ORANGE-ULSTER BOCES
Learning for Life

ADDENDUM TO AGREEMENT
Regarding
Data Privacy and Security
In Accordance with Section 2-d of the New York Education Law

Including
Parents' Bill of Rights for Data Security and Privacy
AND
Supplemental Information

This Data Privacy and Security agreement is by and between Raptor Technologies with its principal place of business located 631 West 22nd Street, Houston, Texas 77008 ("Contractor"), and **Orange Ulster Board of Cooperative Educational Services**, with its principal place of business located at 53 Gibson Road, Goshen, NY 10924 ("OU BOCES"). Upon being executed by Contractor's and OU BOCES's authorized representatives, this Addendum shall be deemed to have been in full force and effect for the following school years 2024-2027.

WHEREAS, OU BOCES is an educational agency within the meaning of New York State Education Law, Section 2-d ("Section 2-d"), and Contractor is a third party contractor within the meaning of Section 2-d; and

WHEREAS, Contractor and its authorized officers, employees, students and agents shall have access to "student personally identifiable information (PII)," "student data" and/or "teacher or principal data" regulated by Section 2-d; and

WHEREAS, the provisions of this Addendum are intended to comply with Section 2-d in all respects. To the extent that any term of the Agreement conflicts with the terms of this Addendum, the terms of this Addendum shall apply and be given effect.

NOW, THEREFORE, it is mutually agreed that the Agreement is hereby amended in accordance with this Addendum, as follows:

1. Confidential Information

1.1 Contractor agrees that in performing the Original Agreement with the OU BOCES, Contractor may have access to confidential information in the possession of OU BOCES, including student, teacher or principal personally identifiable information ("PII"). For the purposes of this Addendum and the Original Agreement, it is agreed that the definition of Confidential Information includes all documentary, electronic or oral information made known to Contractor or developed or maintained by Contractor through any activity related to the Original Agreement. This Confidential information includes student, teacher and/or principal data (as the terms are defined under Section 2-d.)

1.2 Contractor agrees to comply with Section 2-d, and the corresponding regulations promulgated by the Commissioner of Education of New York ("Commissioner") thereunder. In addition, Contractor agrees to comply with any changes in Section 2-d, the Commissioner's regulations and relevant OU BOCES policy that may be amended or modified during the term of the Original Agreement. Upon request by OU BOCES, Contractor shall provide OU BOCES with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws.

1.3 Upon expiration of the Agreement to which this Addendum applies, without a successor agreement in place, Contractor shall assist OU BOCES in exporting all student, teacher and/or principal data previously received by Contractor from, or developed on behalf of, OU BOCES, and Contractor shall, at the request of OU BOCES, either securely delete any student, teacher and/or principal data remaining in Contractor's possession or return the student, teacher and/or principal data to OU BOCES. If student, teacher and/or principal data is to be maintained by Contractor for any lawful purpose, such data shall remain in an encrypted format and shall be stored on systems maintained by Contractor in a secure data facility located within the United States.

1.4 The parties further agree that the terms and conditions set forth in this Confidential Information section and all of its subparts shall survive the expiration and/or termination of the Original Agreement.

2. Data Inspection and Challenges to Data

Education Law Section 2-d and FERPA provide parents and eligible students the right to inspect and review their child's or the eligible student's PII stored or maintained by OU BOCES. To the extent PII is held by Contractor pursuant to the Original Agreement, Contractor shall respond within thirty (30) calendar days to OU BOCES' requests for access to PII so OU BOCES can facilitate such review by a parent or eligible student. If a parent or eligible student contacts Contractor directly to review any of the PII held by Contractor pursuant to the Original Agreement, Contractor shall promptly notify OU BOCES and refer the parent or eligible student to OU BOCES.

In the event that a student's parent or an eligible student wishes to challenge the accuracy of student data (pertaining to the particular student) that may include records maintained, stored, transmitted, and/or generated by Contractor pursuant to the Agreement, the challenge will be processed in accordance with the procedures of OU BOCES.

