised ones. Integration with ID systems, such as RFID-enabled car discs and badges, means seamless access for staff and registered students, while temporary permissions can be assigned for events or visitors.

Vehicle analytics can track occupancy in real time. If a capacity threshold is reached, the system can automatically trigger alerts to open overflow areas. It can also notify security teams if any vehicles remain after hours for follow-up.

Automate patrols of campus grounds

Pre-configured camera tours or 'virtual patrols' can simulate regular sweeps of internal and external areas. This allows your team to maintain wide-area visibility while reallocating personnel to active threats or other alerts, such as well-being check-ins and duty tasks.



Safety in focus

Use video analytics to automatically detect lone individuals on campus grounds after dark so that security operators can virtually escort them to safety.



Detect and respond to vandalism

Vandalism of vehicles, property, and infrastructure is a frequent issue for campuses. AI-based video analytics can identify suspicious behaviour patterns, such as loitering, specific gestures like spray-painting, or scene changes.

When detected, alerts can be dispatched not only to security teams, but also to maintenance staff to enable rapid cleanup.

Maintain clear lines of sight

Video analytics can also be used to detect debris – for example tree foliage – that may be obscuring access to certain areas or a clear line of sight for security purposes. Alerts can then be issued to groundskeepers to resolve the issue.

Benefits and Outcomes

- **Improved student and staff safety** during early mornings, late evenings, and events.
- **Reduction in theft, vandalism, and unauthorised access** across parking and outdoor areas.
- **Faster, more coordinated emergency response**, especially in large or multi-campus institutions.
- **Data-driven decision-making**, enabling facility managers to identify high-risk zones or recurring issues.

Verify and Locate Visitors, Students, and Staff

Know who's on site, where they are, and what they can access.

A modern, unified security and operations management platform equips schools, colleges, and universities with the tools to identify everyone on campus, monitor their movements, and control access to facilities, all in a secure and consistent manner.

Why This Matters:

Knowing who is on campus – and where – is critical for accountability, first responder coordination, and communications.

Check visitor credentials and track movement

Integrated visitor management systems simplify and secure the entire visitor journey – from check-in to departure. When connected to your unified security and operations platform, these systems can:

- Automatically verify identity
- Cross-reference external and internal watchlists
- Flag unauthorised individuals in real time

Your solution will ensure every access attempt is logged, supporting post-incident investigations and policy enforcement.

Screen for:

Registered sex offenders

Known or wanted criminals

Individuals linked to previous issues on campus

False appointment claims

Authorised or unauthorised caregivers and guardians

By integrating with:

External database

External database

Internal database

Internal diary system

Internal database

Temporary access and smart badging

You can also issue time-limited badges or mobile credentials (e.g., RFID, QR codes) that:

- Restrict access to designated areas
- Expire after a defined time window
- Enable real-time location tracking via your unified platform

This ensures guests and contractors are accounted for and flagged if they overstay or access unauthorised areas.

Spotlight: Public Access Events and Shared Facilities

Public events like sports games or community programmes are vital to campus culture – and budgets. Facilities such as gyms, theatres, and halls may also be open during evenings or weekends.

Your security and operations management solution can help balance openness with security and safety by:

- Setting up virtual perimeters around restricted zones
- Prioritising alerts in areas where presence is unexpected
- Deploying additional checks for event-specific entry points

This multi-layered approach helps protect students and staff while maintaining the community-friendly atmosphere campuses are known for.



Student and staff badge integration

Integrating student and staff ID badges into your unified security and operations management solution will also help you create a seamless and secure campus experience. More than just a form of identification, smart credentials become powerful tools for access control, time tracking, and incident response. These include:

1. Access Control

Assign role-based access permissions to ensure that students and staff can only enter areas relevant to their studies, duties or class schedules. For example, ensuring only specific staff and students can access laboratories and research facilities.

Consider using facial recognition to ensure that a person's face matches their ID or access credentials to prevent unauthorised access via stolen or misused badges.

2. Automated Attendance Logging

Use badge scans at building entry points or classroom doors to automatically log attendance, reducing administrative burden and improving accuracy.

3. Zone Monitoring

Know who is where in real time. The system can raise alerts if individuals enter highly secure or hazardous zones without authorisation e.g. server rooms, maintenance areas, equipment storage facilities, and labs.

