

Compliance With New York State Education Law Section 2-d Agreement ("Agreement")

The parties to this Agreement are the Monroe 1 Board of Cooperative Educational Services ("BOCES") and Gaggle.Net, Inc. ("Vendor"). BOCES is an educational agency, as that term is used in Section 2-d of the New York State Education Law ("Section 2-d") and its implementing regulations, and Vendor is a third party contractor, as that term is used in Section 2-d and its implementing regulations. BOCES and Vendor have entered into this Agreement to conform to the requirements of Section 2-d and its implementing regulations. To the extent that any term of any other agreement or document conflicts with the terms of this Agreement, the terms of this Agreement shall apply and be given effect.

Definitions

As used in this Agreement and related documents, the following terms shall have the following meanings:

"Student Data" means personally identifiable information from student records that Vendor receives from an educational agency (including BOCES or a Participating School District) in connection with providing Services under this Agreement.

"Personally Identifiable Information" ("PII") as applied to Student Data, means personally identifiable information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA), at 20 USC 1232g.

"Third Party Contractor," "Contractor" or "Vendor" means any person or entity, other than an educational agency, that receives Student Data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including, but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs.

"BOCES" means Monroe #1 Board of Cooperative Educational Services.

"Parent" means a parent, legal guardian, or person in parental relation to a student.

"Student" means any person attending or seeking to enroll in an educational agency.

"Eligible Student" means a student eighteen years or older.

"State-protected Data" means Student Data, as applicable to Vendor's product/service.

"Participating School District" means a public school district or board of cooperative educational services that obtains access to Vendor's product/service through a cooperative educational services agreement ("CoSer") with BOCES, or other entity that obtains access to Vendor's product/service through an agreement with BOCES, and also includes BOCES when it uses the Vendor's product/service to support its own educational programs or operations.

"Breach" means the unauthorized access, use, or disclosure of personally identifiable information.

"Commercial or marketing purpose" means the sale of PII; and the direct or indirect use or disclosure of State-protected Data to derive a profit, advertise, or develop, improve, or market products or services to students other than as may be expressly authorized by the parties in writing (the "Services").

"Disclose", "Disclosure," and "Release" mean to intentionally or unintentionally permit access to State-protected Data; and to intentionally or unintentionally release, transfer, or otherwise communicate State-protected Data to someone not authorized by contract, consent, or law to receive that State-protected Data.

Vendor Obligations and Agreements

Vendor agrees that it shall comply with the following obligations with respect to any student data received in connection with providing Services under this Agreement and any failure to fulfill one of these statutory or regulatory obligations shall be a breach of this Agreement. Vendor shall:

(a) limit internal access to education records only to those employees and subcontractors that are determined to have legitimate educational interests in accessing the data within the meaning of Section 2-d, its implementing regulations and FERPA (e.g., the individual needs access in order to fulfill his/her responsibilities in providing the contracted services);

(b) only use personally identifiable information for the explicit purpose authorized by the Agreement, and must/will not use it for any purpose other than that explicitly authorized in the Agreement or by the parties in writing;

(c) not disclose any personally identifiable information received from BOCES or a Participating School District to any other party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Agreement, unless (i) if student PII, the Vendor or that other party has obtained the prior written consent of the parent or eligible student, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to the source of the information no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

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

(e) use encryption technology to protect data while in motion or in its custody (i.e., in rest) from unauthorized disclosure by rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5 using a technology or methodology specified or permitted by the secretary of the U.S.;

(f) not sell personally identifiable information received from BOCES or a Participating School District nor use or disclose it for any marketing or commercial purpose unless otherwise expressly authorized by the Services, or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so;

(g) notify the educational agency from which student data is received of any breach of security resulting in an unauthorized release of such data by Vendor or its assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay, in compliance with New York law and regulation;

(h) reasonably cooperate with educational agencies and law enforcement to protect the integrity of investigations into any breach or unauthorized release of personally identifiable information by Vendor;

(i) adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework, Version 1.1, that are in substantial compliance with the BOCES data security and privacy policy, and that comply with Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education and the Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security, set forth below, as well as all applicable federal, state and local laws, rules and regulations;