A teacher or principal who wishes to challenge the accuracy of data pertaining to the teacher or principal personally, which is disclosed to Contractor pursuant to the Agreement, shall do so in accordance with the procedures for challenging APPR data, as established by OU BOCES.

3. Training

Contractor represents and warrants that any of its officers, employees, and/or assignees who will have access to student, teacher and/or principal data pursuant to the Original Agreement will receive training on the federal and state laws governing confidentiality of such student, teacher and/or principal data, prior to obtaining initial or any further access to such data.

4. Use/Disclosure of Data

4.1 Contractor shall not sell or use for any commercial purpose student, teacher and/or principal data that is received by Contractor pursuant to the Agreement or developed by Contractor to fulfill its responsibilities pursuant to the Agreement.

4.2 Contractor shall use the student, teacher and/or principal data, records, or information solely for the exclusive purpose of and limited to that necessary for the Contractor to perform the duties and services required under the Original Agreement. Contractor shall not collect or use educational records of OU BOCES or any student, teacher and/or principal data of OU BOCES for any purpose other than as explicitly authorized in this Addendum or the Original Agreement.

4.3 Contractor shall ensure, to the extent that it receives student, teacher and/or principal data pursuant to the Agreement, that it will not share Confidential Information with any additional parties, including an authorized subcontractor or non-employee agent, without prior written consent of OU BOCES. Contractor shall indemnify and hold OU BOCES harmless from the acts and omissions of the Contractor's employees and subcontractors.

5. Contractor's Additional Obligations under Section 2-d and this Addendum

Contractor acknowledges that, with respect to any student, teacher and/or principal data received through its relationship with OU BOCES pursuant to the Agreement it is obliged to maintain a Data Security & Privacy Plan, and fulfill the following obligations:

- execute, comply with and incorporate as Exhibit "A" to this Addendum, as required Section 2-d, the Parents' Bill of Rights for Data Privacy and Security developed by OU BOCES;
- store all data transferred to Contractor pursuant to the Agreement by OU BOCES, in an electronic format on systems maintained by Contractor in a secure data facility located within the United States or hard copies under lock and key;
- limit internal access to student, teacher and/or principal data to Contractor's officers, employees and agents who are determined to need such access to such records or data to perform the services set forth in the Original Agreement;
- not disclose student, teacher and/or principal data to any other party who is not an authorized representative of Contractor using the information to carry out Contractor's obligations under the Agreement, unless: (I) the other party has the prior written consent of the applicable student's parent or of the eligible student; or (II) the other party has the prior written consent of the applicable teacher or principal; or (III) the disclosure is required by statute or court order, and notice of the disclosure is provided to OU BOCES no later than five business days before such information is required or disclosed (unless such notice is expressly prohibited by the statute or court order);

- use reasonable administrative, technical and physical safeguards that align with the NIST Cybersecurity Framework and are otherwise consistent with industry standards and best practices, including but not limited to encryption, firewalls and password protection as specified by the Secretary of the United States Department of HHS in any guidance issued under P.L. 111-5, Section 13402(H)(2), to protect the security, confidentiality and integrity of student and/or staff data of OU BOCES while in motion or in custody of Contractor from unauthorized disclosure;
- not mine Confidential Information for any purposes other than those agreed to in writing by the Parties. Data mining or scanning of user content for the purpose of advertising or marketing to students or their parents is prohibited; notify OU BOCES, in the most expedient way possible and without unreasonable delay, of any breach of security resulting in an unauthorized release of any PII. In addition, Contractor shall take immediate steps to limit and mitigate the damage of such security breach or unauthorized release to the greatest extent practicable, and promptly reimburse OU BOCES for the full cost of any notifications OU BOCES makes as a result of the security breach or unauthorized release. Contractor further acknowledges and understands that Contractor may be subject to civil and criminal penalties in accordance with Section 2-d for violations of Section 2-d and/or this Agreement.
- understand that any breach of the privacy or confidentiality obligations set forth in this Addendum may, at the sole discretion of OU BOCES, result in OU BOCES immediately terminating this Agreement; and
- Familiarize its applicable officers, employees and agents with this Addendum and with the "Parents' Bill of Rights for Data Privacy and Security."