4. Emergency Response Integration

In lockdown or evacuation scenarios, quickly generate a real-time roster of who is on campus and their likely locations (visitor logs can also be included) critical for first responders.

5. Lost Badge Protocols

Instantly deactivate lost or stolen badges via the centralised platform and issue replacements while preserving existing access profiles.

What type of badge or credential should I use?

There are a few different options, each with their own specific benefits. Here's a quick summary of solutions you could integrate to, and manage with, your unified solution.

Credential type	Features
RFID cards	Widely supported, durable, low-cost.
Mobile credentials	Convenient app-based access using smartphones or wearables.
QR code badges	Good for temporary and one-time use; ideal for events or short-term staff, visiting lecturers etc.
Biometric-linked ID	Combines traditional ID with fingerprint or facial verification for high-security zones on campus.

Benefits of a unified badge system

By consolidating visitor, student, and staff credentials into your larger security ecosystem, you create a foundation for smarter, safer campus operations – without sacrificing user convenience.

- Reduce friction in daily campus operations
- Enhance situational awareness for security teams
- Simplify credential management across departments
- Support audit trails for compliance and investigations



Keep Students and Staff Safe

Quickly spot events and behaviours that pose a potential risk to the safety and wellbeing of students and staff.

Today's campus environments face a broad spectrum of safety challenges – from security threats and unauthorised access to disruptive behaviour, bullying, and health-related concerns and emergencies.

A unified security and operations management platform equipped with intelligent analytics, integrated systems, and automated workflows can help educators identify and respond to these issues rapidly and appropriately, while also creating a deterrent effect.

Detect and deter weapons-based crime on campus

In an era where campuses must be prepared for the possibility of weapons-related incidents, integrating metal detectors or knife arches into a broader unified security platform adds a vital layer of defence.

- **Trigger real-time alerts:** Notify security personnel immediately when a potential weapon is detected.
- **Link with surveillance cameras:** Auto-cue nearby surveillance feeds to record and display the incident, providing context and visual verification for faster response.
- **Log detection events:** Store incident data (time, location, response actions) to support investigations, policy reviews, and compliance audits.
- **Restrict access based on detection:** Interface with access control systems to automatically deny entry if a metal detector is triggered and not cleared.



Fact:

The use of knife arches in schools by one UK local authority was shown to reduce violent crime by 47%. A study in London also found that walk through metal detectors made 79% of students feel more reassured⁸.

Monitor for signs of bullying or aggression

Not all threats come from external sources. Bullying, harassment, and aggression among students – or even between staff and students – can have a major impact on campus life. Leverage video analytics tools as part of your unified solution to:

- Detect instances and repeated patterns of physical confrontation and hostile behaviour – including shouting (acoustic sensors), hand gestures, pushing, etc.
- Identify groups forming in unusual or restricted areas (a common precursor to incidents), or moving as a group in an unusual direction.
- Use loitering detection and crowd density monitoring (people-counting) to flag areas that require human supervision.
- Automatically save video footage and other relevant data to an ‘evidence locker’ when incidents are suspected, supporting policy enforcement and student safeguarding investigations.

Suicide prevention

Sadly, suicide is the second leading cause of death for college-aged individuals worldwide and in the US⁹, and in 2024, 75% of English colleges recorded more than five attempted suicides within the previous 12 months¹⁰.

While no technology can replace the role of mental health professionals, integrated security systems can play a supportive role in identifying warning signs and enabling timely intervention. Advanced video analytics can monitor for behaviours that may indicate distress, such as repeated visits to isolated areas (e.g. rooftops, stairwells, or restricted access zones), lingering near high-risk locations, or prolonged inactivity in unusual places.

Spot health and well-being risks

Beyond physical threats, campuses also face behavioural challenges that affect student well-being. AI tools integrated with surveillance systems can support detection of:

1. Vaping, smoking and drugs

Environmental sensors placed in bathrooms or common areas can detect chemical signatures from e-cigarettes or smoke and trigger real-time alerts. AI-based video analytics can also be used to flag behaviours congruent with drug dealing.

2. Signs of bullying or harassment

Advanced audio and video analysis can recognise repeated aggressive posturing and physical confrontations. Audio integration via cameras can also pick up distress cues such as raised voices, crying, or calls for help in hallways, cafeterias, or outdoor spaces.

