

Protecting Student and Staff Privacy



MUTUALINK K12 VIDEO SHARING

FERPA Compliant School Security Communications



“*The ability to instantly and securely share multimedia information in an emergency situation — including live video feeds, school building blueprints and police and fire radio to school radio and public address audio — is a potentially life-saving asset to first responders and the students and teachers they are protecting. The fact that Mutualink K12 ensures that all parties maintain control over their resources cuts down on time-wasting red-tape while protecting the privacy of everyone involved.*”

- **Patrick Fiel, Sr., former Executive Director of Security, District of Columbia Public Schools**

<https://thejournal.com/articles/2014/04/08/mutualink-gateway-device-links-schools-with-emergency-responders.aspx>

The Challenge.

In the face of heightened concern and interest in school safety, some districts have given law enforcement agencies remote access to school video surveillance systems for security monitoring. While well-intended, many school districts recognize that these arrangements raise serious student and staff privacy concerns and interfere with a school official's ability to use professional discretion in student disciplinary and behavioral matters. In particular, concern about “criminalizing schools” arises when incidents traditionally handled by schools escalate unnecessarily when police observe suspected behavior they assess as unlawful and feel duty-bound to act. Moreover, some law enforcement agencies have implemented intelligence-led policing initiatives which are perceived as information-gathering efforts intended to identify criminal associations and activities. These efforts include identifying tracking drug- and gang-related affiliations. Access to school surveillance feeds can enable the surreptitious collection of information regarding student activities, interactions and associations, some of which may not be criminal in nature but are inferred as such. This, in turn, may provide a pretext or basis for more opportunistic law enforcement intervention within the school.

Another side of this challenge is many law enforcement agencies do not have the resources to constantly monitor school surveillance feeds, heightening concern about missing or failing to identify a critical event resulting in liability. Reported cases of lapses in effective monitoring by police agencies resulting in loss of life amplify these concerns.

While school districts debate the desirability of providing police access to their surveillance systems a federal privacy law called the Family Educational Rights and Privacy Act of 1974 (FERPA) is already in place. It effectively prohibits general access to monitoring school environments, except in emergency situations. A FERPA-compliant solution to the video access problem requires implementing a system allowing for instant sharing when an emergency necessitates, but otherwise blocks police access to school video. Mutualink's patented emergency incident based, secure video sharing solution uniquely satisfies this requirement.

How Mutualink Works with FERPA.

FERPA is federal law implemented to protect student privacy. Mutualink is designed to be, and is accepted as being, compliant with applicable various legal privacy protection and confidentiality requirements. These include HIPAA, FERPA, state and local camera surveillance and access restrictions, and similar privacy and confidentiality laws.

Compliance is achieved through Mutualink's peer-based invitation and acceptance-based interoperability platform. The platform enables on-demand, secure sharing of video and bridging of communications between entities, such as a school and public safety agency, only when a party, such as school, voluntarily starts an incident and sends an invitation to the other party to join an incident session. Incident invitations to an outside agency may be manually initiated or auto-initiated (such as when a panic button is pushed) by a school in an emergency.

Invitations are dynamically-generated encrypted incident keys sent within an encrypted connection that enable an invited party to join an incident session. The invitation keys last only as long as the incident session lasts. Once a session is completed, no residual IP address, system login or access credentials or other means of accessing the video system remains. If no invitation is sent, no outside agency can access a school system's video platform. This sovereign invitation and acceptance-based model, coupled with a robust encryption and security framework, has enabled fundamental compliance in key areas that otherwise create significant barriers to compliance and functional usability in conventionally architected, server-based designed systems for purposes of achieving secure and flexible multiagency interoperability.

Mutualink's privacy control framework also includes selective sharing of cameras by the camera owner. Within an incident session, the owner (such as the school) retains control over what video may be accessed and shared with the outside agency. This enables, for example, correlated compliance with public safety and emergency response safe harbors under HIPAA and FERPA. Additional privacy protections exist as result of Mutualink's unique peer architecture model. Importantly, Mutualink does not store sensitive data. Rather, media and content are transported in real time between endpoints without trusted third party storage intermediation. The Mutualink system does not record endpoint communications or content. Events are logged in real time related to user functions, communications events (i.e., a user entering or leaving a session, an endpoint sharing video). Substantive content may be recorded by an endpoint agency using its existing recording and storage facilities which retains the then current compliance posture of the agency.

