Frequently Asked Questions: Data Collection and Security

Data Collection and Storage

What data is collected and stored when a visitor ID is scanned into the Raptor system?
The Raptor scanner collects the ID photo, name, date of birth, and the last four digits of the license number (the other digits are replaced with ***). If two or more visitors have the same first name, last name, and date of birth, Raptor uses the last four digits of the license number to differentiate between them. Only the minimum data needed to accurately identify an entrant is collected (i.e., no address information, no Social Security Numbers, no physical characteristic data, etc.). No other data is collected from the ID and no photocopy of the ID is retained.

What is the Raptor's data retention policy?
Raptor believes strongly that the all data belongs to the client. Client data is retained until the client requests in writing that the data be deleted. This deletion can be performed at any time, but cannot be undone.

Data Usage

How is the data used? To what purposes am I authorizing its use?
The data is used to ensure that the district/school maintains a log of all visitor and other entry data through the front office, and the district/school can instantly check that data against two databases: 1) a database of the registered sex offenders in all 50 U.S. states, and 2) a custom database populated by school administrative personnel which can contain entry alerts such as custodial orders, known gang members, etc.

Is the data shared with any third parties? If so, which ones and which data?
No data is shared with third parties.

Data Protection

How is the data protected?
In addition to requiring unique usernames and passwords for each user of the Raptor system, Raptor utilizes firewalls, intrusion prevention systems, host integrity monitoring, and port filtering as well as the latest security processes and procedures to protect all its systems. All information transmitted to Raptor's servers during the login/sign in process is encrypted using 256 bit AES encryption. Raptor utilizes a nationally-recognized cloud provider.

How is the datacenter physically secured? Do they collocate? If so, is the cage physically secured and how?

Raptor does not collocate, but rather uses a nationally-recognized cloud provider with decades of experience in datacenter security.

Is the data encrypted on disk?
The data is fully encrypted when in transit to and from the disk and when at rest.

How are all communications to the system and within components of the system secured?
All communications are fully encrypted when in transit using 256 bit AES encryption.

Data Access

Who has access to the data? What access do Raptor employees have to the data?
Raptor employees have different access to the data based on their job requirements and associated permissions. Access and permissions are controlled by unique usernames and passwords.

What access do district/school employees have to the data?
District/school employees have different access to the data based on their job requirements and associated permissions. Permissions by user level are set by the district/school. Front desk personnel generally are restricted to the ability to sign in/sign out entrants and generate reports.

Have all Raptor employees with access to private data been screened, and have they signed proper non-disclosure agreements (not just protecting Raptor's intellectual property, but with regard to the data collected and stored about individuals)?
All Raptor employees have been given full criminal background screenings and are required to sign a non-disclosure agreement that covers all areas of confidentiality prior to working at Raptor.

What are the password requirements for internal and external users (length, complexity, recycle, etc.)?
For both internal (Raptor employee) and external (Raptor client) users, password requirements include a minimum of 8 characters, upper case, lower case, symbol, and number.

Can a user review the data collected about them to ensure it is accurate?
Whether an entrant can review their data would be a policy decision on the part of the district/school and not a decision by Raptor.

Is the software open source or closed source?
Raptor's system is a proprietary application based on the Microsoft stack of tools and products.

Does Raptor have adequate quality assurance practices to reduce the likelihood of data leaking bugs?
Raptor has a dedicated Quality Assurance team responsible for the continuous review and testing of our product.

What is Raptor's disclosure policy with regards to discovered vulnerabilities and possible or actual leaks of data?

In the event of a possible or actual data leak, Raptor would immediately inform the District so that the District could immediately communicate to the parents/visitors. Raptor does not store the email and/or phone numbers of the parents/visitors.