The Contractor acknowledges that failure to fulfill these obligations shall be a breach of the Agreement. Except as specifically amended herein, all of the terms contained in the Original Agreement are hereby ratified and confirmed in all respects, and shall continue to apply with full force and effect.

IN WITNESS WHEREOF, Contractor and OU BOCES execute this Addendum to the Agreement as follows:

Contractor Name:
By: Melissa Pearson
Title: General Counsel
Signature: Melissa Pearson
Melissa Pearson (Jan 23, 2025 09:18 CST)
Date: 1/23/25

OU BOCES
By: Mark Coleman
Title: Assistant Superintendent
Signature:
Date: 1/27/25

Exhibit A

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

In accordance with the requirements of Section 2-d of the New York Education Law, Orange-Ulster BOCES (the "OU BOCES") provides the following Parents' Bill of Rights with respect to maintaining the privacy and security of student data:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes;

2. Parents have the right to inspect and review the complete contents of their child's education record;

3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred. Towards this end, OU BOCES has implemented the following safeguards to protect personally identifiable information about students, which is stored or transferred by OU BOCES, against unauthorized disclosure.

    - All databases that have student information are protected by a secure password and login. Logins are monitored, and passwords are kept up-to-date.

    - All databases that have student information are protected by a secure firewall, and intrusion detection. All data bases that contain student information are encrypted with 256 bit secure socket layer protection.

4. Parents may access a complete list of all student data elements collected by NYSED at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, or may obtain a copy of this list by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.

5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to: Director of Technology, 4 Harriman Drive, Goshen, NY 10924 (845)781-4358; support@ouboces.org.

PLEASE NOTE: Accordingly, this Parents' Bill of Rights is subject to revision and/or supplementation as needed to comply with OU BOCES' obligations under the law.

Additional information is available on the New York State Education Department's website at: https://www.nysed.gov/sites/default/files/programs/data-privacy-security/parents-bill-of-rights_2.pdf

Exhibit B

Supplemental Information

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, OU BOCES is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	Raptor Technologies, Inc
Description of the purpose(s) for which Contractor will receive/access PII	Contractor may receive access to PII through the purchase and usage of any of the products and/or services that are offered by Raptor Technologies including but not limited to VisitorSafe, StudentSafe, VolunteerSafe, DismissalSafe, SchoolPass
Type of PII that Contractor will receive/access	Check all that apply: ▣ Student PII □ APPR Data
Contract Term	Contract Start Date 1/15/2025 Contract End Date Ongoing
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) ▣ Contractor will not utilize subcontractors. □ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: ● Securely transfer data to OU BOCES, or a successor contractor at OU BOCES' option and written discretion, in a format agreed to by the parties. ● Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting OU BOCES. If a correction to data is deemed necessary, OU BOCES will notify Contractor. Contractor

	agrees to facilitate such corrections within 21 days of receiving OU BOCES' written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) □ Using a cloud or infrastructure owned and hosted by a third party. □ Using Contractor owned and hosted solution □ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: See provider's attached Data Security and Privacy Plan
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
[Signature]	Melissa Pearson Melissa Pearson (Jan 23, 2025 09:18 CST)
[Printed Name]	Melissa Pearson
[Title]	General Counsel
Date:	1/23/2025

RAPTOR
TECHNOLOGIES

RAPTOR DATA SECURITY & PRIVACY
CURRENT AS OF JANUARY 2024

SECTION 1: DATA STORED BY PRODUCT

Visitor Management

How it works

Modern, configurable technology screens each visitor's information against registered sex offender registries and custom databases, alerting schools if they are a potential threat and automatically creating robust visitor records. Raptor syncs with Student Information Systems (SIS) to pull student, staff, and guardian data, helping ensure school staff is well-positioned to release students to the appropriate guardians, as well as track student tardiness and early dismissals.