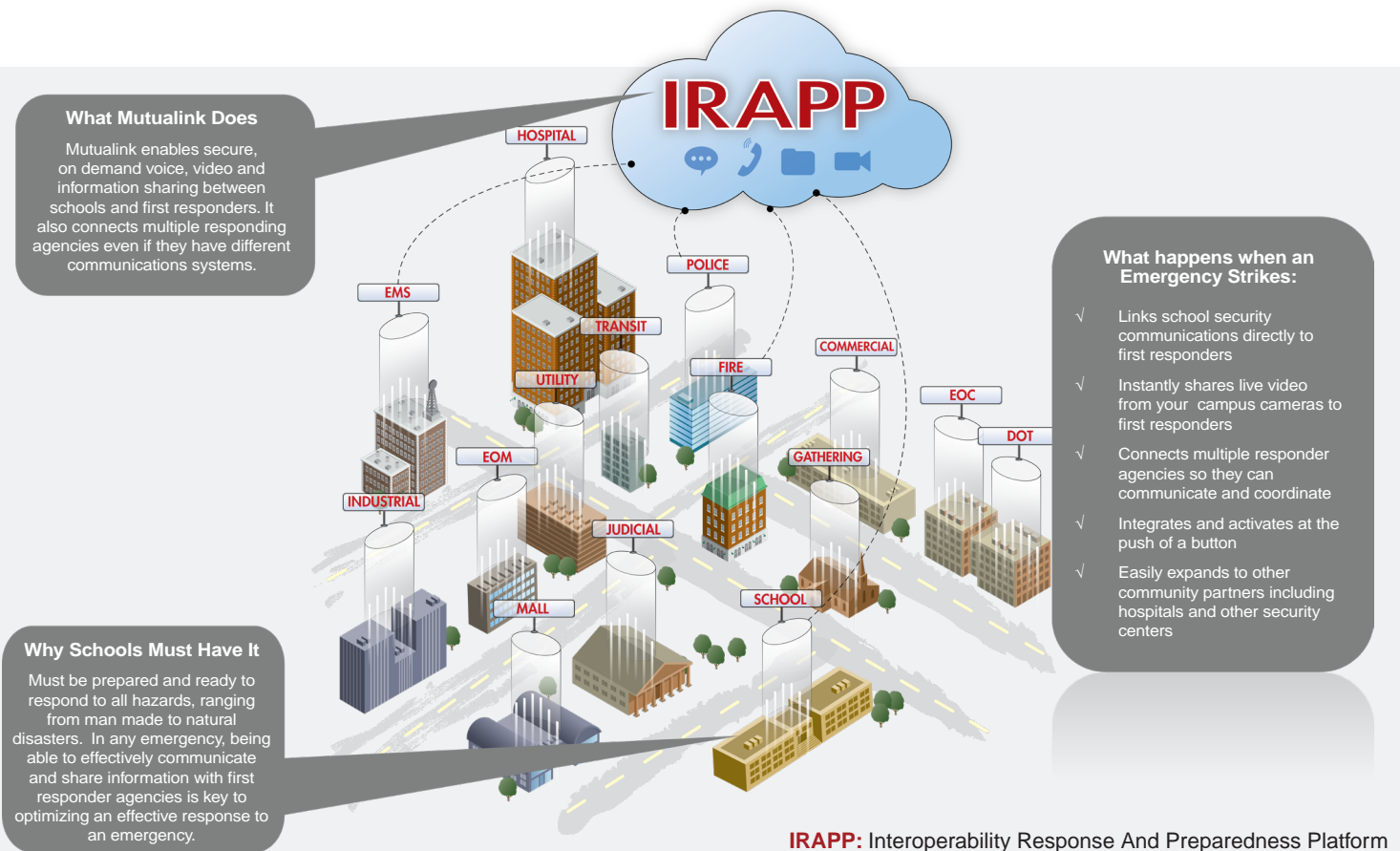
By contrast, many video surveillance platforms use a federation model that provides access credentials to an outside party via remote access or through an outside party's own video system. In effect, an outside party is given trusted-user access to another party's video environment. A classic federate use example is providing federated video system access between police and schools. Heightened compliance risks related to timeliness, controllability, accessibility and regulatorily-defined situationally allowable access exist in federated models of sharing. Those promoting federated video system solutions for police access to school videos rely on access logging, administrative access credential controls, and even rules-based access control to provide security. However, these implementations are ineffective and generally unsecure with, at best, after-the-fact audit mechanisms to detect improper access and use. Moreover, unlike with Mutualink, there is no owner-controlled real-time camera sharing control. Access is typically preset; the ability to stop view access by outside parties requires administrative access control, causing delay. Finally, the ability to control recording of video is unrestricted. In the school context, agencies can freely record any video stream to which they are given access on a continuous basis, whether or not an incident is occurring. This provides for unsupervised storage and monitoring of student behavior.