(j) acknowledge and hereby agrees that the State-protected Data which Vendor receives or has access to pursuant to this Agreement may originate from several Participating School Districts located across New York State. Vendor acknowledges that the State-protected Data belongs to and is owned by the Participating School District or student from which it originates;

(k) acknowledge and hereby agrees that if Vendor has an online terms of service and/or Privacy Policy that may be applicable to its customers or users of its product/service, to the extent that any term of such online terms of service or Privacy Policy conflicts with applicable law or regulation, the terms of the applicable law or regulation shall apply;

(l) acknowledge and hereby agrees that Vendor shall promptly pay for or reimburse the educational agency for the full third party cost of a legally required breach notification to parents and eligible students due to the unauthorized release of student data caused by Vendor or its agent or assignee;

(m) ensure that employees, assignees and agents of Contractor who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access to such data; and

(n) ensure that any subcontractor that performs Contractor's obligations pursuant to the Agreement is legally bound by legally compliant data protection obligations imposed on the Contractor by law, the Agreement and this Agreement.

Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security

(<https://www.monroe.edu/domain/1478>)

The Monroe #1 BOCES seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the BOCES, to enhance the opportunities for learning and to increase the efficiency of our operations.

The Monroe #1 BOCES seeks to ensure that parents have information about how the BOCES stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law.

To further these goals, the BOCES has posted this Parents' Bill of Rights for Data Privacy and Security.

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. The procedures for exercising this right can be found in Student Records Policy 6320. (<https://www.monroe.edu/6320>)
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 at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx> and a copy may be obtained 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:

Chief Privacy Officer
New York State Education Department
Room 863 EBA
89 Washington Avenue
Albany, New York 12234.

or
Monroe One Data Protection Officer
William Gregory
Monroe #1 BOCES
41 O'Connor Road
Fairport, NY 14450

Supplemental Information About Agreement Between Vendor and BOCES

(a) The exclusive purposes for which the personally identifiable information provided by BOCES or a Participating School District will be used by Vendor is to provide examination services to BOCES or other Participating School District pursuant to a BOCES Purchase Order.

(b) Personally identifiable information received by Vendor, or by any assignee of Vendor, from BOCES or from a Participating School District shall not be sold or used for marketing purposes.

(c) Personally identifiable information received by Vendor, or by any assignee of Vendor shall not be shared with a sub-contractor except pursuant to a written contract that binds such a party to at least the same data protection and security requirements imposed on Vendor under this Agreement, as well as all applicable state and federal laws and regulations.

(d) The effective date of this Agreement shall be immediately and the Agreement shall remain in effect unless terminated by either party for any reason upon sixty (60) days' notice.

(e) Upon expiration or termination of the Agreement without a successor or renewal agreement in place, and upon request from BOCES or a Participating School District, Vendor shall transfer all educational agency data to the educational agency in a format agreed upon by the parties. Vendor shall thereafter securely delete all educational agency data remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies) as well as any and all educational agency data maintained on behalf of Vendor in secure data center facilities, other than any data that Vendor is required to maintain pursuant to law, regulation or audit requirements. Vendor shall ensure that no copy, summary or extract of the educational agency data or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the secure data center facilities unless Vendor is required to keep such data for legal, regulator, or audit purposes, in which case the data will be retained in compliance with the terms of this Agreement. To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers permanently removed with no possibility of reidentification), they each agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to the BOCES or Participating School District from an appropriate officer that the requirements of this paragraph have been satisfied in full.

(f) State and federal laws require educational agencies to establish processes for a parent or eligible student to challenge the accuracy of their student data. Third party contractors must cooperate with educational agencies in complying with the law. If a parent or eligible student submits a challenge to the accuracy of student data to the student's district of enrollment and the challenge is upheld, Vendor will cooperate with the educational agency to amend such data.

(g) Vendor shall store and maintain PII in electronic format on systems maintained by Vendor in a secure data center facility in the United States in accordance with its Privacy Policy, NIST Cybersecurity Framework, Version 1.1, and the BOCES data security and privacy policy, Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education, and the Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security, set forth above. Encryption technology will be utilized while data is in motion and at rest, as detailed above.