The Raptor system scans a driver's license (including digital) or federal, state, or local government-issued ID, including District-issued cards, for every individual entering each school. Raptor scans the 1D and/or 2D barcode on the back of government-issued IDs, and the scanner simultaneously captures the photo on the front of the ID. If a visitor has no scannable form of ID, the Raptor system allows for the manual entry of information (first name, last name, and date of birth) for screening purposes.

A school district can create an unlimited number of custom database files that will be used to screen each visitor every time they sign into the system. These custom lists can be imported into the system and can include banned/restricted visitors, custody issues, court rulings or adjudications, individuals with restraining orders, and so on. In addition, the Raptor system supports a custom student alerts database, which is checked each time a student is signed into or out of the school.

This database further ensures that known concerns about students or parents/guardians get alerts to the appropriate staff. Raptor allows authorized administrators to manage and configure all systems throughout the district, as well as view reporting and system usage data.

Once a visitor is cleared by the Raptor system, a visitor badge that is unique to each school/site is printed with the visitor's photo, their name, visit destination and/or staff whom the person is visiting, and expiration date and time.

How data is collected and stored

The Raptor scanner collects the ID photo, name, date of birth, and the first 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 first 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.** Additional data can be imported into the Raptor system and stored similarly to visitor data, such as student and staff directory data including the name, student ID number, and grade level of the student. **No student record data is imported** (i.e., no test scores, no home address, etc.).

The data is used to ensure that the district/school maintains a log of all visitors and other entry data through the front office. When a district also uses Raptor Emergency Management software, staff can account for all visitors on campus during a drill or emergency.

Volunteer Management

How it works

Raptor Volunteer Management system is designed to support the full volunteer lifecycle and includes an integrated online volunteer application, full criminal background checks, volunteer hour tracking, event management, batch printing, and reporting.

The volunteer process begins with an online, customizable volunteer application accessed by a link on the school's website. The system screens the applicant against a database with registered sex offenders in all 50 states and U.S. territories, as well as the criminal background screen through JD Palatine (JDP).

The Volunteer Management system is integrated with a district Volunteer Portal. The Volunteer Portal is an online web portal designed specifically for district volunteers and active community members to track volunteer hours, sign up for volunteer events, communicate with other volunteers, and communicate with district Volunteer Coordinators. Volunteers can view their volunteer history through various reports. Reports show the role/function(s) with total time volunteering, as well as the building, start date and time, end date and time, total time and log method displays. If you allow, volunteers can add, edit, and/or delete their hours for events.

How data is collected and stored

The volunteer process begins with an online, customizable volunteer application accessed by a link on your website. The prospective volunteer will complete the application, filling in their personal information, school preference, and volunteer role type of interest. If you request, the volunteer will also pay for their JDP background screening by providing their credit card information as part of their application.

You can request the applicant upload various documents as part of their application (driving record, immunization record, etc.), as well as request an electronic signature and include a customizable legal disclaimer. Once submitted, the applicant receives email confirmation.

Raptor stores all the data the applicant is asked to upload which varies based on the volunteer role and district policy. This information is retained even after the application is approved or denied, including any uploaded documents for customer records.

Emergency Management

How it works

A comprehensive solution, Raptor Emergency Management consists of a series of products, administered through a single software-as-a-service portal. Raptor Emergency Management runs on a standard configured personal computer with internet access. The Raptor system can be accessed through multiple internet browsers, including Google® Chrome® and Microsoft Edge. Our Raptor Emergency Management mobile application solution is compatible with iPhones and iPads running iOS 14, 15 and 16 and Android phones and tablets running Android versions 8 through 12.