Mutualink Already in Use in Schools Around the County.

With respect to civil rights and public privacy matters, Mutualink is in use in various schools, law enforcement fusion and intelligence centers. It has been favorably viewed by privacy advocates, such as local ACLU organizations, because the system employs a selective information sharing model with information shared by an owning or possessing agency on a need basis, as opposed to a dragnet syndication and publication or wide access model. Likewise, agencies have been favorably disposed to this model because it allows limited and controlled situational access and sharing to sensitive information.



Mutualink is a DHS Safety Act certified antiterrorism technology. This designation provides limited liability for Mutualink and its customers relating to claims arising out of terrorism.

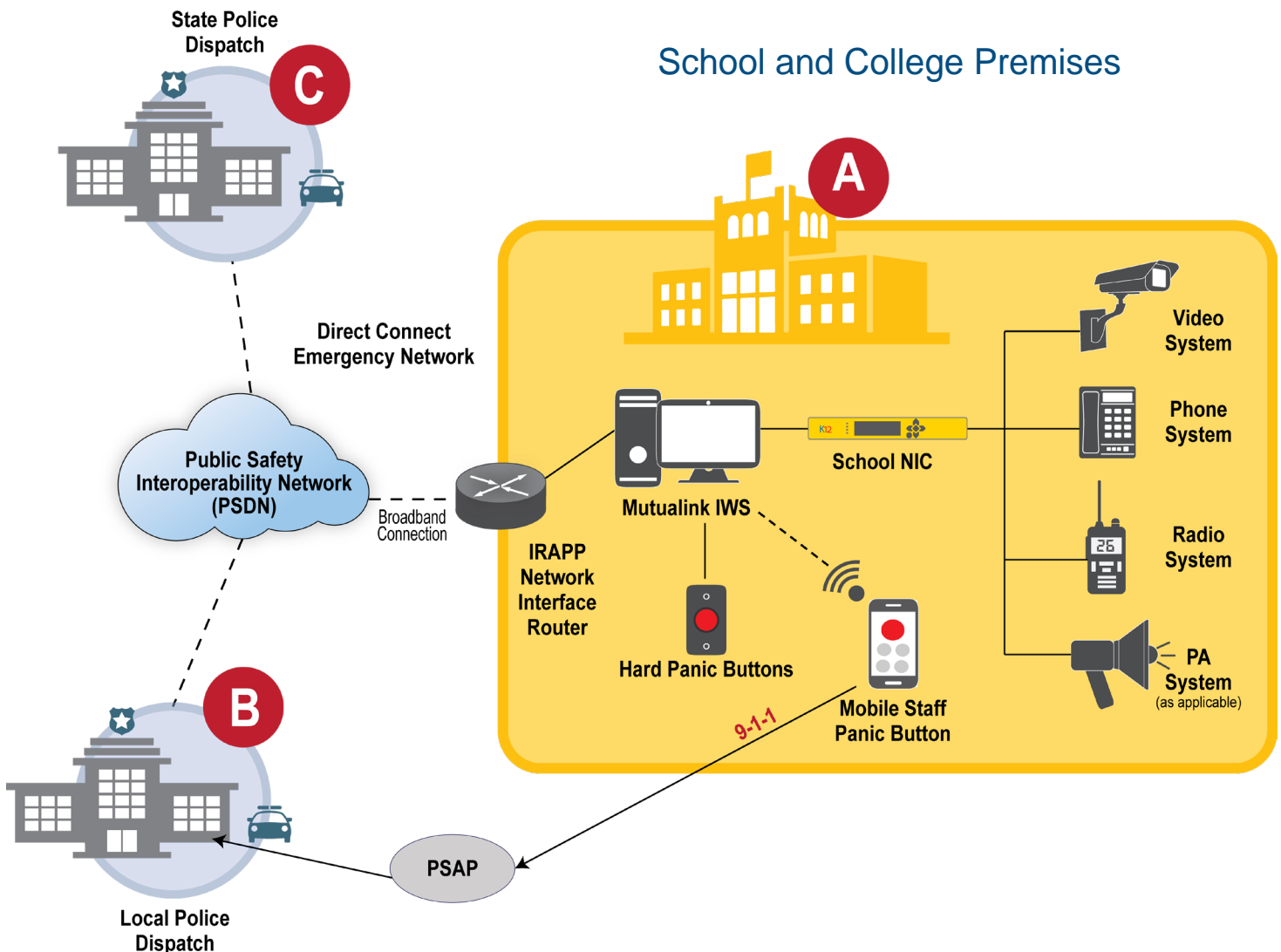


- ✓ Mutualink enables secure, on demand voice, video and information sharing between schools and first responders.
- ✓ Instantly shares live video from your campus cameras to first responders. The school decides when to stop sharing video.
- ✓ Complies with Federal and State Student Privacy Laws – incident-based permissive sharing vs giving school video system access credentials to police

With Mutualink, schools share video with law enforcement as and when needed through our invitation-based incident management system. The school shares video in one of two ways:

1. By initiating a Mutualink incident and inviting law enforcement (or others) to participate. Once the invited agency accepts, the school may initiate real-time video.
2. Automatically through a pre-programmed set of actions initiated by the activation of a panic button. Depending on the school's selected action, an invitation-based incident will be initiated, in which case video can be automatically shared upon acceptance; or an incident can be opened with automatic real-time video streaming.

In either case, the school decides when to stop sharing video and when to withdraw from the incident.



Commonly Asked Questions:

Q. We already have a Video System that our local police can access, isn't that good enough?

DISCUSSION. Your district may be in jeopardy of violating student privacy and confidentiality rights under the Federal Educational Rights and Privacy Act (FERPA) and may be in violation of state and local laws and regulations.

