



## **Partner Alliance for Safer Schools**

### **WHITE PAPER: Digital Mapping and 911**

*The volunteers who make up the Partner Alliance for Safer Schools (PASS) bring together their research and expertise from the education, public safety, and industry communities to develop and support a coordinated approach to make effective use of proven security practices for schools. The PASS team is also dedicated to developing white papers on specific school-safety topics.*

*The content in these white papers may point to specific products, brands, or organizations as illustrations of how certain safety and security measures are implemented. PASS does not endorse specific products or brands. Together, the volunteers and partners of the PASS share a single vision: making all schools safer is both achievable and urgently needed.*

---

#### **AUTHORS**

Contributing Authors: Laurie Anderson, Senior Advisor — Emergency Comm. & Response, TSG Advisors Public Safety; Dan Craigie, Director of Government Affairs, GeoComm; Sylvia Ifft, Executive Director & Co-Founder, National Institute for School Safety Policy; and Scott Lord, Solutions Consultant, ECC, Inc. & Co-Chair of the Technical Committee for PASS

#### **KEY TOPIC**

Alyssa's Law, digital mapping, studying requirements and processes for implementation of panic alarms, collaborating among agencies and school personnel, choosing the right technology, and training.

#### **PROBLEM SOLVED**

Digital mapping of a school campus provides vital information to first responders in cases of school emergencies. In turn, this enables a targeted, and effective response from emergency personnel to preserve the safety and security of all staff and students on a given campus.

## RELEVANT PASS GUIDELINES SECTIONS

- Introduction
- District-Wide Layer
- Digital Infrastructure Layer
- Policies and Procedures Component
- Communication Component
- Detection and Alarms Component

## MOST RELEVANT FOR

- K-12 school administrators
- School and district security leaders
- Facilities leaders
- Information technology professionals
- 911 and public safety communications professionals
- Law enforcement and first responders
- School safety policymakers

## TIME TO READ

Approximately 18 minutes

---

## Executive Summary

Panic buttons are beneficial—when they’re understood. This timely and practical white paper unpacks how laws such as Alyssa’s Law are driving the rapid implementation of panic button technology, and why there is no single, consistent solution that works for every environment.

The white paper explores the real-world challenges behind these fast-moving deployments: systems being rolled out before a full plan is in place, or before the correct team of people can be matched with the appropriate technology. The white paper also explores manufacturers and integrators navigating new territory without comprehensive implementation frameworks, and the often underestimated complexities of integration with public safety answering points (PSAPs) and 911 centers. We’ll examine why 911 center approval is essential, where coordination commonly breaks down, and how misalignment can undermine even the best intentions.

Digital maps can provide advantageous situational awareness by helping responders understand where an emergency is occurring and what they may encounter when they arrive. Depending on the needs of the school and responding agencies, mapping information may include building layouts, room numbers, entrances, access points, emergency equipment, security systems, cameras, utility information, and other relevant data.

The value of this information depends on its accuracy, accessibility, and usability.

Schools should also recognize that implementation is not the end of the process. Buildings change, rooms are repurposed, technology evolves, personnel change, and emergency response procedures may be updated. Digital mapping data and associated emergency systems should therefore be constantly updated, maintained, and incorporated into ongoing training and exercises.

Successful implementation of digital mapping begins with a strategic approach:

- Build the right team.
- Engage 911 and emergency responders early, and start building those relationships.
- Define the alert and response process before selecting technology.
- Start with established standards and leading practices.
- Once the mapping team is identified, select technology that supports the school's and community's operational needs.
- Consider interoperability and integration.
- Train everyone who interacts with the system.
- Test the technology and the process.
- Maintain accurate, up-to-date information.
- Continuously evaluate and improve the system.

Technology can provide valuable information during an emergency, but technology alone does not create an effective response. The most successful approach brings together people, and identifies their strengths and roles within the mapping process. Then, information and technology can be used to ensure that the right information reaches the right people at the critical moment.

---

## **Why This Topic Matters**

“If you’ve seen one school, you’ve seen one school.”

