DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

DATA SECURITY AND PRIVACY PLAN

Vendor's DATA SECURITY AND PRIVACY PLAN is as follows:

Raptor believes strongly that all data belongs to the client. Client data is retained until the client request in writing that the data be deleted. This deletion can be performed at any time, but cannot be undone.

The data that Raptor collects is used to keep a log of all visitors and other entry data. The Raptor system uses the visitor's first name, last name, and date of birth to check against two databases:
1) a database of registered sex offenders in all 50 U.S. states, and
2) a custom database populated by school administrative personnel which contains custom alerts such as custodial orders, known gang members, etc.

The Raptor scanner collects the ID photo, first name, last 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 a photocopy of the ID is not retained. No data is shared with third parties.

Raptor uses best practices in protecting data. In addition to requiring unique usernames and passwords for each user of the Raptor system, the system 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 the Raptor Technologies servers during the login/sign in process is encrypted using 256-bit AES encryption and utilizes a nationally-recognized cloud provider. The data is fully encrypted when in transit to and from the disk and when at rest. All communications are fully encrypted when in transit using 256-bit AES encryption.

Raptor limits data to those who need it. 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. 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 Technologies. District/school employees have different access to the data based on their job requirements and associated permissions. User permissions are set by the district/school. Front desk personnel are generally restricted to sign in/sign out entrants and generate reports.

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