DocuSign Envelope ID: 8AEE851D-50B6-4627-A53A-04C13063DCE9

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 and 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.

DocuSign Envelope ID: 8AEE851D-50B6-4627-A53A-04C13063DCE9

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:

Bloomz Security Pledge

Bloomz was created to promote and facilitate communication between schools and families in a safe and private environment. Parental engagement, which is proven to help improve student performance, requires open communication channels and straightforward coordination and collaboration between educators, students and their families.
In order to provide this environment, Bloomz complies with regulations like FERPA and COPPA, and all applicable privacy laws. Bloomz is also a signatory of the Student Privacy Pledge, taking responsibility to both support the effective use of student information and safeguard student privacy and information security.
To meet these guidelines, Bloomz has created a platform that accounts for privacy and security at both the front end, where teachers, students and parents interact with our service, and the backend where all information is stored and organized. For example, users can receive messages via text message, mobile app, or email, but contact information like phone numbers and email addresses are only visible to class and school administrators and not exposed to others. We have also implemented strict advanced cloud computing practices and policies to ensure the integrity of the data we manage. We strive to bring best-in-class security and controls to users and educational organizations, and continually work with school and district administrators to build upon our existing infrastructure.
This document provides an overview of the policies and practices that comprise our security approach.
Overview
Bloomz's approach to security consists of the following components to maintain data security and integrity:
1. Internal policies
2. Identity security
3. Physical security
4. Server security
5. Database & Software security
6. Privacy principles
7. Regulatory compliance
Each of these components are described in more detail below.

DocuSign Envelope ID: 8AEE851D-50B6-4627-A53A-04C13063DCE9

1. Internal policies
Bloomz is constantly listening to and acting upon industry-leading security guidelines, regulation and recommendations to guide our own policies and procedures.
• Bloomz's policies and practices are intended to safeguard sensitive information, providing assurance to educational organizations who entrust us.
• Bloomz is developing privacy and security training that all employees will take at the time of hire and annually thereafter.
• All Bloomz employees and contractors sign agreements that require them to preserve and protect the confidentiality of sensitive information they may access while working with us.
• Information security controls are in constant evolution to ensure they are current, relevant and in compliance.

2. Identity security
Bloomz's technology is thought of with security in mind to prevent inadvertent access of user information.
• Sensitive information is protected at rest and in transit across untrusted networks using encryption.
• Clear text passwords are not stored in the DB. Passwords should be at least 8 characters long and must have one alphabet and one number.
• Salted passwords with one-way encryption are recorded.
• Passwords are only sent via HTTPS only.
• Request old password while updating to new password.
• Request password to change the identity of the user.
• Authentication tokens are valid for one week for authenticated users.
• All Cookies are HTTPS and domain associated so that other services cannot read the cookies.
3. Physical security
While the Bloomz team works remotely, strong measures are taken to protect systems that access, store, transmit or process user information.
• Logging into a sensitive system is controlled by strong password requirements and access is assigned by role under need-to-know basis.
• All devices used by Bloomz personnel are required to include antivirus software and strong authentication requirements.
• Bloomz is hosted in AWS and Microsoft Azure data center facilities with rigorous physical security controls including a non-descript location, security staff, layered electronic access controls from all building ingress points to interior zones, intrusion detection, and surveillance monitoring.

4. Server security
Bloomz uses Amazon Web Services (AWS) and Microsoft Azure to host and operate our service.
• AWS's environmental protections reduce the risks associated with fire, loss of power, flood, humidity, and temperature changes in their facilities.
• Data center facilities are strategically located in regions that are less commonly affected by natural disasters.
• Cloud-based information storage is protected from environmental threats using fault tolerance and redundancy.
• The AWS cloud infrastructure has been designed and managed in compliance with regulations, standards, and best practices, including HIPAA, SOC 1/SSAE 16/ISAE 3402 (formerly SAS70), SOC 2, SOC 3, PCI DSS Level 1, ISO 27001, FedRAMP, DIACAP and FISMA, ITAR, FIPS 140-2, CSA, and MPAA.
• All the APIs to the server are on HTTPS. The API servers do not accept any requests on HTTP.
• Only ports 443 (HTTPS), and 22 (SSH) are opened on the API servers.
• SSH port can only be logged in via provided certificate.
• WW web server runs on Apache and redirects all HTTP requests to HTTPS endpoint.

5. Database and Software security
Bloomz is delivered using industry tested technology with privacy, end user safety, and security in mind.
• All databases run on top of Linux Ubuntu 64-bit servers.
• MongoDB, a NoSQL DB is used as the backend database.
• The databases are run on a network mask that is opens connections only from specific API servers
• Machines that run the primary and slave databases accept DB connections only through restricted Virtual Network (VNet).
• Only ports 22 (SSH) and DB ports are opened on the API servers.
• SSH port can only be logged in via provided certificate.
• Hard backups are stored on MongoDB MMS service.
• Bloomz works with researchers of varied disciplines and expertise under a bounty program to perform security assessments of our applications.
• Vulnerabilities discovered in our applications are prioritized and remediated to improve the overall security of our platform.
• Bloomz follows an industry standard secure development process that aims to avoid common security exposures.