The mobile app has biometric login by using a device's native Touch ID or Face ID for quick access, allowing personnel to respond to and resolve incidents swiftly. Raptor supports all industry-standard device biometric types for both Apple and Android operating systems, on both smartphones and tablets.

Drill Management automates scheduling, conducting, and reporting on drills. Required drill types and frequencies are configured in the system. Building administrators schedule drills and can initiate them from the app or desktop program. Information about each drill is recorded and available for analysis to improve emergency response procedures and generate compliance reports at school and district levels.

Raptor Alert is a panic alert that can handle both large and everyday emergencies, connect to 911 and chat with the staff. The web and mobile app connect with hard-wired, wireless and cellular networks. Designed to work under duress, Raptor Alert is a silent panic alert system that expedites and streamlines emergency response by allowing users to initiate an alert directly through 911 and provide critical information to first responders, law enforcement, and campus personnel.

Situation-specific notifications are sent via text, phone, email, desktop notifications, and push notifications. Push notifications show and play audio even if the phone is in silent/do not disturb mode to help inform your staff an incident is taking place.

Raptor Alert is compatible with all standard Public Safety Answering Points (PSAP) and emergency calling infrastructure and is RapidSOS Ready™ which accelerates the transfer of critical emergency alert data to 911 and first responders. Raptor automatically shares caller information with 911 dispatchers, including caller name, callback number, precise location, school name and dispatchable address, and type of emergency. This level of context is critical for 911 dispatchers to deliver the appropriate depth and breadth of first responders.

Geofences may be created during the implementation process by a Raptor Implementations Engineer with school administration guidance. Maintenance to the geofence can be facilitated any time there is a change necessary, simply by contacting Raptor Support for assistance.

The Raptor Connect integration platform, enables native, bi-directional integration with a school's existing digital security systems and peripherals. This means you can activate an emergency response from a single point instead of activating separate systems. For example, initiating a response protocol such as a lockdown within Raptor Alert can automatically activate a school's existing mass notification devices such as sirens, flashing lights, digital signage, etc. Similarly, a school's gun detection software can automatically activate Raptor Alert to initiate the designated response protocol. Raptor Connect streamlines a school's digital emergency response activations, speeding notifications and minimizing the impact of the situation.

Accountability connects with your student information system (SIS), Active Directory and Raptor Visitor Management (with subscription) to enable teachers and staff to account for themselves, students, and visitors directly in the Raptor mobile app while providing real-time status and location information. Raptor Accountability updates in real-time as status and location data change, making it easy for incident commanders and first responders to know exactly where someone is located and whether they are safe or in need of medical assistance. Reports include a detailed history of events for after-incident review.

Reunification is a patented workflow designed to increase the speed, accuracy and safety of reunification events. Connected to your student information system (SIS), Raptor helps ensure students are only reunified with approved guardians. Raptor helps reuinifiers confirm the guardian's identity, check for sex offender status and custodial restrictions, and record their signature at reunification. Raptor is 100% aligned with the Standard Reunification Method from The "I Love U Guys" Foundation and allows for the creation of designated roles and responsibilities for the reunification process. Raptor reunification dashboards update in real-time during emergencies and automatically create summary reports with a detailed history of the entire response for better after-incident debriefs.

How data is collected and stored

To successfully integrate with Student Information Systems (SIS), Raptor uses Clever, ClassLink, or file import. The data accessed and stored include the student's name, student ID number, and grade level. **No student record data is imported** (i.e., no test scores, no home address, etc.). Active Directory data includes staff names and class rosters.

The data is used to support the transfer of critical information to 911, accounting for the location and status during a drill or emergency and reunifying students and approved guardians.