(h) A copy of Vendor's Data Privacy and Security Plan, which vendor affirms complies with 8 N.Y.C.R.R. 121.6 is attached hereto as Attachment 1 and is incorporated herein by reference as if fully set forth herein.

Monroe 1 BOCES


By:

Daniel T. White, District Superintendent

Date

Gaggle.Net, Inc.

By:



Jennie Eft, Director of Sales Operations

5/12/2023

Date

Gaggle Service Level Agreement

Last Updated: March 29, 2023

This Enterprise Service Level Agreement (SLA) for Gaggle.Net, Inc. ("Gaggle") Solutions ("Services") is made in connection with, and is a part of, your (Customer) Gaggle invoice, Customer contract, or Subscription Agreement for Services including, but not limited to: Archiving & Backup, Safety Management, SpeakUp for Safety, After Hours, Mental Health Services, and ReachOut. This SLA establishes the understanding for Gaggle to provide any of these Services to ensure maximum performance and uptime. Compensation for the Services provided under this SLA shall be at the rates and terms set forth in a Gaggle invoice, Customer contract, or Subscription Agreement.

1. Descriptions of Services

Archiving & Backup

Gaggle Archiving & Backup includes the archiving of all Customer email messages up to 50 megabytes (MB) in size, and all cloud-based (Drive) files up to 300 megabytes (MB) in size.

This Service includes full-text indexing, tiered administrator access permissions, granular litigation management, audit logs of access and activity, policy-based data retention, and advanced search, data recovery, and export options. Gaggle shall not be required to archive, and Customer shall not transmit, miscellaneous documents, which are not attachments to specific email communications for the sole purpose of archiving non-email-related documents.

A separate drive-based archiving solution can also be purchased, which provides archiving of cloud-based files subject to certain file size and file type limitations. This service is intended for individual user-based file archiving versus the archiving of data systems.

Upon request, for an additional charge, all email content and cloud-based files archived by Gaggle may be delivered to the Customer.

Safety Management and SpeakUp for Safety Tipline

Gaggle shall monitor email, message communications, documents, and other file types subject to certain file size limitations within third-party services including, but not limited to, those from Google Inc. and Microsoft Corporation.

Gaggle shall not make Safety Management or SpeakUp for Safety tipline available to Customer until Customer has provided Gaggle with the identity of three (3) designated emergency contacts including all emergency contact information. "Designated emergency contact" means the individual(s) designated by you to receive and act upon Gaggle notifications. If applicable, Customer must also provide access to student information system (SIS) data.

If there is a change in any designated emergency contact and/or emergency contact information, you must immediately notify Gaggle of all applicable changes. Your failure to immediately notify Gaggle of any changes to the designated emergency contact information will result in the delay or inability of Gaggle to properly send notifications to your organization.

Chrome Extension

Gaggle's Chrome Extension is a safety monitoring solution for web searches performed by students when using a Chrome Browser on your school-provided account or devices. The extension is a lightweight add-on that does not interfere with activity on your device. It logs all searches and sends them to Gaggle for review by artificial intelligence and our human safety team. Searches that indicate suicide ideation or self-harm and threats of violence will result in email notifications and immediate emergency phone calls when warranted.

After Hours

Gaggle Safety Team Members will alert designated local authorities, who can then determine the appropriate course of action to help ensure student well-being. Possible Student Situation (PSS) incidents occurring after hours, overnight, and on weekends will be handled by the Gaggle Safety Team. Gaggle will reach out to local authorities or social workers to perform a wellness check.

Gaggle will pull data from the district's Student Information System (SIS) so that we can provide the relevant information to authorities. Files with the student data will need to be uploaded daily via a file transfer (SFTP) for each group.

Mental Health Services

Gaggle shall provide outpatient individual and group therapy or coaching sessions to address a variety of experiences, symptoms, and disorders. These services are evidence-based and individualized to meet student or staff needs addressing symptoms related to mood disorders, substance use disorders, depression, anxiety, self-harm, PTSD, grief and loss, stress, trauma, etc.