3. Anti-social or isolated behaviour patterns

Behavioural trend analysis over time can highlight students repeatedly isolated from peer groups or exhibiting escalating conflict patterns – potentially enabling early intervention from counsellors or staff.

4. Accident and injury indicators

AI-powered video analytics can be used to identify falls, trips, and slips, and unusual postures or immobility. Smart workflows then trigger automatic alerts and coordinate the appropriate level of response from the right support personnel.

8 Are Knife Arches in UK schools necessary? | School Metal Detector

9 <https://pmc.ncbi.nlm.nih.gov/articles/PMC8130819>

10 <https://www.aoc.co.uk/news-campaigns-parliament/aoc-newsroom/colleges-reveal-the-scale-of-the-suicide-and-mental-health-crisis-in-new-aoc-research>



Investigate Incidents Quickly

Use AI and other tools to simplify and speed up investigations into incidents and allegations.

Fast footage review

While preventing incidents from occurring and detecting events quickly is the primary aim of safety and security measures, enabling fast and thorough investigation of reported incidents is also crucial.

AI-based tools can be a huge help. As well as allowing control room teams to apply search filters – such as vehicle type, face matching and clothing attributes – the integration of analytics also enables rapid footage review by presenting objects and events of interest (that appeared over the course of the filtered time period) on-screen simultaneously.

This can dramatically reduce the amount of time and effort needed to investigate and interrogate footage, especially on large campuses.

Tools are available that further speed up footage review using natural language processing. This allows users to search massive volumes of footage with intuitive, descriptive queries.

For example: ‘Show all footage of men wearing a red sweater, jeans, and a baseball cap during x time period.’



Incident type: attacks and assaults

Security management tools also play a critical role in investigating reports of attacks or assaults. A unified solution leveraging AI can be used to:

- Cross-reference reports with access control logs, emergency calls, or witness accounts to identify the approximate time and location of the incident. With AI tools then applied to filter footage to that window.
- Identify and track victims, suspects and witnesses across multiple cameras using facial recognition and clothing attribute search.
- Reconstruct the events leading up to and following the incident. This can confirm whether an encounter was random or targeted.

Incident type: thefts

Theft is one of the most widely reported crimes on any campus. Security teams can use AI-based footage filtering to quickly:

- Find certain objects, e.g. stolen bicycles or backpacks.
- Hone in on relevant footage for identifying suspects, e.g. 'show me anyone leaving the locker rooms at this location carrying a bag.'



Focus On: Corroborating or refuting claims against teachers or students

Claims relating to any kind of misconduct by teachers, lecturers, or any other authority figure responsible for the education and well-being of students in their care have to be taken very seriously. It's also a highly contentious issue. Genuine issues need to be addressed quickly. But careers can be damaged by false accusations.

In the UK, a government study revealed that nearly half of serious allegations against schoolteachers were unsubstantiated, malicious, or unfounded. Specifically, out of 2,827 allegations against teachers, 1,234 were found to lack merit.

A unified security and operations management solution can help you handle these cases with speed and impartiality.

- By providing time-stamped video evidence, security and operations management tools can play a crucial role in either corroborating or refuting claims. Whether it's reviewing classroom behaviour or verifying the presence and actions of individuals during reported incidents, recorded footage (and audio in some cases) offers clarity when emotions and memories may conflict.
- AI-powered search capabilities streamline investigations to quickly locate relevant footage based on time, location, or descriptive filters. This not only protects potential victims by enabling prompt responses but also safeguards staff and students from the long-lasting impact of false or mistaken allegations.
- Handled with care and confidentiality, this kind of evidence-backed process reinforces trust, transparency, and fairness across your institution.

Faster response to footage requests

Security and operations management tools that help you identify and share relevant footage faster can be invaluable in efficiently managing footage requests from external parties, such as Data Subject Access Requests. These tools can include cloud evidence management to securely share footage requests on a permission-based and time-limited access.

In the UK this might be related to UK GDPR compliance. In the US, the Family Educational Rights and Privacy Act (FERPA) specifically classifies surveillance footage relating to a specific student as part of their education record and as such, this footage can be requested by parent for review.

This applies to schools, universities, and other educational institutions.