Seconds matter during an emergency. Traditional emergency communication may identify that an emergency is occurring at a particular school, but responders may still need to determine where the emergency is occurring within a building or campus and what conditions they may encounter when they arrive. Digital mapping provides a way to add context and situational awareness beyond simply pinpointing the location of a 911 call. It also gives examples of information that may be included, such as

door numbers, AEDs, fire extinguishers, utility shutoffs, cameras, and links to camera feeds. The quicker the help can be deployed to the area of need, the more lives can be saved.

---

## **Learning Objectives**

By the end of this white paper, readers should be able to:

- Define digital mapping and understand the benefits of the panic alarm process and how to get the right information to the right people during an event. Readers should also understand the operational impact on 911, how to manage digital map data, assign responsibility with implementation and accountability, train staff on panic alarm processes accordingly, and treat digital map maintenance as an ongoing process to be updated immediately upon changes to the campus landscape.
- 

## **Introduction: A Strategic Approach to Digital Mapping and Emergency Alerting**

The goal of digital mapping is to get the right information to the right people at the right time. When integrated into an effective emergency response process, digital maps can provide information that impacts the strategy of first responders to support faster access to vulnerable areas of a campus. Digital mapping and panic alerting act as part of a larger emergency response ecosystem; technology cannot stand as the sole solution.

---

## **The Evolution of School Emergency Alerting**

Alyssa's Law is accelerating conversations about school emergency notification systems and the power they give school personnel to summon help quickly during an emergency. The evolution of state laws has expanded the focus well beyond a simple panic button or alarm system.

First, emergency alerting has moved from fixed devices toward mobile solutions—and more accessible solutions—that may be easily reached or physically carried by school personnel.

Second, legislation and implementation strategies have increasingly emphasized the need to integrate emergency alerts with other safety infrastructure, including digital mapping and public safety communications systems.

Third, requirements have improved how emergency information is communicated to building occupants, through audio and visual notification capabilities. They have increased the emphasis on precise location information to provide better, and more accurate, information to the responders who need it.

## **What Is Digital Mapping, and Why Does It Matter?**

A digital map is not a duplication of a paper floor plan. Contextually, a digital map used in emergency response can provide advantageous information that helps responders understand the physical layout and environment of a school campus before and during an incident.

Depending on the school, responding agencies, and what technology, requirements, and mapping information is available, these digital maps may include:

- Campus and building layouts
- Room numbers and locations.
- Hallways and access routes.
- Doors, entrances, and other access points.
- Emergency equipment.
- Fire extinguishers.
- Automated external defibrillators.
- Utility shutoffs.
- Security cameras.
- Links or access to relevant security information.
- Other information that may support emergency response.

Information provided by digital mapping may help responders understand where an emergency is occurring or where the alert originated, and whether its location is changing. Digital mapping can also tell responders how to access the building or affected area, what rooms, entrances, or other landmarks are nearby, as well as what equipment or security resources may be handy, and what conditions they may encounter.

Digital maps shine as situational awareness tools, moving beyond building-level location information. They provide supporting information for emergency response teams, schools, and PSAPs.

## **Understanding the Legislative and Funding Landscape**

Despite these efforts, Alyssa's law and related legislation vary from state to state. Schools and districts should clarify the requirements in their jurisdiction before committing to an implementation strategy.

### Some requirement differences to watch out for:

- The type of panic alert technology permitted or required, and how it is procured
- Digital mapping and detailed location information
- Funding availability
- Whether mobile devices are required
- Integration with public safety answering point infrastructure
- Protocols for notifying school personnel, and indoor emergency notification
- The use of central monitoring or other emergency communications methods

Schools should not assume that a successful approach in one state presumes an identical result, requirement, or operational need in another.

---

### Build the Right Team

Digital mapping is most effective when it supports the needs of the people who will use the information. This includes the school, the public safety answering point, law enforcement, and other emergency responders. For this reason, a digital mapping discussion should not begin with the technology before the team is developed.

This type of emergency alerting is a collaborative effort. Digital mapping is a multi-step process, with multiple systems, organizations, and responsibilities. No single department should be expected to manage the entire process alone.

A successful team includes:

- School and district leadership
- School security
- Information technology, facilities, and operations
- Emergency management
- 911 centers, known as Public Safety Answering Points (PSAP)
- 911 industry organizations
- Law enforcement, fire, and emergency medical services (as needed)
- School safety organizations
- Vendors, integrators, and other implementation partners

The specific team will vary based on the school, district, jurisdiction, and technology being considered.