School staff identify students for therapy or mental health coaching and Gaggle will reach out to those students' parents to coordinate the student intake process and obtain informed consent. Gaggle will then match the students with licensed counselors and send a secure HIPAA-compliant video login link for each session.

Students will participate in ongoing 45-minute video sessions for a duration determined by the provider. Therapy sessions will be scheduled at convenient times for students, including evenings and weekends. Students will be able to log on for therapy sessions from home or at school.

All Gaggle Mental Health Services and activities comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Family Educational Rights and Privacy Act (FERPA).

ReachOut

Gaggle will provide a 24/7 mental health crisis and support line designed for kids and teens. Students are partnered with trained crisis responders to address youth crisis situations and de-escalate to keep students safe. Students communicate in a 2-way conversation with a crisis responder via SMS text, web-based chat, or phone.

2. Service Standards

Gaggle shall regularly maintain and update, as needed, all Services. General maintenance typically shall not result in an interruption of Services (Downtime) except for Scheduled Downtime or Emergency Downtime, which is outside the control of Gaggle.

Gaggle guarantees that its Services shall be available 99.5% of the time in a given month, excluding Scheduled Downtime for maintenance and Emergency Downtime. Downtime exists when a particular Customer is unable to send or receive data from Gaggle servers, the failure is resolvable by Gaggle, and such failure has been clearly and fully communicated in writing to the Gaggle technical support team. Downtime shall be applicable until the server is able to send and receive data as confirmed by Gaggle's monitoring systems. Maintenance and updates to Services, which may require an interruption of Services, shall be scheduled by Gaggle through notice to Customer of the Scheduled Downtime. Gaggle shall undertake commercially reasonable efforts to arrange Scheduled Downtime for maintenance and updates to be performed during off-peak hours.

When third-party applications are used within Gaggle Services, Gaggle does not have control over these applications. Downtime of these applications is specifically excluded from this SLA.

3. Limitations

This SLA and any applicable Services do not apply to any of the following:

Issues that are due to factors outside of Gaggle's control including, but not limited to, natural acts of God, acts of any governmental body, war, insurrection, sabotage, armed conflict, embargo, fire, flood, strike or other labor disturbance, interruption of or delay in transportation, unavailability of or interruption or delay in telecommunications or third-party services, virus attacks or hackers, failure of third-party software, or inability to obtain raw materials, supplies, or power used in or equipment needed for the provision of this SLA.

Interruptions that result from Customer and/or a third-party hardware or software and that are not within the primary control of Gaggle.

Issues that result from outages between Gaggle's Internet Service Provider and Gaggle servers.

Interruptions relating to Domain Name Server ("DNS") issues outside the control of Gaggle including DNS propagation or any delays in the registration or transfer of domain names and browser or DNS caching that may make Customer Site appear inaccessible when others can still access Customer Site.

Scheduled Downtime including upgrades and Emergency Downtime, as described in Section 2.

Customer acts or omissions (or acts or omissions of others engaged or authorized by Customer) including, without limitation, custom scripting or coding and any unauthorized, unlawful email practices.

Issues due to any negligence, willful misconduct, or use of the Services in breach of this SLA, Terms & Conditions, and other related documents.

4. Duration

This SLA shall commence on the Service Start (Commencement) Date and ends on the earlier of the Service End (Expiration) Date or at the time of termination in accordance with Section 7.

5. Roles and Responsibilities

The Services under this SLA are provided to Customer pursuant to Tiered Administrator Access Permissions, which Customer will select and assign to its users based on the access and security needs of the Customer's organization. Users shall only be allowed to access and utilize the Services based on the designated Administrator Access Permission. Customer is responsible to communicate all usernames and passwords to its users. Customer shall control all Customer Tiered Administrator Access Permissions and any changes to those Permissions.

Use of accounts shall be limited to those individuals granted access by the Customer, who is solely responsible for the assignment of accounts and the enforcement of user access security. Gaggle shall use commercially reasonable efforts to advise Customer in identifying any known security breach, but Gaggle shall not be liable to Customer or any user for any inability, failure, or mistake in connection with such assistance. Customer is responsible, at its own cost and expense, to maintain all Customer (Client) Software and Hardware Configurations recommended by Gaggle, which may be updated from time to time. Customer shall report to Gaggle any changes to its Customer (Client) Software and Hardware Configurations.

