Visitor Aware®

singlewire

HOW VISITOR AWARE SECURES YOUR DATA

As schools look to enhance safety measures with visitor management solutions like Visitor Aware, it is critical to understand how data is collected and secured. No school wants to expose themselves to risk due to lax security practices, which is why we've assembled this explainer on how Visitor Aware secures customer data.

HOW IS DATA TRANSFERRED?

Data is transferred securely using HTTPS (SSL connections) to and from all check-in devices, computers, and databases to Visitor Aware's secured, monitored infrastructure.

HOW IS DATA STORED?

Data is stored securely in encrypted databases, and high-risk PII (personal identifiable information) such as driver's license numbers, street addresses, and more are encrypted using AES encryption. All infrastructure logs are encrypted, secured, and rotated with continuous access monitoring, meaning the Visitor Aware team knows if the logs have been accessed, and logs may only be accessed by select internal infrastructure and security personnel.

WHAT'S PUBLICLY AVAILABLE?

Visitor Aware does not have any publicly available databases, customer-uploaded files, or API endpoints.

WHAT INFORMATION IS COLLECTED?

No unnecessary information is collected, and any unnecessary information that is sent is discarded. Visitor Aware collects only the minimum data used for students, guardians, visitors, volunteers, and staff.

WHAT DOES THIS MEAN?

These security measures mean Visitor Aware:

- Never collects or uses student photos
- Never collects or uses student social security numbers
- Never collects or stores behavioral health notes, student risk assessments, health records, documents, or other information
- Has no PII in document storage for any reason, on any server
- Uses AES256 encryption for visitor photographs. Only the most recent photo is stored, and at each new visit, the previous photo is securely destroyed.
- Securely destroys all visitor information that was collected during the check-in process from any kiosk device after securely transferring the data to encrypted databases via SSL and HTTPS.

Schools can have confidence that they are implementing a solution that provides strict visitor verification and secures the data it uses to do so.