**An important lesson from the webinar is that stakeholders should be involved early.**

The people responsible for receiving, interpreting, and acting on emergency information should have an opportunity to explain how their systems and processes operate before technology decisions are finalized. This is particularly important for 911 and public safety communications personnel. A

technology solution may appear effective from the perspective of a school or vendor, but implementation may create challenges if it does not fit the operational environment of the public safety answering point.

Frontline telecommunicators can provide particularly valuable feedback because they understand how information is received and managed during actual emergency operations. Schools should establish relationships before implementation whenever possible. These relationships can support better communication during planning, implementation, training, testing, and future system changes.

---

## **Define the Process Before Selecting the Technology**

One of the most important recommendations from the webinar is to establish the emergency response process before selecting a technology solution. Technology should support the process; The process should not be unnecessarily redesigned to accommodate the limitations of a particular technology.

Before implementation, stakeholders should consider:

### **What Is an Alert?**

Schools should clearly define what constitutes an emergency alert.

Questions may include:

- What circumstances justify activation?
- Who is authorized to activate the system?
- Is the system intended only for a life-threatening emergency?
- Are there different alert types?
- How will personnel distinguish between different types of emergencies?

### **How Is the Alert Initiated?**

Stakeholders should understand how an alert is activated and whether the activation method is appropriate for the people who will use it.

Considerations may include:

- Fixed devices.
- Mobile or wearable devices.
- Applications.
- Classroom-based systems.
- Other approved technologies.

The system should be accessible and understandable to those expected to use it.

### **What Information Is Transmitted?**

Stakeholders should determine what information is sent when an alert is activated. Depending on the system and process, information may include:

- School identification.
- Building location.
- Specific room or area.
- Location of the person initiating the alert.
- Movement or changing location information.
- Additional emergency information.

The information should be relevant, understandable, and actionable.

### **Who Receives the Information?**

Schools should identify:

- Which information is sent to 911.
- Which information is sent directly to law enforcement or other responders.
- Which information is provided to school personnel.
- How information is shared among responding agencies.
- How digital mapping information is accessed.

### **What Happens Next?**

The response process should be understood from alert initiation through emergency response (and beyond).

A school may find it useful to map the workflow:

**Alert → Transmission → Receipt → Interpretation → Notification → Dispatch → Response → Ongoing Incident Management → Alarm Close/Demobilization → After Action/Documentation**

The exact workflow will vary, but documenting the process can help stakeholders identify gaps before an emergency occurs.

---

## Consider the Operational Impact on 911

Because emergency communications centers operate continuously, personnel need to consider that existing 911 operations might be flooded with calls from the same single event. A new alerting or mapping system does not exist separately from operational 911 facilities. Therefore, the call center becomes another component within an active environment that may already be receiving calls, texts, alarms, or other emergency information.

During a major school emergency, a PSAP may receive:

- Panic alerts
- Multiple 911 and mobile calls
- Automated notifications
- Intel from school personnel
- Information from other technology systems

Personnel should consider how the information will be received, processed, prioritized, and managed. More information is sometimes detrimental if it overwhelms the people responsible for processing it.

Schools and technology providers should work with PSAP personnel to determine:

- How alerts will enter the system and be displayed.
- Whether additional software or interfaces are required.
- Whether information can be integrated with existing systems.
- How telecommunicators will distinguish alerts.
- Differences among PSAPs
- Coordination of technology across districts and jurisdictions
- How to ensure information is actionable
- How testing will affect daily operations.

Testing needs to be carefully coordinated. Some states may require emergency alerting systems to be tested and incorporated into drills. Testing multiple schools or systems without previous coordination can create operational challenges, and therefore necessitate involvement from the public safety communications professionals in test scheduling and procedures.

---

## Select Technology That Supports the Process

Once stakeholders have established the desired process, they can evaluate technology solutions. As mentioned above, technology product decisions come last, after requirements have been determined.

Before engaging vendors or procuring digital mapping technological tools, schools should identify the capabilities needed to support their emergency response process. Additionally, they should also consider established standards and leading practices, such as what PASS provides in their Guidelines.