Problem 1: As a general matter, even within an agreement known as an MOU (Memorandum of Understanding), providing police agencies with log-in access to a school's surveillance system enables uncontrolled system access to look into a school's environment. If a potential criminal act is observed, police may be required to act or face liability. This method of access is prohibited in many districts that seek avoid criminalizing educational environments and students.

Problem 2: Police agencies that accept video access rights may become subject to liability for failing to adequately or properly monitor a school's video feeds.

ANSWER: Mutualink's patented secure invitation-based system only connects police to your video system when a school decides to allow access such as in an emergency. No remote access credentials are provided to the school's video system, providing maximum security. Instead, incident based encrypted access is given only for as long as the emergency requires.

Q. We have other security priorities such as installing panic buttons. Shouldn't that come first?

DISCUSSION. Panic buttons are popular security initiatives for schools. The problem is panic alarm without reliable communications between first responders and the school offers little value beyond providing location and basic information. This is the same information that is relayed in a 9-1-1 call, and arguably less in many instances. In most cases panic buttons alert others in the school, which is valuable in helping quickly lock down and shelter, but it does little to hasten fundamental resolution of an active threat.

ANSWER: Mutualink connects to panic button systems (fixed and mobile) and when activated, Mutualink will automatically connect the school with the police for immediate communications and also automatically begin sending video from the school to the police. This provides critical situational awareness that speeds response and resolution by knowing what is happening, where it is happening and who is involved in real time. When the school no longer deems it necessary to share video, they may stop sharing, thus complying with and respecting FERPA, as well as various state and local privacy laws and regulations.

Headquarters

1269 South Broad Street
Wallingford, CT 06492
(866) 957-5465

Research & Development Facilities

3 Lan Drive
Westford, MA 01886
(978) 392-0040

313 South Jupiter Road
Ste 110
Allen, TX 75002

Western Industrial Park
Rochelaise # 26 Bo. Guanajibo
Mayagüez, PR 00682



info@mutualink.net
www.mutualink.net