NATIONAL SCHOOL SAFETY AND SECURITY SERVICES
Experts You Can Trust!
www.schoolsecurity.org

School Safety Product and Technology Decision Checklist

An Independent Due-Diligence Tool for
Boards, Superintendents, and District Leadership

Prepared by:
Kenneth S. Trump, Ed.D.
National School Safety and Security Services
Cleveland, Ohio

Technology can support school safety.
It cannot replace supervision, judgment, training, or leadership.

This document is intended as a decision-support resource to guide thoughtful discussion and analysis. It is not a legal document, not exhaustive, and not intended to establish a legal or industry standard of care.

Version (1.0): January 6, 2026

EXECUTIVE SUMMARY

School Safety Product and Technology Decision Checklist

For Boards, Superintendents, and District Leadership Teams

School safety product and technology decisions are often made under pressure—after a high-profile incident, during a limited funding window, or in response to persuasive vendor claims. In these moments, districts may confuse **action with effectiveness**.

This checklist is designed to slow the process down—not to delay safety, but to ensure **sound, defensible decision-making**.

What This Tool Is

This checklist is an **independent due-diligence framework** to help school districts:

- Clearly define the problem before selecting a solution
- Separate vendor marketing from operational reality
- Identify human, organizational, and system dependencies
- Anticipate failure modes and unintended consequences
- Understand legal, liability, and community trust implications
- Make transparent, well-documented decisions that can withstand scrutiny

What This Tool Is Not

- It is **not** a rejection of technology
- It is **not** a vendor evaluation scorecard
- It does **not** promote or oppose any specific product

Instead, it provides the questions responsible leaders should be asking **before** committing public funds and shaping safety expectations.

Why This Matters

No security product or technology:

- eliminates risk,
- replaces supervision or judgment,
- guarantees prevention, or
- removes legal responsibility.

Most school safety failures occur not because a district lacked technology, but because of other factors such as:

- unrealistic assumptions,
- unexamined limitations,
- human factors,
- and gaps between policy and practice.

How to Use This Checklist

Districts are encouraged to:

- Review this checklist **before** procurement or renewal
- Use it during board discussions and administrative planning
- Attach it to RFPs or internal decision records
- Revisit it after pilots, incidents, or system changes

Using these question as a starting point for deliberations could be a first step toward **reasonable, good-faith due diligence**, regardless of whether a district ultimately adopts a technology.

> *Technology should support people—not replace them.*
> *Sound school safety decisions are grounded in realism, not promises.*

SCHOOL SAFETY PRODUCT AND TECHNOLOGY DECISION CHECKLIST

An Independent Due-Diligence Tool for School Leaders & Boards
National School Safety and Security Services
Kenneth S. Trump, Ed.D.

> **Purpose:** This checklist is designed to help school districts begin informed, decision processes **before** purchasing, piloting, or renewing school safety products and technology.
> **Guiding Principle:** Technology can support safety. It cannot replace supervision, judgment, training, or leadership.

---

1. PROBLEM DEFINITION

(Start with the problem, not the product)

☐ What **specific problem** are we trying to solve?
☐ Is this problem **frequent, rare, or hypothetical** in our district?
☐ How is this risk currently addressed **without technology**?
☐ What evidence shows the problem is **not already mitigated**?
☐ Does this product/technology address a need **identified by an independent, comprehensive assessment** of the district's/school's security and emergency preparedness?
☐ Are we reacting primarily to:
  - ☐ A recent incident elsewhere
  - ☐ Media coverage

- ☐ Political or community pressure
- ☐ Grant or funding availability
- ☐ Vendor outreach

Red Flag: Buying security products and technology before clearly defining the problem.

---

2. CLAIMS & EVIDENCE

(Separating marketing from reality)

☐ What does the vendor **explicitly claim** the technology does?
☐ What outcomes are **implied but not guaranteed**?
☐ Are claims supported by:
- ☐ Peer-reviewed research
- ☐ Independent evaluations
- ☐ Real-world K-12 data (not simulations)

☐ Has the vendor disclosed **known limitations**?
☐ Are **false positives and false negatives** acknowledged and documented?
☐ Is the product or technology **designed specifically for PreK-12 school contexts** or is it designed for other settings and is now being sold to schools?
☐ Have we contacted **vendor-provided references AND independently spoken with other boards, superintendents, and administrators using the product or technology, including users not identified by the vendor**, to obtain candid, real-world feedback on its strengths and limitations?
☐ What do other school leaders say about the **vendor's history of technical support, repair and replacement, and ongoing service**?

