Midland Independent School District

Raptor Visitor and Volunteer Management System FAQS

What is the Raptor System?

Raptor is a visitor management system that enhances school security by reading a visitor's drivers' license (or other approved government issued ID), comparing information against a sex offender database to alert school administrators and District police if a match is found. Once cleared through the system, a visitor badge is produced that includes a photo, name of the visitor, date & time, and destination. The Raptor system is designed to permanently replace paper sign in.

How does Raptor work?

Raptor compares government-issued ID information to a database that contains registered sex offenders from 50 states as well as local flags placed into Raptor by a school site. In the event of a match, Raptor alerts designated school officials.

What is the purpose of the Raptor system?

Raptor enhances and automates visitor management. By proactively alerting personnel to certain potential threats, Raptor allows school administrators and, at times the School Resource Officer, to take appropriate steps to keep our students, employees, and visitors safe. For approved visitors, the system prints visitor badges that include the visitor's name, photo, date, and destination. Badges enable personnel within the building to quickly determine if visitors are in areas where they should, or should not be.

Why is Midland Independent School District using this system?

The safety of our students and staff is our highest priority. Raptor will provide a consistent, standardized system to track visitors and volunteers. This is especially useful during emergencies to know who is on campus. The system quickly prints visitor badges that include a photo, the name of the visitor, time, date and destination.

Does the school/District have the right to require visitors, even parents, to produce identification before entering the school?

Yes, school officials are required to know who is in the building and why they are there, particularly when a student is involved (e.g. early pickup). School officials need to be able to confirm that an individual has the authority to have access to the student. In addition to requiring visitors to give their name and purpose for visiting, it also requires visitors to present proof of identity.

What types of IDs will work in Raptor?

Raptor is able to scan all U.S.government issued licenses,identification cards, concealed handgun licenses, permanent resident card, active military cards, and passport ID cards (not the full passport).

What other information is the school taking from driver's licenses?

Raptor is only scanning the visitor's name, date of birth, photo, and the last four digits from their ID card for comparison with a national database of registered sex offenders and any private alerts at the school, such as restraining/custody orders. Additional personal data will not be gathered and no data will be shared with any outside company or organization.

What does a visitor do if he/she doesn't have a government-issued ID?

Visitors without a government-issued ID will be required to either return with a valid ID or meet with a school administrator. The school administrator will determine access to the campus. If the individual is granted access they will be asked to provide their last name, first name, and date of birth for manual entry into Raptor.

Is an ID card scan necessary each time a person comes into the building?

Yes. All visitors, volunteers and contractors must present an approved ID each time you enter a building. The school receptionist is able to view the ID card picture in Raptor to make a visual verification of the person entering the campus.

What visitor information is stored in the Raptor database?

The database stores the following visitor information:

- Full name
- Date of birth
- First four digits of ID
- ID Photo

Will volunteers or employees have to be scanned into the Raptor System?

Volunteers must follow the same procedures as any visitor to a school or site. Identity must be verified with an acceptable form of identification (i.e. Drivers License, State ID, etc.). MISD employees who do not work at the specific site will be required to present their District ID or driver's license if they do not have their District ID. They are then entered into Raptor as a staff member either manually or by scanning their license.

Do vendors and contractors need to be scanned with the Raptor system?

Yes, all visitor's IDs need to be scanned.

Will the district scan police officers, firefighters, and other uniformed or similar governmental officials into the system?

If the visitor is a known, uniformed, government employee, no. If the visitor is not a known, and uniformed, government employee, yes. Again, this is to allow us to know who is in our schools at all times and to not assume people are who they say they are without providing proper identification. However, law enforcement personnel visiting campus on official business can be given the option to have their information entered manually by presenting their badge or state-issued identification.

Will I be required to complete this process if I am simply dropping off an item in the office for my child?

No, this process is only for persons wishing to enter the campus past the reception desk.

Are there less invasive ways to track visitors, who are usually moms, dads, and grandparents, without requiring them to scan their driver's license to gain access to one of our public school buildings?

The Raptor system strives to require as little information as possible from visitors while still being able to provide the school with the information needed to uniquely and accurately identify entrants and provide for enhanced safety at the school. The minimum information required is full name, date of birth, first four digits of ID, and photo. No other data is collected from the ID and no copy of the ID is taken.

What is the checkout process for Visitors leaving the building?

The checkout process doesn't involve scanning the card again.The receptionist will simply find the name of the person who is signing out and click a 'sign out' button. This provides a record of entry and departure and time on any campus. The visitor badge will be returned to the receptionist and destroyed.

What if a 'hit' on the system occurs? What is the protocol?

The staff member scanning the I.D. will contact an administrator immediately to confirm that the information is correct. No identified visitor with a positive sex offender 'hit' will be permitted onto the campus. Texas law provides the site administrator with the ability to grant limited, escorted

access to a campus where the identified visitor's child attends under specific circumstances and conditions.

How does Raptor keep its database up to date?

Raptor updates the registered sex offender database once per week. Any new publicly registered sex offenders are added to the database at that time and expired records are removed.

Who owns the data?

The district owns the data created by its use of the Raptor system (all visitor data, custom alerts, visitor logs, etc.). Raptor maintains ownership of the software and the sex offender database (used by all Raptor clients). Raptor does not use the data except as requested by the client (i.e., to create a custom report, etc.). The district may at any time terminate its relationship with Raptor and request that all data provided by TVUSD be copied to storage media and returned to the district or destroyed. In such an event, no backup or other copies will be maintained by Raptor. Raptor does not sell any client or demographic data to any outside entity and does not use that data for any purpose other than visitor management for TVUSD schools.

Is the system data secure?

Raptor Technologies utilizes some of the most advanced technology for Internet security available. Secure Socket Layer (SSL) technology protects the data using both server authentication and data encryption, ensuring that the data is secure and only available to the subscribing school or facility. The protected data is inaccessible to anyone not authorized to view the information. Strict access policies, 256-bit encryption, firewalls, and private secure bandwidth are in use to ensure the highest standards for our security requirements. Data is stored on the Raptor servers behind a firewall which requires a unique ID and password, through an operating system, which requires a second unique ID and password, and inside a database which requires a third unique ID and password.

Privacy of Information

Raptor Technologies, Inc. (Raptor) warrants that the confidentiality of data from our clients will be maintained according to all Federal and State laws, and any local policies that are communicated to us. Raptor acts as an agent and representative for the client in the storage, import, and/or analysis of data. Access to personally identifiable data will not be allowed for anyone other than Raptor staff directly responsible for the storage, import, and/or analysis of the data. Data will be provided by Raptor only to persons or entities authorized by the client. Data will be used by Raptor only according to the terms of our signed agreements.