Customer shall be responsible for monitoring and reporting any problems with its Customer (Client) Software and Hardware Configurations to Gaggle through written or digital format. All Gaggle Services shall only be used in a manner consistent with the appropriate uses associated with the operations and functions of Customer's organization and shall not be contrary to public policy, the law, and commercially acceptable online etiquette. Failure to comply with these limitations may result in Gaggle suspending or terminating the Services of the violating user or all Customer accounts without notice. Gaggle maintains a ticket system to manage all Customer issues. Gaggle provides customer service between the hours of 6:00 AM and 7:00 PM CT Monday through Friday.

Customers can reach our Customer Service team by email (support@gaggle.net), telephone (800-288-7750), or by accessing a live chat feature within the Gaggle interface and on the [Gaggle website](#). After-hours support is provided through a monitored email account at support@gaggle.net. Gaggle provides additional technical support twenty-four (24) hours per day, seven (7) days per week. Response time commitments are made based on the severity of the issue, ranging from six (6) hours for critical issues to twenty-four (24) hours for informational requests.

6. SLA Claim

If Customer believes Gaggle is in violation of this SLA, Customer should send an email to Gaggle at support@gaggle.net indicating the day(s) and time(s) in which the unavailability of Services occurred. Gaggle will review each claim and respond to the sender of the email within one (1) full business day.

7. Termination

Either party may terminate the Services under this SLA at any time by providing thirty-day (30) written notice of the intent to terminate. Gaggle may also terminate or suspend any and all Services immediately, without prior notice or liability, if Customer breaches any conditions set forth in this SLA or in the Terms & Conditions the Customer accepted by clicking the Accept button prior to accessing Gaggle Services. Gaggle can, at any time, modify or discontinue any of its Services without liability to any user or third party.

8. Notifications

Unless specified otherwise herein: (a) all notices must be in writing and addressed to the attention of the other party's legal department and primary point of contact; and (b) notice will be deemed given: (i) when verified by written receipt if sent by personal courier, overnight courier, or when received if sent by mail without verification of receipt; or (ii) when verified by automated receipt or electronic logs if sent by facsimile or email.

9. Assignment

Neither party may assign or transfer any part of this SLA without the written consent of the other party, but only if: (a) the assignee agrees in writing to be bound by the terms of this Agreement; and (b) the assigning party remains liable for obligations incurred under the Agreement prior to the assignment. Any other attempt to transfer or assign is void.

Gaggle Services Terms & Conditions

Last Updated: January 31, 2023

Please read the following Agreement carefully. This Agreement explains your rights and obligations as a user of "Services" provided by Gaggle.Net, Inc. ("Gaggle"). Gaggle Services include but are not limited to, Archiving & Backup, Safety Management, SpeakUp for Safety, Mental Health Services, and ReachOut. For a further Description of Services, please consult the Gaggle Service Level Agreement.

It may be necessary for us to update or revise parts of this Agreement or any feature of Gaggle Services without prior notice. If we make material changes to this Agreement, we will post the updated Agreement (with a notice that the Agreement has been updated) and notify Customers by email using the primary email address specified in their accounts.

1. Acceptance of Terms

The Terms & Conditions herein establish the understanding for Gaggle to provide Services to you ("Customer"). Compensation for the Services provided shall be at the rates and terms set forth in a Gaggle invoice, Customer contract, or Subscription Agreement. By completing the registration process and providing Gaggle with current, complete, and accurate information, you are agreeing to be bound by these Terms & Conditions. If you choose not to agree with the changes, your only remedy would be to cancel Gaggle Services in accordance with Section 8.

2. Unauthorized Access, Password Protected, and Secured Areas

Users of Gaggle Services shall be responsible for unauthorized access made through their usernames and passwords. For this reason, Gaggle recommends that users change their passwords periodically. Access to and use of current or future password-protected or secured Services is restricted to authorized users only. You will be asked to provide accurate and current information on all registration forms for Gaggle Services. You are solely responsible for maintaining the confidentiality of any username and password that you choose or is chosen by someone on your behalf. You agree not to misuse or share your username or password, misrepresent your identity or your affiliation with an entity, impersonate any person or entity, or misstate the origin of any materials that you are exposed to through Gaggle Services. If you violate your obligations under this section, you may be subject to criminal prosecution or civil damages. You agree to notify Gaggle and your applicable administrator immediately of any unauthorized use of your account or any other breach of security known to you.