Information from Raptor Emergency Management stored in the system includes detailed activity logs, drill schedules, drill activities, drill notes, student and staff accountability logs and reunification activity logs. This information is used for compliance reporting and after-incident review. Additionally, schools can upload emergency operations documents so that they are available during an incident.

RAPTOR
TECHNOLOGIES

StudentSafe

How it works

Raptor's patented StudentSafe technology brings together the systems that help schools recognize, document, support and manage the wellbeing of individual students. The intuitive and robust platform includes safeguarding and behavioral threat assessment (BTA) methodologies which are proven to help schools recognize a student in need of early intervention and support for their wellbeing.

Any school staff member or administrator can log in to StudentSafe and enter a low-level concern by providing some basic information. Schools establish categories of concerns such as mental wellbeing, home/family, relationships, etc. at the district level. When a staff member logs in, they select the student and category and write a few notes. Districts can set alerts to notify counselors or other designated staff when a specific category is used (e.g., bullying). Additionally, the StudentSafe dashboard will provide a quick view for designated staff to easily identify students that may need early help and support.

Student information is available through integration with the district's student information system (SIS).

Most staff members will only be able to enter data, not view data. StudentSafe includes four-dimensional provisioning enabling your district to configure permissions in a highly detailed and precise manner.

Raptor StudentSafe software includes the ability to document and manage low-level concerns, create student chronologies, run BTA workflows, manage BTA cases, gain immediate insight through alerts and robust dashboards, determine trends and gaps with full-scale reporting and more.

StudentSafe helps reduce your liability when it comes to meeting compliance and reporting requirements and demonstrating that proven processes are followed with fidelity. The secure, cloud-based platform includes proven methodologies and thorough case management features for full documentation of findings, actions, and follow-through.

How data is collected and stored

To successfully integrate with the Student Information Systems (SIS), Raptor uses Clever, ClassLink, or file import. The data accessed and stored include the student's name, student ID number, and grade level. **No student record data is imported** (i.e., no test scores, no home address, etc.).

The data is used to associate low-level concerns and when applicable, behavioral threat assessments with the appropriate students. Information from StudentSafe stored in the system includes low-level concerns identified by staff, associated tasks, workflows, interventions, interviews, uploaded content such as documents, images or screenshots, and other materials and data related to supporting student wellbeing.

SECTION 2: DATA HANDLING POLICIES & PRACTICES

Data Privacy and Security

Raptor Technologies designs its processes and procedures related to its Software as a Service solution to meet the requirements of K12 schools, including privacy and security requirements. These requirements are based on the service commitments that Raptor Technologies makes to user entities, the laws and regulations that govern the provision of its services, and the financial, operational, and compliance requirements that Raptor Technologies has established for our services.

Raptor's commitment to protecting the security and privacy of customer information includes, but is not limited to, the following:

- Following a standardized risk management process led by the Security and Compliance Program Manager and overseen by top-level management,
- Conducting annual assessments of service providers to collect, track, and manage third-party security controls based on the risk presented to the business,
- Ensuring data are encrypted at rest and in transit,
- Conducting regular vulnerability scanning and web application penetration testing of our products,
- Maintaining and periodically testing business continuity and disaster recovery plans.

Raptor uses service organizations (e.g., Windows Azure) to perform Platform as a Service, including data center hosting and capacity management, automated source code monitoring, and system performance monitoring service. Raptor designs its processes and procedures to meet the business objectives and the security and privacy requirements of K12 schools. A Defense in Depth control strategy is implemented throughout the Raptor platform which encompasses multiple layers of perimeter defense around the core application and database servers including network and application firewalls, load balancers, logical access restrictions, and threat monitoring and logging utilities.

Microsoft Azure, which hosts Raptor's platform, is a cloud-based computing platform operated by Microsoft for application management. Raptor uses Azure for its operating systems, cache services, storage, processing, and a variety of system monitoring. Therefore, Azure's compliance with security regulations and standards is relevant to how we deliver services to our customers. Azure undergoes rigorous auditing and is compliant with the highest industry standards for security and privacy. For a more extensive overview of Azure compliance documentation, see here.