DocuSign Envelope ID: 8AEE851D-50B6-4627-A53A-04C13063DCE9

6. Privacy Principles
Bloomz has adopted modern practices with respect to handling personal information.
• Groups/Classes/Communities with controlled level of access for effective coordination,
• calendar and knowledge sharing
• Classroom membership is only via invitation – teachers can invite explicitly, even with class codes, additional security for verifying members is added.
• Classrooms are visible only for members of a school community
• None of the child information is pushed to the services that Bloomz uses for user
• analytics purposes.
• Bloomz maintains a Privacy Notice in a clear and visible location on our website to inform consumers about how personal information is used, collected, and shared.
• The processing of personal information is limited to the purposes identified by our terms of use and never repurposed.
• Bloomz will never sell, trade, barter, or exchange for value consumers' personally identifiable information or personal data.
• In the case of a security incident resulting in a data breach or the unauthorized disclosure of personal information, as defined by a state, federal or other regulation, Bloomz will promptly notify impacted parties and authorities.

7. Regulatory compliance
Bloomz works with legal counsel to ensure that our products and practices remain compliant with relevant mandates and regulations.
• Bloomz meets COPPA legislative requirements.
• Bloomz helps schools comply with federal FERPA regulations.

DocuSign Envelope ID: 8AEE851D-50B6-4627-A53A-04C13063DCE9

Bloomz Subscription (Product) Options

	Teacher Free	Teacher Premium ($125 per year)	Schoolwide Essentials	Schoolwide Premium
Auto Notices & Robocalling	No	No	Add-On Optional	Yes
Posts & Announcements	Yes	Yes	Yes	Yes
SMS Messaging	Can invite parents via phone numbers, but no ongoing SMS	Yes	Yes	Yes
Calendar & Event Scheduling	Limited Agenda View	Yes	Yes	Yes
Parent-teacher conferences	Yes	Yes	Yes	Yes
Volunteer signups	Yes	Yes	Yes	Yes
Student portfolios	Yes	Yes	Add-On Optional	Yes
Behavior management	Limited	Yes	Add-On Optional	Yes
PBIS/SEL Interactions Access	2 Interactions per day per student OR Daily Limit of 80 Interactions per day No support for Flags (escalations) or locations	Unlimited Interactions per day No support for Flags (escalations) or locations	Add-On Optional	Unlimited
Health Checks	No	No	Yes	Yes

DocuSign Envelope ID: 8AEE851D-50B6-4627-A53A-04C13063DCE9

Bulk media downloads	No	Yes	Yes	Yes
Attendance Reports	No	Yes	Yes	Yes
Premium features for parents included	No	Yes	Yes	Yes
Cloud storage*	125 media items (including photos & videos) - 1 GB	2 GB	Unlimited	Unlimited
Calendar monthly and weekly views	No	Yes	Yes	Yes
Photo captions	No	Yes	Yes	Yes
Premium Calendar View	No	Yes	Yes	Yes
Classroom Reports	No	Yes	Yes	Yes
Data/Engagement dashboard	No	No	Yes	Yes
Print event history	No	Yes	Yes	Yes
Media Sharing	No	Yes	Yes	Yes
Class Archival	No	Yes	Yes	Yes
Classes allowed per Teacher	1	3	Unlimited	Unlimited
Co-Teachers per class	1 Co-Teacher	1 Co-Teacher	Unlimited	Unlimited
Room Parents per class	1	2	Unlimited	Unlimited
Class Admins per class	None	1	Unlimited	Unlimited

DocuSign Envelope ID: 8AEE851D-50B6-4627-A53A-04C13063DCE9

Students per class	30	50	Unlimited	Unlimited
Parents per class	60	100	Unlimited	Unlimited
Translation	Posts & Announcements only	Posts, Announcements, Alerts, and Messages	Posts, Announcements, Alerts, and Messages	Posts, Announcements, Alerts, and Messages

(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 [*check one*] _____will __**X**_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. **Additional Statutory and Regulatory Obligations**

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. **Notification of Breach and Unauthorized Release**

(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

(d) 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.

(e) 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.

(f) 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)

DocuSign Envelope ID: 8AEE851D-50B6-4627-A53A-04C13063DCE9

ERIE 1 BOCES

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:

Signature

Chakrapani Appalabattula

Printed Name

CEO and Founder

Title

June 30th, 2023

Date

DocuSign Envelope ID: 8AEE851D-50B6-4627-A53A-04C13063DCE9

Supplemental Information

about the Master License and Service Agreement
between
Erie 1 BOCES and [**Bloomz**]

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

Bloomz Communication App

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: [***NA***]

Duration of MLSA and Protected Data Upon Expiration:

The MLSA commences on [**5-31-2023**] and expires on [**6-30-26**].
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.