Top Tip:

Consider using privacy protection tools to blur the faces of anyone who is not the subject of the access request. In some cases, this is a mandatory requirement.

Manage and Improve Emergency Response Scenarios

**Make sure the right people
get the right information and
assistance in a crisis. And
that the students and staff
know exactly what to do.**

When a crisis unfolds – whether it's a medical emergency, fire, lockdown, or active threat – seconds matter. In these moments, fragmented systems and unclear communication can lead to confusion, delays, and increased risk. A unified security and operations management solution ensures critical information flows instantly and securely to those who need it most.

By integrating video, access control, communication tools, alarms, and response protocols into one cohesive solution, educational institutions can remain calm, coordinated and procedurally compliant in a crisis.

Key Capabilities for Emergency Response

Automated lockdown triggers

Initiate full or partial lockdowns instantly based on real-time inputs, such as panic button activation, gunshot detection, or unauthorised access attempts.

Live video and location data

Give security teams and first responders immediate visual context and geolocation data to assess the threat and locate affected individuals.

Mass notification integration

Trigger pre-configured alerts via email, SMS, PA systems, lighting, and mobile apps, all from a single platform – with tailored instructions for students, staff, and emergency personnel.

First responder access and briefing

Grant police, fire, or medical teams controlled, time-limited access to video feeds and floorplans – even before they arrive on site – ensuring they're prepared to act as soon as they enter.

Incident command tools

Assign roles, coordinate response teams, and track activity in real time from a centralised platform, eliminating risk of duplicated actions or confusion that could delay timely response. This can be particularly useful where incident response involves multiple parties.

With your unified solution, every action, from system triggers to human responses, is logged and time-stamped for post-incident review and legal or regulatory reporting.

What kinds of emergencies can my system support?

Scenario

Unified Solution Capabilities

Active shooter or terror threat	Lockdown buildings, alert staff and authorities, track movement via cameras
Medical emergency	Alert and dispatch medically trained personnel on campus. Support emergency responders such as paramedics with maps and footage
Fire, smoke, or other hazard detection Individuals linked to previous issue on campus	Trigger building-specific evacuations, control access points, highlight evac routes with lighting/announcements
Severe weather	Issue campus-wide shelter-in-place instructions, monitor shelter areas
Missing student	Use ID badge location data, video analytics, and access logs to support search. Trigger alert notifications to relevant parties

Spotlight on: missing students

Being able to locate a missing student fast is critical for any campus security team. Here's how a unified security and operations management platform could help.



Scenario: A student has not returned to class and has not been seen for several hours.

Step	Action	System Tools Used
1	Trigger Internal Alert: The teacher notifies the front office, which immediately flags the case in the unified platform as a potential missing person.	Incident Reporting Tool / Internal Alert Workflow
2	Lock Down Entry and Exit Points (optional based on policy): If abduction or danger is suspected, perimeter doors can be temporarily locked.	Access Control Integration
3	Review Student Location Data: Pull badge scans or mobile credential history to identify the student's last known location.	Smart ID / RFID Badge System / Access Logs
4	Search Surveillance Footage: Use AI-assisted search tools to track the student's movements across campus cameras.	Video Surveillance and AI Video Analytics
5	Send Internal Notifications: Alert key individuals e.g. security, teachers, support staff etc. with photos and last-seen data.	Remote access and mobile solutions
6	Check Nearby Risk Zones: Flag areas like rooftops, stairwells, and remote buildings for immediate review. Loitering or lingering analytics may offer clues.	Behaviour Detection and geofencing alerts
7	Alert Parents/Guardians: Notify authorised contacts with verified updates. If necessary, notify local authorities with live access to video and location data.	Remote access, mobile solutions and integrated comms.
8	Log Incident Details: All actions, alerts, and footage are automatically logged for reporting and follow-up.	Incident Management & Audit Log Tools



Learn from Drills to Improve Outcomes

Emergency drills, from fire evacuations to active shooter or terror threat scenarios, are vital to campus safety and preparedness. But their true value lies not just in running them, but in learning from them.

A unified security and operations management platform can help in several ways:

1. Capture and review drill performance

Use recorded video and system data to analyse how students, staff, and security teams responded during the drill. Did people follow evacuation routes? Were there delays or confusion? Surveillance footage provides a clear, objective view of what happened and where procedures broke down.

