

# Visitor Aware Overview

Visitor and student management solutions



# The Visitor Aware Difference

---

- Five tools to enhance student and building safety, that feature:
  - ✓ **Visitor screening** using encrypted facial recognition
  - ✓ **No proprietary hardware** requirements
  - ✓ **Multi-site communication**
  - ✓ **QR codes** to easily identify and verify visitors
  - ✓ **Preregistration links**
  - ✓ **Safety drill scheduling**
  - ✓ **Real-time bus insights**
  - ✓ **Reunification** capabilities

# Visitor Manager

- Screen visitors and volunteers before granting them access
- Maintain digital records of visitors and volunteers
- Print badges to verify guests
- Track student tardies with digital records
- Release students to authorized guardians
- Assign temporary relationships permit non-guardians to pick up students



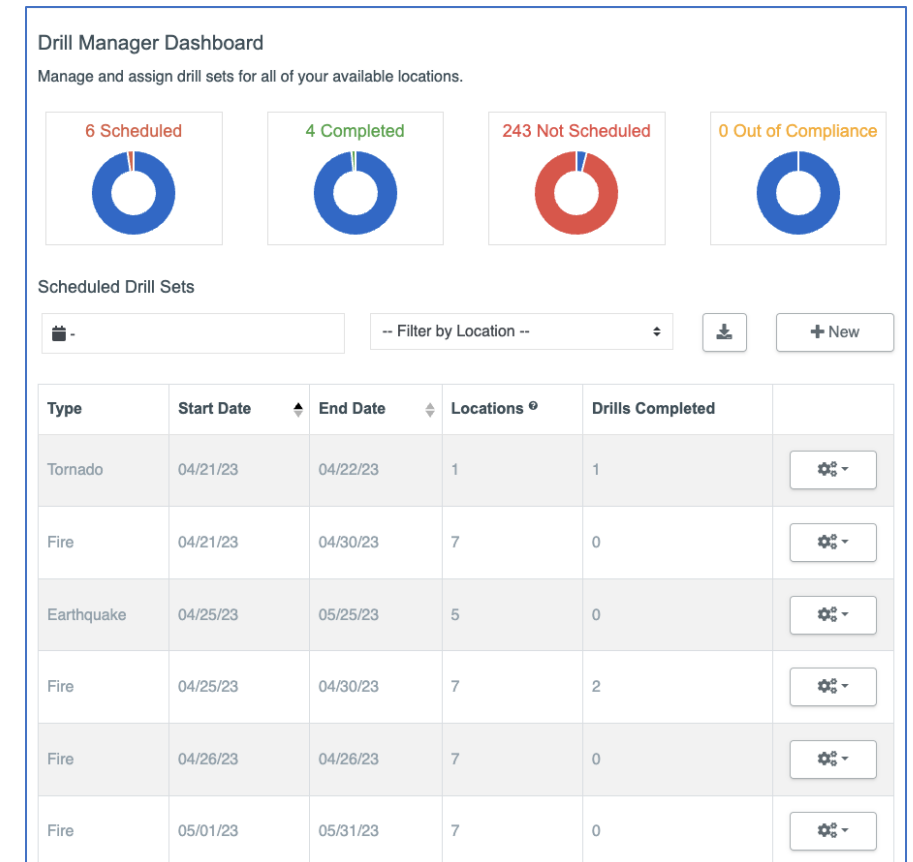
# Hall Manager (Coming Summer 2025)

- Digitally permit students to be excused from class
- Create restrictions around granting student passes
- Maintain digital student hallway activity log



# Safety Manager

- Schedule and assign drills across your district
- Monitor compliance and drill completion
- Maintain digital records to demonstrate compliance
- Submit tips about potential school threats
- Easily account for students and reunite them with guardians following an incident



# Dismissal Manager (Coming Spring 2025)

- Monitor and track student dismissal types
- Streamline the carpool line pickup process
- License Plate Recognition integration





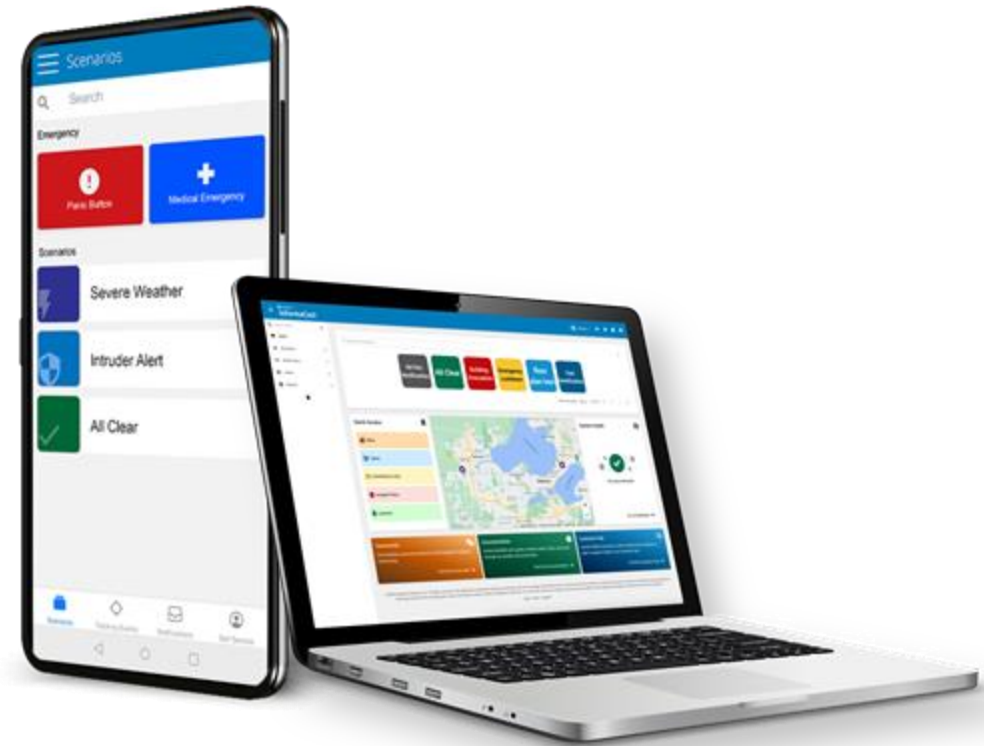
# Bus Manager

- Verify students get on the correct bus
- Share student bus location insights with guardians
- Know when students have gotten off the bus
- Use GPS to track bus and student locations in real-time



# InformaCast Integration

- Add mass notification and incident management capabilities
- Leverage text, audio and and visual notifications throughout a school
- Manage school bells and paging
- Automatically enroll visitors to receive notifications
- Initiate alerts when flagged guests attempt entry





# How is Data Secured?

- All data is:
  - Transferred securely using HTTPS
  - Stored securely in encrypted databases
- There are no publicly available documents, databases, customer uploaded files, or API endpoints.
- No unnecessary information is collected, and any unnecessary information that is sent is discarded.
- Only the minimum data is collected and used for students, guardians, visitors, volunteers, and staff.

# How is Data Secured? (cont.)

- This means:
  - No student photos are ever collected or used
  - No student social security numbers are ever collected or used
  - No behavioral health notes, student risk assessments, documents, health record, or other information is collected or stored
  - No PII in document storage for any reason, on any server
  - Visitor photographs are AES256 encrypted. Only the most recent photo is stored, and at each new visit the previous photo is securely destroyed.
  - Check-in devices such as iPad kiosks or web-kiosk do not store any information; all visit/visitor information is destroyed after each visit