3. Privacy and Security

Gaggle uses a variety of measures to protect the security and privacy of its users. Users should be aware, however, that Gaggle cannot guarantee security and confidentiality through its Services. Gaggle accepts no responsibility for harm caused directly or indirectly by the use of its Services. Users should also be aware that the use of Gaggle email and/or email through third-party products, such as those from Google Inc. and Microsoft Corporation, is not private. Although Gaggle is not obligated to do so, it has the right to review and monitor your content and communications, including but not limited to fulfilling obligations set forth in your contract or Subscription Agreement, to back up or review messages to identify network problems, or to

determine whether you comply with our Terms & Conditions. Gaggle, at its discretion, may choose to turn over or make available message content to appropriate personnel, the National Center for Missing and Exploited Children ("NCMEC"), and/or law enforcement agencies, if required.

For more information, please also refer to the [Gaggle Privacy Policy](#) and [Gaggle Student Data Privacy Notice](#).

4. Confidentiality Policy

As used herein, "Confidential Information" shall mean the respective parties' proprietary information or material to which the other party may become aware of as a result of this Agreement, including but not limited to research data, methodologies, products, services, processes, formulas, technology, or other business information disclosed to one party by the other, either directly or indirectly, whether in writing, orally, or otherwise, but not including any of the foregoing that was known to the receiving party at the time of disclosure from a source other than the disclosing party or any third party that owed a duty of confidentiality with respect to such information to the disclosing party or which has become publicly known and made generally available through no wrongful act or omission of the receiving party or of others who were under confidentiality obligations with respect thereto. Each party agrees that with respect to the Confidential Information of the other party, during the term of this Agreement and thereafter, such party: (a) shall at all times maintain the confidentiality of the Confidential Information, using the same degree of care that such party uses to protect its own confidential information of a like nature and, (b) shall not disclose the Confidential Information to any other individual, entity, or third party, except as permitted herein or as may be requested or required by (or as deemed advisable by counsel under) applicable law, rule, regulation, court order, legal process, or governmental, judicial, regulatory, or self-regulatory oversight.

5. Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. §1232g; 34 CFR Part 99) is a federal law that protects the privacy of student education records. You are required to comply with FERPA and its applicable regulations. Gaggle shall not disclose any student's education records, personally identifiable information, or other related records monitored, maintained, and retained by Gaggle and/or other Services provided by Gaggle to any third party (other than your school organization) without prior authority. Gaggle shall maintain the privacy and confidentiality of all student education records and shall make available to your school organization the right to inspect and review the student education records upon request. Gaggle shall not disclose or transmit student education records or information to any unauthorized party without the prior consent of the student, guardian, and/or your school organization, or by court order, administrative order, or subpoena. Notwithstanding the foregoing, to protect your school or district against the risks involved in handling explicit content involving minors, Gaggle registers incidents containing pornographic videos and images of possible minors with the CyberTipline at the National Center for Missing and Exploited Children ("NCMEC"). It is NCMEC's mission to prevent the spread of these materials, as well as to prevent the sexual exploitation of children. For more information, consult the Gaggle Student Data Privacy Notice.

6. Support

Gaggle maintains a case system to manage all Customer issues. Gaggle provides customer service between the hours of 6:00 AM and 7:00 PM CT Monday through Friday. Customers can reach Gaggle by email (support@gaggle.net), telephone (800-288-7750), or by accessing a live chat feature within the Gaggle

interface and on the Gaggle website. After-hours support is provided through a monitored email account at support@gaggle.net.

Gaggle provides additional technical support twenty-four (24) hours per day, seven (7) days per week. Response time commitments are made based on the severity of the issue, ranging from six (6) hours for critical issues to twenty-four (24) hours for informational requests.