Red Flag: "Trust us" answers or refusal to discuss limitations.

---

3. OPERATIONAL DEPENDENCIES

(What must go right for this to work?)

☐ Who must do the following and how will it be done:
- monitor alerts?
- interpret alerts?
- decide on action?
- initiate response?

☐ Is system effectiveness dependent on:
- ☐ Staffing levels?
- ☐ Training quality?
- ☐ Response time?
- ☐ Camera placement, lighting, or other equipment or technology?
- ☐ Network reliability?

☐ How does the system function:
- during class changes?
- during breakfast and lunch periods?
- after school hours, during athletic and extracurricular events, etc.?
- with substitute or short staffing?

Key Question: What **human action** ultimately determines success or failure?

---

4. FAILURE MODES & CONSEQUENCES

(Planning for when—not if—it fails)

☐ What happens if the system:
- misses a real threat?
- generates a false alarm?
- malfunctions or goes offline?

☐ Who decides:
- lockdown vs. no lockdown?
- evacuation vs. hold?
- other emergency preparedness response?

☐ What are the consequences of:
- unnecessary lockdowns?
- police response to false alerts?
- student or staff trauma?
- loss of community trust?

Red Flag: No documented plan for false activations or system failure.

---

5. HUMAN FACTORS & SCHOOL CULTURE

(Technology in real schools—not ideal ones)

☐ Will this technology:
- reduce staff vigilance?
- create over-reliance on alerts?
- displace security risks to other areas?
- shift responsibility away from active supervision?

☐ How will students, staff, and parents:
- understand the system's role?
- respond to false alarms, system failures, unintended consequences, etc.?
- continue reporting concerns to adults?

☐ Does this technology strengthen—or undermine—situational awareness and relationships?

Reminder: When you add new products or technology to your system, you likely alter other aspects of your systems.

---

6. LEGAL & LIABILITY CONSIDERATIONS

(After-action scrutiny matters. Consult legal counsel with these and other questions.)

☐ Does this system raise expectations of detection or response?
☐ If the system fails, how will the district explain:
- reliance on the technology?
- known limitations?

☐ Has legal counsel reviewed:
- vendor contracts?
- indemnification language?
- data ownership and retention, student and staff privacy, and discovery risks?

Critical Point: Technology does not eliminate liability—it may reshape it.

---

7. COSTS & OPPORTUNITY TRADEOFFS

(What are we not funding?)

☐ Total cost includes:
- ☐ Purchase
- ☐ Installation
- ☐ Training
- ☐ Maintenance
- ☐ Staff time
- ☐ AI, software, and related ongoing subscription renewals
- ☐ Renewal escalation

☐ What non-technology investments may be reduced or delayed?
- ☐ supervision
- ☐ staffing
- ☐ training
- ☐ threat assessment
- ☐ student support services

Key Question: Is this the **highest-impact** use of limited safety resources?

---

8. PILOT, REVIEW & EXIT STRATEGY

(Avoid permanent pilots)

☐ Is this a pilot or long-term commitment?
☐ What defines:
- success?
- failure?
- unacceptable disruption?

☐ Who evaluates results—the vendor or the district?
☐ Is there a documented **exit strategy** if performance is unacceptable?

Red Flag: No clear off-ramp.

---

9. TRANSPARENCY & COMMUNITY TRUST

(Before parents ask)

☐ How will this decision be explained to:
- parents?
- staff?
- students?
- media?

☐ Are we, as school leaders, raising unrealistic expectations within the school community?
☐ What will the district say:
- after a false alarm?
- if the system fails during a real incident?
- if the district has to reverse course, remove or stop using the product or tech?

☐ Is the district prepared to release performance data and incident records?

Trust is easier to maintain than to rebuild.

OPTIONAL SCORING RUBRIC (1–5 SCALE)

(For Board and Administrative Documentation)

This rubric allows districts to **document the initial consistency and quality of their decision-making**, not just the decision itself. Scores could be assigned collaboratively by district leadership and reviewed with legal counsel as appropriate.