Questions for vendors, manufacturers, and integrators may include:

- What standards and leading practices inform the solution?
- How does the technology integrate with existing systems?
- How does information reach the PSAP?
- How is digital mapping information accessed?
- Does the solution require additional software or specialized interfaces?
- Can the system work with multiple responding agencies?
- How are technology updates managed?
- What training is provided?
- How will implementation be coordinated?
- What support is available after installation?
- How will ongoing maintenance be addressed?
- How are digital map updates managed?

---

## **Interoperability and Open Architecture**

Schools and public safety agencies may use different systems. Therefore, technology should be evaluated with interoperability in mind.

Where appropriate, stakeholders should consider vendor-agnostic approaches and open architecture that can support the exchange of information among different systems and organizations. The goal is not necessarily to create a single platform for every function. Instead, the goal is to avoid creating unnecessary barriers that prevent important information from reaching those who need it.

Schools should also consider the practical impact of requiring users to access multiple systems, applications, or screens during an emergency.

A solution that requires significant manual effort, extensive navigation, or is rarely used may be less effective during a time-sensitive incident.

---

## **Consider Infrastructure and Connectivity**

Technology is dependent on infrastructure.

Schools considering mobile panic alerts, wireless systems, digital mapping platforms, or integrated emergency communication technologies should understand the infrastructure necessary to support those systems.

Depending on the technology, considerations may include:

- Wireless coverage.
- Signal strength.
- Network capacity.
- System reliability.
- Building design.
- Areas with limited connectivity.
- Redundancy.
- Integration with existing communications infrastructure.

Wireless surveys and appropriate system design may be necessary to determine whether technology can operate effectively throughout the areas where it is intended to be used.

A system should not be assumed to work effectively throughout a campus simply because it functions in selected locations.

Testing and validation should include the full environment in which the technology will operate.

---

## **Build, Maintain, and Validate Digital Map Data**

Digital mapping is not a one-time project; school buildings and campuses change.

Rooms may be repurposed. Construction projects may alter access routes. New security equipment may be installed. Temporary spaces may become permanent classrooms.

These changes can affect the accuracy of information available to responders.

Schools should establish a process for:

- Identifying changes that affect mapping information.
- Reporting those changes.
- Updating the map.
- Validating the updated information.

- Communicating relevant changes to appropriate stakeholders.

Responsibility for maintaining the information should be clearly assigned.

A school should not assume that a map will remain accurate throughout the school year without active management.

Digital maps should also be incorporated into emergency planning and exercises.

If the information is intended to support responders during an emergency, stakeholders should confirm that it is accessible and useful during training and testing.

---

## **Establish Accountability During Implementation**

Complex projects can lose momentum when the responsibility is divided among multiple organizations and departments.

The webinar discussion highlighted the value of assigning a project lead to ensure that the implementation process is smooth from beginning to end. Depending on the organization, this person may serve as a customer advocate, lead, school advocate, or implementation coordinator.

Their duties may include:

- Coordinate all communication among stakeholders.
- Confirming that appropriate agencies are engaged.
- Tracking implementation milestones.
- Confirming system integrations.
- Schedule testing.
- Documenting maintenance responsibilities.
- Ensure the implementation process does not end at installation, and that outstanding issues are addressed.

The exact role may vary, but basic accountability should be clear.

Final stages of implementation are among the most crucial, because this is the point when stakeholders test the system to confirm that the technology, protocols, and people actually work together.

---

## **Train, Test, and Exercise the Entire Process**

Training should include everyone who interacts with the system. It is more than the person responsible for activating an emergency alert; anyone who interacts with the system or depends on the information it provides should understand their role.

### **Training may involve:**

- School administrators.
- Teachers and staff.
- Security personnel.
- IT personnel.
- Facilities personnel.
- 911/PSAP professionals.
- Law enforcement.
- Other emergency responders.

### **Training should address:**

- Defining appropriate use
- Building familiarity and muscle memory
- Testing the entire technology ecosystem
- Tabletop exercises
- Drills
- Full-scale exercises
- Coordinating testing with PSAP operations
- Evaluating and improving after exercises

Schools should avoid creating a situation in which personnel encounter a system for the first time during a life-threatening emergency.

