wnyric
www.wnyric.org
Erie 1 BOCES Education Campus • 355 Harlem Road • West Seneca, NY 14224-1892
erie boces

EXHIBIT D

DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND
SUPPLEMENTAL INFORMATION ABOUT THE MLSA

1. **Purpose**

(a) This Exhibit supplements the Master License and Service Agreement ("MLSA") to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES' Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Erie 1 BOCES' website.

(b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. **Definitions**

Any capitalized term used within this Exhibit that is also found in the MLSA will have the same definition as contained within the MLSA.

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

(d) "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with a BOCES, and as a result is licensed to use Vendor's Product pursuant to the terms of the MLSA. For purposes of this Exhibit, the term also includes Erie 1 BOCES or another

BOCES that is licensed to use Vendor's Product pursuant to the MLSA to support its own educational programs or operations.

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and Erie 1 BOCES's policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy.. Erie 1 BOCES will provide Vendor with a copy of its policy. Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Erie 1 BOCES' Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

(a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.

(b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA:

Rocket Drones

Data Security and Protection Policy

1. Purpose

The company must restrict access to confidential and sensitive data to protect it from being lost or compromised in order to avoid adversely impacting our customers, incurring penalties for non-compliance and suffering damage to our reputation. At the same time, we must ensure users can access data as required for them to work effectively.

It is not anticipated that this policy can eliminate all malicious data theft. Rather, its primary objective is to increase user awareness and avoid accidental loss scenarios, so it outlines the requirements for data breach prevention.

2. Scope

2.1 In Scope

This data security policy applies all customer data, personal data and other company data defined as sensitive by the company's data classification policy. Therefore, it applies to every server, database and IT system that handles such data, including any device that is regularly used for email, web access or other work-related tasks. Every user who interacts with company IT services is also subject to this policy.

2.2 Out of Scope

Information that is classified as Public is not subject to this policy. Other data can be excluded from the policy by company management based on specific business needs, such as that protecting the data is too costly or too complex.

3. Policy

3.1 Principles

The company shall provide all employees and contracted third parties with access to the information they need to carry out their responsibilities as effectively and efficiently as possible.

3.2 General

a. Each user shall be identified by a unique user ID so that individuals can be held accountable for their actions.

b. The use of shared identities is permitted only where they are suitable, such as training accounts or service accounts.

c. Each user shall read this data security policy and the login and logoff guidelines, and sign a statement that they understand the conditions of access.

d. Records of user access may be used to provide evidence for security incident investigations.

e. Access shall be granted based on the principle of least privilege, which means that each program and user will be granted the fewest privileges necessary to complete their tasks.

3.3 Access Control Authorization

Access to company IT resources and services will be given through the provision of a unique user account and complex password. Accounts are provided by the IT department based on school records.

Passwords are managed by the IT Service Desk as well as a user who is assigned a role in the Rocket Drones portal giving them access to manage their student and racers access. Requirements for password length, complexity and expiration are stated in the company password policy.

Role-based access control (RBAC) will be used to secure access to all file-based resources in Active Directory domains.

3.4 Application and Information Access

a. All company staff and contractors shall be granted access to the data and applications required for their job roles.

b. All company staff and contractors shall access sensitive data and systems only if there is a business need to do so and they have approval from higher management.

c. Sensitive systems shall be physically or logically isolated in order to restrict access to authorized personnel only.

3.5 Access to Confidential or Restricted information

a. Access to data classified as ‘Confidential’ or ‘Restricted’ shall be limited to authorized persons whose job responsibilities require it, as determined by the Data Security Policy or higher management.

b. The responsibility to implement access restrictions lies with the IT Security department.

4. Technical Guidelines

Access control methods to be used shall include:

- Auditing of attempts to log on to any device on the company network
- Azure Active Directory permissions to files and folders
- Role-based access model
- Azure Active Directory access rights
- Firewall permissions
- Web authentication rights
- Database access rights and ACLs
- Encryption at rest and in flight
- Network segregation

Access control applies to all networks, servers, workstations, laptops, mobile devices, web applications and websites, cloud storages, and services.