Score each category from 1 (Poor / Unacceptable) to 5 (Strong / Defensible).

1. Problem Definition & Need Alignment

1 – Problem unclear; driven by external pressure or vendor pitch
2 – Problem loosely defined; limited local data
3 – Problem identified but scope or frequency uncertain
4 – Clear problem definition supported by district data
5 – Well-defined problem with documented risk history and priorities

Score: ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

---

2. Evidence & Claim Validation

1 – Claims accepted at face value; no independent review
2 – Limited evidence; reliance on vendor materials
3 – Mixed evidence; some independent information reviewed
4 – Independent data reviewed; limitations acknowledged
5 – Strong evidence review including failures, limits, and context

Score: ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

---

3. Operational Readiness

1 – Staffing, training, and response roles undefined
2 – Roles identified but not tested or realistic
3 – Basic readiness with acknowledged gaps
4 – Clear roles, training plan, and operational procedures
5 – Demonstrated readiness through drills, staffing plans, and oversight

Score: ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

---

4. Failure Mode Planning

1 – No plan for false alarms or system failure
2 – Informal discussion but no documentation
3 – Partial planning for common failures
4 – Documented procedures for failures and false activations
5 – Comprehensive failure planning with review and training

Score: ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

---

5. Human Factors & Culture Impact

1 – Human behavior impacts not considered
2 – Minimal consideration of vigilance or reliance issues
3 – General awareness of human factors
4 – Clear plan to support supervision and reporting culture
5 – Technology intentionally integrated to strengthen human performance

Score: ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

---

6. Legal & Liability Review

1 – No legal review conducted
2 – Contract reviewed only for cost
3 – Legal review conducted with limited operational input
4 – Legal counsel reviewed contracts, data, and liability implications
5 – Legal review integrated with operational and leadership planning

Score: ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

---

7. Cost–Benefit & Opportunity Tradeoffs

1 – Cost only considered at purchase stage
2 – Partial lifecycle cost awareness
3 – Costs understood but tradeoffs unclear
4 – Lifecycle costs and opportunity tradeoffs reviewed
5 – Clear justification as highest-impact use of safety resources

Score: ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

---

8. Transparency & Community Trust

1 – No communication plan
2 – Reactive communication only
3 – Basic messaging prepared
4 – Proactive, clear communication strategy
5 – Transparent plan including failure scenarios and data sharing

Score: ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

TOTAL SCORE (Max = 40)

Guidance (Suggested):
- **32–40**: Strong steps toward a decision process
- **24–31**: Proceed with caution; address gaps
- **Below 24**: High risk; reconsider decision or pause

FINAL DECISION CHECK

Before moving to next steps, leadership should be able to answer **yes** to all of the following:

☐ We know what problem we are solving.
☐ We understand the system's limitations.
☐ We have planned for failure modes.
☐ We understand legal and operational tradeoffs.
☐ This fits within a **people-centered safety approach**.

Closing Statement

Technology should support people—not replace them.
Sound school safety decisions are grounded in realism, not promises.

Disclaimer

This checklist is provided as a **general, non-exhaustive discussion tool** intended to help school administrators, boards of education, and other decision-makers **identify relevant topics and questions** when considering school safety technology.

It is designed to serve as a **starting point** to guide more detailed analysis, discussion, and decision-making. It is **not** intended to be an all-inclusive or comprehensive list of considerations, nor does it address every factor that may be relevant in a particular school or district.

This checklist is **not a legal document**, **not legal advice**, and **not intended to establish or define a legal, regulatory, or industry standard of care**. It should not be interpreted or applied as a strict, rigid guideline or checklist that must be followed in every circumstance.

Each school and school district is unique, with differing environments, resources, student populations, staffing, and community expectations. Decisions regarding school safety technology should be made based on the **specific facts, conditions, and needs of each district**, and in consultation with appropriate professional advisors, including legal counsel.

About the Author
Kenneth S. Trump, Ed.D., is President of National School Safety and Security Services (www.schoolsecurity.org), a Cleveland-based independent consulting firm specializing in PreK-12 school safety, security, emergency preparedness, and litigation support. He is not affiliated with or compensated by security technology vendors.

Version (1.0): ***January 6, 2026***