Regular training can help create familiarity and build confidence.

The objective is to develop an understanding of the system and the process so that users are better prepared to respond under stress.

---

## **Test the Technology and the Process**

Testing should address both technology and operations. A system may successfully transmit an alert while another component in the overall process fails. For example, an emergency response process may involve:

- An alerting system.
- A mapping platform.
- A telephone system.
- An email or notification system.
- A Computer-Aided Dispatch System (CAD)
- Other communications or security technologies.
- Audio and visual emergency notifications to building occupants.

Testing should help determine whether each component functions as expected and whether the complete process works together.

Schools and responding agencies should consider multiple types of exercises, including:

### **System Testing**

Testing individual technology components and integrations.

### **Tabletop Exercises**

Allowing stakeholders to walk through an emergency scenario, discuss responsibilities, identify gaps, and evaluate decision-making.

### **Drills**

Incorporating the technology in emergency response drills such as active threat, severe weather, or earthquake.

### **Functional Exercises**

Testing specific functions or components of the emergency response process.

### **Full-Scale Exercises**

Testing the process from alert generation through emergency response, when appropriate and practical. Exercises should include the stakeholders who would participate in an actual emergency. The objective should not be simply to demonstrate that a button works. The objective is to determine whether the complete process works as intended.

**Following an exercise, stakeholders should evaluate:**

- What worked.
- What did not work.
- What information was useful.
- What information was missing.
- Whether responsibilities were clear.
- Whether the technology supported the process.
- What changes should be made.

Lessons learned should be incorporated into future training, procedures, and system improvements.

---

## **Maintain and Continuously Improve**

School safety and emergency response are not static. Technology evolves. Buildings develop. Personnel turn over. Public safety operations improve. Therefore, a successful implementation should also entail a continuous, cyclical process.

Some regular procedures for schools and districts to consider are:

- Ongoing maintenance
- Data updates
- Regular testing
- Adjusting processes and technology as needs change
- Updating digital maps.
- Validating information.
- Testing technology.
- Reviewing connectivity.
- Training new personnel.
- Conducting refresher training.
- Coordinating with 911 and emergency responders.
- Reviewing changes in legislation and requirements.
- Evaluating vendor support.
- Reviewing lessons learned.

Frequent and ongoing communication between the school, public safety partners, and technology providers is an important part of maintaining an effective system, as is a team's awareness of the data itself. Digital mapping data should be treated as a constantly changing, active operational resource, rather than a document that is created and immediately abandoned.

## **The biggest takeaway:**

**Do not start with the technology. Start with the people, the process, the information that needs to be communicated, and the desired emergency response—then select technology that supports that process.**

## **A Step-By-Step Checklist for Implementation**

Below is a helpful, 10-step checklist to help schools and districts who are considering the implementation of digital mapping and emergency alert systems. These steps follow a particular order based on the expert panelists' recommendations from the webinar:

### ☐ **1. Build the Right Team**

Identify the participants who will use, support, receive, or respond to the information.

### ☐ **2. Understand Local Requirements**

Review applicable legislation (Alyssa's Law) in your area, as well as regulations, available funding opportunities, and your district's operational requirements.

### ☐ **3. Define the Emergency Response Process**

Define what constitutes an alert, what information is needed (and how much information is too much), who receives it, and how the response will occur. Start building relationships with your public safety answering points (PSAP) now. Learn how they operate, what methods of reporting they prefer, and how they can support your team.

### ☐ **4. Identify Technology Requirements**

Develop requirements based on PASS guidelines' applicable leading practices to start, and interweave them into the established process according to local regulations.

## ☐ **5. Evaluate Solutions**

Consider ways to achieve smooth intraoperability, infrastructure, PSAP integration, usability, implementation support, training, and maintenance.

## ☐ **6. Implement with Accountability**

Assign responsibility for participants, and confirm that all components of the implementation are completed. Also, assign roles and responsibilities to match the strengths of school personnel. Assign a project lead to be in charge of upkeep of digital mapping and emergency systems. (See the “Establish Accountability” section above for a complete list of project lead responsibilities.)