5. Reporting Requirements

a. Daily incident reports shall be produced and handled by the Rocket Drones IT Security department or the incident response team.

b. Weekly reports detailing all incidents shall be produced by the Rocket Drones IT Security department and sent to the IT manager or director.

c. High-priority incidents discovered by the Rocket Drones IT Security department shall be immediately escalated; the IT manager should be contacted as soon as possible.

d. The Rocket Drones IT Security department shall also product a monthly report showing the number of IT security incidents and the percentage that were resolved.

6. Ownership and Responsibilities

- **Data owners** are employees who have primary responsibility for maintaining information that they own, such as an executive, department manager or team leader.

- **Information Security Administrator** is an employee designated by the IT management who provides administrative support for the implementation, oversight and coordination of security procedures and sys- tems with respect to specific information resources.

- **Users** include everyone who has access to information resources, such as employees, trustees, contractors, consultants, temporary employees and volunteers.

- **The Incident Response Team** shall be chaired by an executive and include employees from departments such as IT Infrastructure, IT Application Security, Legal, Financial Services and Human Resources.

7. Enforcement

Any user found in violation of this policy is subject to disciplinary action, up to and including termination of employment. Any third-party partner or contractor found in violation may have their network connection terminated.

8. Definitions

- ***Access control list (ACL)*** *— A list of access control entries (ACEs) or rules. Each ACE in an ACL identifies a trustee and specifies the access rights allowed, denied or audited for that trustee.*
- ***Database*** *— An organized collection of data, generally stored and accessed electronically from a computer system.*
- ***Encryption*** *— The process of encoding a message or other information so that only authorized parties can access it.*
- **Firewall** *— A technology used for isolating one network from another. Firewalls can be standalone systems or can be included in other devices, such as routers or servers.*
- ***Network segregation*** *— The separation of the network into logical or functional units called zones. For example, you might have a zone for sales, a zone for technical support and another zone for research, because each group has different technical needs.*
- ***Role-based access control (RBAC)*** *—A policy-neutral access-control mechanism defined around roles and privileges.*
- ***Server*** *— A computer program or a device that provides functionality for other programs or devices, called clients.*
- ***Virtual private network (VPN)*** *— A secure private network connection across a public network.*
- ***VLAN (virtual LAN)*** *— A logical grouping of devices in the same broadcast domain.*

9. Related Documents

This section lists all documents related to the policy and provides links to them. This list might include:

- Data Classification Policy
- Password Policy
- Data Loss Protection Policy
- Encryption Policy
- Incident Response Policy
- Workstation Security Policy
- Data processing agreement

(c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" below.

(d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.

(e) Vendor ___X___will _____will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.

(g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. **<u>Additional Statutory and Regulatory Obligations</u>**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

(a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.

(c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:

   (i) the parent or eligible student has provided prior written consent; or
   (ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. <u>Notification of Breach and Unauthorized Release</u>

(a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).

(c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.

(e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

EXHIBIT D (CONTINUED)

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community of the following:

(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.

(4) A complete list of all student data elements collected by the State is available for public review at **http://www.nysed.gov/data-privacy-security/student-data-inventory**, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website **http://www.nysed.gov/data-privacy-security/report-improper-disclosure**.

BY THE VENDOR:

DocuSigned by:

Chris Tonn

E1D0D140E1F5448...

Signature

_Chris Tonn_________________________________

Printed Name

_COO_________________________________

Title

4/27/2023

Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND ROCKET DRONES, LLC

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with Rocket Drones, LLC which governs the availability to Participating Educational Agencies of the following Product(s):

Rocket Drones School Starter Kit
Rocket Drones Curriculum – Drone 101 (middle school) & Drone 102 (high school)

Pursuant to the MLSA, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: All subcontractors will be required to keep records of any alterations to existing code or database. Before implementing any changes to our system, subcontractor's work will be evaluated by Rocket Drones lead developer first. Subs will also be required to have professional liability insurance coverage.

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on March 15 ~~July 1~~, 2023 and expires on June 30, 2026.
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a

Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.