Raptor completed SOC 2 Type 2 for both Privacy and Security. SOC 2 is a security framework that specifies how organizations should protect customer data from unauthorized access, security incidents, and other vulnerabilities.

Raptor does not modify, correct or delete the data of students, school staff, employees, visitors, volunteers or other individuals ("individuals") that are processed for customers (typically school districts) without direction from customers to do so. Accordingly, individuals are to direct such requests to the customer with whom they interact directly. Raptor will work with the customer to address any questions or requests that the customer raises.

Raptor often does not interact directly with individuals or does so only at the customer's direction as a processor. Raptor's customers may provide individuals with notice and updates to this Policy and, where appropriate, provide individuals with access (including the ability to confirm whether the customer holds any individual's PII and access, correct, or request deletion of PII) as well choices in connection with Raptor's services. Raptor notifies customers via the service in the event of significant changes to this Policy. If individuals have questions about the use of the services, they are to contact the customer who has provided access—this may be a school, employer, government entity, corporation or someone else. Raptor will work with the customer to address any questions or requests brought to our attention within a reasonable timeframe, but Raptor might not interact directly with individuals.

Upon request from our customers, Raptor will provide individuals with information about whether we hold any of your PII if we control such information. Customers may access, correct, or request deletion of individuals' PII by emailing support@raptortech.com.

Additional data privacy information regarding Raptor's services can be found at https://apps.raptortech.com/About/Privacy

Data Access

Raptor maintains and enforces safety and physical security procedures with respect to its access and maintenance of all personal information that (a) is at least equal to industry standards for such types of personal information and (b) provides reasonably appropriate technical and organizational safeguards against accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access of personal information.

Raptor Employees

Raptor employees are 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. This protects not only Raptor's intellectual property but any data that is collected and stored about individuals in Raptor software.

- All Employees complete security and privacy awareness training upon hire and at least annually thereafter. The Security Awareness program includes online security training modules and quarterly phishing campaigns.
- Access to the production environment is limited to and only authorized to employees with a need for access.
- Access to make changes to source code is limited to only appropriate individuals based on job function and active employment with the Company.

School Staff

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 and can be customized to fit specific needs.

User Roles and Permissions

Raptor Employees

Raptor employees are granted access to data based on job requirements and associated permissions. Access and permissions are controlled by unique usernames and passwords.

School Staff

Raptor's system organizes permissions out of the box to typical roles within the school or district (teachers, administrators, supporting staff, etc.). User permissions are fully configurable, enabling school or district administrators to assign appropriate system access. This ensures that employees have different access to the data based on their job requirements and associated permissions. Further, Raptor supports Single Sign On with the district's Identity Provider, typically Active Directory, enabling automated user provisioning, role assignment, and authentication.

OUB_DPA_Raptor_Updated 1.23.25

Final Audit Report 2025-01-23

Created:	2025-01-23
By:	Mikayla Pineda (mikayla.pineda@raptortech.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAwHLsxtUU1IC0-4nx_Xy2MTDsGjdh7nwa

"OUB_DPA_Raptor_Updated 1.23.25" History

Document created by Mikayla Pineda (mikayla.pineda@raptortech.com)
2025-01-23 - 2:33:57 PM GMT

Document emailed to Melissa Pearson (melissa.pearson@raptortech.com) for signature
2025-01-23 - 2:35:06 PM GMT

Email viewed by Melissa Pearson (melissa.pearson@raptortech.com)
2025-01-23 - 3:17:31 PM GMT

Document e-signed by Melissa Pearson (melissa.pearson@raptortech.com)
Signature Date: 2025-01-23 - 3:18:29 PM GMT - Time Source: server

Agreement completed.
2025-01-23 - 3:18:29 PM GMT

Adobe Acrobat Sign