## ☐ **7. Train the People**

Ensure that everyone who interacts with the system understands their role. This includes who reports an emergency, what and how much they should report, how to report, and what actionable steps to take after a report has been submitted. They also need to understand the process of the PSAP, and how a report will be displayed, both among personnel and for the different agencies involved.

## ☐ **8. Test the Technology and the Process**

Conduct pre-scheduled, coordinated testing and exercises involving appropriate stakeholders. This is also the role of the project lead—to schedule regular, pre-scheduled testing among PSAPs, 911, and other participating agencies.

## ☐ **9. Maintain and Validate**

Keep maps, systems, and procedures updated, current, and accurate as facilities, technology, and operations change.

## ☐ **10. Continuously Improve**

Use exercises, testing, stakeholder feedback, and lessons learned to constantly improve the process.

---

## Conclusion

Digital mapping and emergency alert systems can offer invaluable support to schools, emergency responders, and PSAPs. However, technology should never be step one.

The starting point is to identify the emergency response process in your specific jurisdiction, and then identify people involved in this process. This includes determining what information is needed, how that information will be communicated by your specially tailored team, and the best process by which to transfer said information to 911 professionals. This will establish how the information will support decision-making and emergency response.

Don't wait to establish relationships among your school personnel, 911 professionals,, emergency responders, technology providers, and even utilities and other stakeholders.

Only then should school decisionmakers choose which technologies can best support those needs.

Successful implementation requires collaboration among schools, 911 professionals, emergency responders, technology vendors, and other stakeholders. It also necessitates continuous monitoring after implementation. Digital maps must be maintained. Systems must receive continual evaluation and testing. Personnel must continue to be trained. Processes must be exercised and improved.

The ultimate objective is straightforward: During an emergency, the people responsible for making decisions and responding to the incident should have access to accurate, relevant, and actionable information to ensure safety and preservation of life on campus. By taking this strategic approach that prioritizes people and processes before technology, schools and their public safety partners can build systems that are most compatible with their infrastructure, which results in more reliable and effective emergency response.

---

## Resources

- Florida Legislature. "[Chapter 1006, Support for Learning](#)." *The Florida Senate*, 2025.
- Florida Legislature. "[Section 1013.13, School Safety Requirements for School Construction and School Mapping Data](#)." *The Florida Senate*, 2024.
- Oklahoma State Department of Education. "[Alyssa's Law — HB 4073 Information](#)." *Oklahoma.gov*, updated June 22, 2026.
- Partner Alliance for Safer Schools. *Safety and Security Guidelines for K-12 Schools*. 7th ed., 2025. [www.passk12.org](http://www.passk12.org)

- Texas Legislature. Senate Bill 838, “[Relating to School Districts and Open-Enrollment Charter Schools; Providing Silent Panic Alert Technology in Classrooms.](#)” 88th Legislature, Regular Session, 2023.
- New York State Senate. Senate Bill S2588, “[Requires School Safety Plans to Include Site Mapping for Emergency Response Data and Provides Guidelines for the Creation and Sharing of Digitized Maps With Law Enforcement.](#)” 2025-2026 Legislative Session.
- New York State Senate. Senate Bill S6410, “[Requires Panic Alarm Systems in Schools.](#)” 2025-2026 Legislative Session.
- U.S. Department of Justice, Office of Community Oriented Policing Services. [School Violence Prevention Program.](#)

### Additional Resources

- PASS School Safety and Security Checklist
- State school safety centers
- State and regional 911 offices
- Local public safety answering points
- Local law enforcement, fire, and emergency medical services
- Applicable Alyssa’s Law requirements (by state)
- School emergency operations plans
- District technology and facilities plans
- Relevant federal and state school safety funding programs

---

### Take the Next Step

To begin developing your comprehensive security roadmap, I encourage you to leverage the resources from the Partner Alliance for Safer Schools (PASS). The PASS School Safety and Security Guidelines and the accompanying PASS Checklist/Assessment Tool are designed to help you navigate today’s complex safety challenges by providing a framework to assess your current state, prioritize your needs, and make evidence-based decisions about your security investments.

Don’t navigate these challenges alone. Visit [www.passk12.org](http://www.passk12.org) to download the latest edition of the Guidelines and the editable Checklist. These tools will help you define your specific path to a safer, more secure environment for your students, staff, and community.