

FACT SHEET: District Tech Directors

A Quick Guide to Data, Security, Systems Integration, and Network Requirements

Raptor Technologies®, the market leader in integrated safety technologies for K-12 schools, provides visitor management, volunteer management, and emergency management systems proven to help protect students and school staff. The Raptor® system helps schools and districts screen for registered sex offenders, manage custody issues, coordinate volunteers, and respond quickly and efficiently to emergencies. More than 32,000 campuses across the U.S. place their trust in Raptor Technologies. This sheet summarizes key technical facts of the Raptor system.

DATA COLLECTION, USAGE, AND SECURITY

The Raptor system scans any ID with a 2D barcode or MRZ, such as a state-issued ID or Mexican Consular Card, and only captures the minimum data necessary to positively identify a campus visitor (ID photo, name, date of birth, and the last 4 digits of the ID number). No other data is captured, and no photocopy of the ID is kept.

Data is used to ensure the integrity and accuracy of school and district visitor logs. The data will be instantly screened against the sex offender registries in all 50 states as well as any locally configured alert databases generated by district administrators. No visitor data is ever shared with third parties.

Data is protected with firewalls, intrusion prevention systems, host integrity monitoring, and port filtering. All data transmission is encrypted using 256-bit AES encryption.

Raptor Technologies believes that all captured data is property of the client school or district. Raptor Technologies retains client data until receipt of a written request from the client to delete.

SYSTEMS INTEGRATION

District Student Information Systems are easily integrated with the Raptor system through Raptor Link. After the district shares their SIS information with Raptor Link via Clever or ClassLink, Raptor imports that data into your Raptor system. Districts can also manually import data files or set up automated import using the Raptor Command Line Interface (CLI) import process. Student, approved guardian, staff, volunteer, and contractor data can be imported into the Raptor system. Visitor data cannot be imported. Clever, Raptor Link's systems integration provider, abides by all FERPA guidelines. Manual and CLI processes can also import selected .xls or .csv data files residing outside a district's SIS.

SUPPORTED OPERATING SYSTEMS AND BROWSERS

The Raptor® system works with the following operating systems and browsers:

- ▶ Microsoft® Windows® 7 Professional 64bit
- ▶ Microsoft® Windows® 10 Education or Professional 32bit or 64bit
- ▶ Microsoft® Internet Explorer
- ▶ Google® Chrome®

RECOMMENDED SYSTEM CONFIGURATION

Requirement	Recommended Configuration
Operating System	Microsoft® Windows® 10 Education or Professional 64 bit
CPU	Quad-Core, 3.5 GHz or better CPU (minimum Dual-Core, 3.0 GHz)
RAM	8 GB RAM or higher (minimum 4 GB)
Disk Space	200 MB
Graphics Card and Display	Capable of 1920 x 1080 (16:9) or 1280 x 1024 (4:3) resolution or higher
USB Ports	One physical USB port for each piece of hardware. Note: Raptor does not provide or support the use of third-party USB cables, external USB hubs, or extenders.
Internet Connection	High-speed Ethernet. Note: Using a wireless connection or a computer that only meets the minimum system requirements may result in delays during printing, scanning, transitioning between screens, and downloading reports.
Electrical Outlet or Surge Protector	Must be available for each printer to be installed

For software prerequisites and OS settings, power settings for Raptor USB devices, drivers (printing/scanning IDs), optional components (scan 1d and/or 2d barcodes, capture photos), and network requirements, consult Raptor Technical Support.

**For more detailed information about the
Raptor system, call us or visit our website.**