2. Identify bottlenecks and blind spots

Video analytics can highlight areas where congestion occurred, exits were blocked, or people ignored alarms. These insights help refine protocols and adjust signage, access control settings, or staff placement.

3. Integrate access and communication logs

By linking surveillance with access control and communication systems, you can see how quickly lockdowns were triggered or how effectively alerts were broadcast. This end-to-end view helps assess the coordination and timing of your response.

4. Train more effectively

Footage from drills can be used in future training sessions to illustrate real scenarios, reinforcing correct procedures and showing where improvements are needed. It turns each drill into a learning opportunity.

5. Benchmark progress over time

Compare footage and response data across multiple drills to track how your team's readiness improves, and demonstrate compliance with safety regulations.



Manage Multiple Sites and Mobile Services

Centralise security management for campuses, districts, and mobile operations.

For educational institutions with multiple campuses or satellite facilities, or those responsible for mobile services like school transport, fragmented approach to security can lead to gaps, inefficiencies, and higher risk.

Cloud technology and web-based client solutions offer a practical way to bridge this gap, providing secure, flexible access to security and operations management platforms from any internet-connected

device. This enables both real-time oversight and rapid response, even across geographically dispersed sites.

From district-level school systems to universities with remote buildings or separate halls of residence, administrators and security personnel can monitor, manage, and respond from a single, secure interface.



Centralised command and control

View and manage all surveillance feeds, access controls, visitor logs, and alerts from one central platform – accessible securely from anywhere, via web or mobile app. Even during off-hours or at facilities with minimal physical security presence.

Cross-site access management

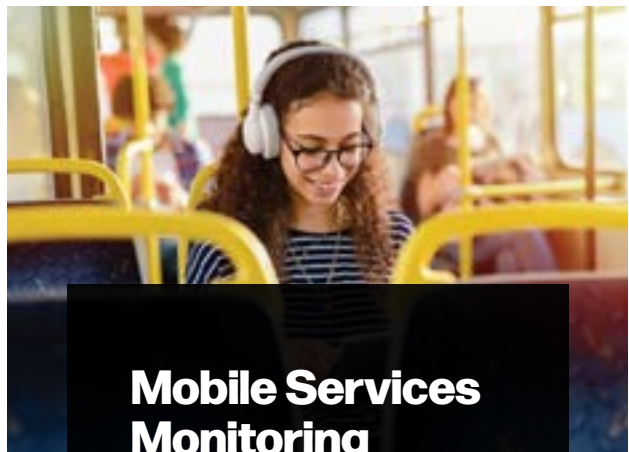
Apply consistent access policies across sites. Issue and revoke credentials centrally, and customise permissions by role, location, or time of day.

Live status and response

Instantly check system health, device connectivity, and event history across locations. Dispatch personnel or notify local responders with a few clicks.

Remote incident response

Investigate security alerts and review footage remotely in real time – reducing response time and eliminating the need to be physically present at each location.



Mobile Services Monitoring

Integrate GPS-tracked mobile units such as school buses into your unified view. Features include live vehicle tracking, on-board camera feeds, driver ID verification and behaviour monitoring, student boarding and disembarkation logs via smart card or facial recognition.

Protect Privacy and Data



Ensure that student, staff, and public privacy is protected at all times. And that your data is always secure.

Control who sees what

Monitoring must be conducted in a way that aligns with educational standards, ethical considerations, and data protection regulations. To achieve this, work closely with your technology provider and request solutions that support the following:

- **Permission-based access:** ensure your platform uses role-based access, so only employees with the appropriate clearance can view certain footage, access sensitive data, or use high-level system functions. This limits exposure and helps maintain trust among staff, patients, and the wider public.
- **Automated redaction:** modern AI-powered systems can automatically detect and redact or blur identifiable features such as faces or license plates displayed in footage, in real time or during post-event reviews. This protects individuals' identities during routine monitoring and when footage is shared for training, investigation, insurance, or legal purposes.
- **Built-in audit trail functionality:** your platform should include a robust audit trail system that logs every user action – what was accessed, when, by whom, and why. This not only supports accountability and transparency, but also provides a valuable tool for training, compliance reviews, and demonstrating adherence to data protection frameworks.

Protect your data from vulnerabilities

Educational facilities are also increasingly common targets for cyber-attacks. In addition to ransomware cases, common incident types include unauthorised access and email compromise.

It's crucial that your unified security and operations management solution doesn't present a weak link in the cyber security chain. With this in mind, here are some essentials to look out for.

Your cyber security checklist

- **Multi-layered protection:** Firewalls, intrusion detection systems (IDS), and up-to-date virus scanners to safeguard your network perimeter.
- **Standards compliance:** Full adherence to modern cybersecurity protocols and data privacy regulations (such as GDPR or FERPA).
- **Automated configuration audits:** Built-in tools to flag risks like default passwords, missing updates, or inactive workstation lockdowns.
- **End-to-end encryption:** All data, whether at rest or in transit, should be encrypted. For evidence transfer, include hashing to verify data integrity.
- **Multi-factor authentication (MFA):** Ensure both users and connected devices are validated through robust MFA protocols.

With these foundations, your system becomes an integral part of your cyber defence strategy, not a liability.

¹¹ 61% higher education institutions experience a negative outcome, such as a loss of money or data from any breaches or attacks.

Quick Fact:

50% of higher education institutions in the UK, and 3 in 10 further education colleges report experiencing breaches or attacks at least weekly. 61% higher education institutions experience a negative outcome, such as a loss of money or data from any breaches or attacks¹¹.



Spotlight on: data retention

While there is no one specific law dictating how long schools, colleges or universities should keep surveillance footage, data protection regulations and best practices strongly influence retention periods.

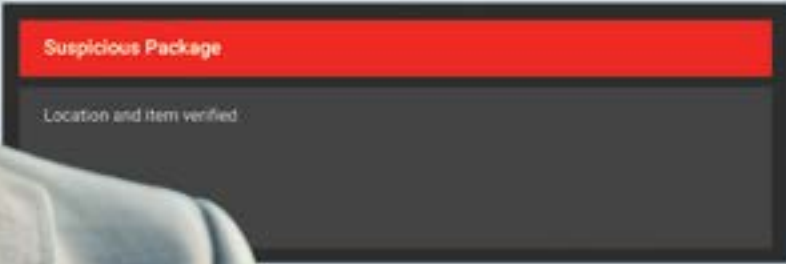
Generally, footage should be retained for between 30-90 days, but the specific duration depends on various factors, including local regulations, storage capacity, and the purpose for which the footage is stored.

Ask your solution provider about automating footage retention in line with your specific requirements. You should be able to customise settings allowing you to record, retain and lock down footage for specific time frames, by the individual camera, zone, or universally across your whole campus.

A Platform for the Future

The right unified security and operations management solution doesn't just protect, it empowers. Streamlining critical safety tasks and enhancing situational awareness, it helps your team detect, respond to, and reduce threats in real time – safeguarding students, staff, visitors, assets, and data.





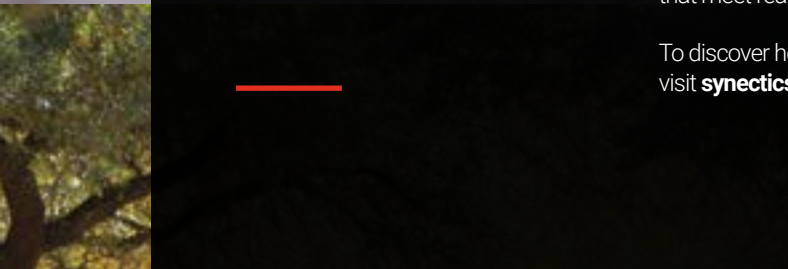
Designed with adaptability in mind, these platforms support seamless integration of new technologies as your needs evolve. That means you can expand capabilities without replacing your core investment, ensuring long-term value and future-ready transformation with minimal disruption.



Let's Talk

With extensive experience supporting complex campus environments, Synectics partners with educators to create tailored, scalable solutions that meet real-world challenges.

To discover how we can support your organisation visit synecticsglobal.com.



Specifications subject to change. E & OE.

Literature Reference: CAMPUS/EB Iss 1
Copyright © Synectic Systems Group Limited 2025.
All Rights Reserved.

SYNECTICS

synecticsglobal.com