7. Assignment

Neither party may assign or transfer any part of this Agreement without the written consent of the other party, but only if: (a) the assignee agrees in writing to be bound by the terms of this Agreement, and (b) the assigning party remains liable for obligations incurred under the Agreement prior to the assignment. Any other attempt to transfer or assign is void.

8. Term of Agreement.

This agreement commences with the start of Services and continues until otherwise terminated, by written agreement of the parties, in accordance with Section 10 or upon the expiration of the last Service Term or Renewal thereof.

9. Automatic Renewal of Services

Except as otherwise specified, Services shall automatically renew for successive one-year periods, unless and until terminated by either party in accordance herewith or unless either party provides written notice of non-renewal to the other party prior to the end of the then-current Services Term. Gaggle may increase pricing applicable to the renewal of any then-current Services Term by providing Customer with notice thereof, including by email, at least 30 days prior to the end of such term.

10. Termination

Customer may terminate the Services under this Agreement at the end of any contract by providing thirty (30) days' written notice of the intent to terminate. Gaggle may also terminate or suspend Services if you breach the conditions of this Agreement, the Gaggle Service Level Agreement (SLA), your contract, or Subscription Agreement.

You can cancel your Services by sending your cancellation notice to Gaggle, P.O. Box 735566, Dallas, TX 75373-5566; sending email to support@gaggle.net; or by fax to 309-665-0171.

Gaggle can, at any time, modify or discontinue any of its Services without liability to any user or third party.

11. Limitation of Liability, Statute of Limitations

In no event shall Gaggle be liable with respect to Services (i) for any amount in the aggregate in excess of the fees paid by you; or (ii) for any indirect, incidental, punitive, or consequential damages of any kind whatsoever. Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitations and exclusions may not apply to you. You agree that regardless of any statute or law to the contrary, any claim or cause of action against Gaggle arising out of or related to use of Services or the

terms of use must be filed within one (1) year after such claim or cause of action arose or be forever barred.

You assume total responsibility for the use of Gaggle Services and use these Services at your own risk. Gaggle exercises no control over and has no responsibility whatsoever for actions taken on the internet, and Gaggle expressly disclaims any responsibility for such actions. You acknowledge to Gaggle, and for Gaggle's benefit and the benefit of its directors, employees, licensors, and agents, that the Services may contain bugs and are not designed or intended for use in mission-critical environments requiring fail-safe performance.

12. Message Storage, Content Storage, and Other Limitations

The amount of email storage space and content storage space is limited for each user depending upon your contract or Subscription Agreement.

13. Communications

Except for any disclosure by you for technical support purposes, or as specified in the Gaggle Privacy Policy, all communications from you will be considered non-confidential and nonproprietary. You agree that any and all comments, information, feedback, and ideas that you communicate to Gaggle will be deemed, at the time of the communication, the property of Gaggle, and Gaggle shall be entitled to full rights of ownership including, without limitation, unrestricted right to delete, use, or disclose such communication in any form, medium, or technology now known or later developed, and for any purpose, commercial or otherwise, without compensation to you. You are solely responsible for the content of your communications and their legality under all laws and regulations. You agree not to use Gaggle Services to distribute, link to, or solicit content that is defamatory, harassing, unlawful, libelous, harmful to minors, threatening, obscene, false, misleading, or infringing a third-party intellectual property or privacy rights.

14. Miscellaneous

Gaggle provides Services to your organization to assist it in the protection of your students and your organization. Gaggle shall undertake every commercially reasonable effort to update its Services to maximize detection of unsafe, graphic, and/or obscene communications. Gaggle does not warrant, represent, and/or guaranty that all unsafe communications can or will be detected while monitoring your student communications or website content.

Gaggle shall not be responsible for contacting, notifying, or alerting any governmental agency or bureau including, but not limited to, child protective services agencies, with jurisdiction over your organization (Customer) for which notification has been provided to Customer. Your organization is responsible for reviewing all Gaggle communications, and to take all reasonable and precautionary actions required by your organization to protect the interests of students including, but not limited to, notifying applicable governmental agencies and/or bureaus, such as child protection services pursuant to the Family Educational Rights and Privacy Act (FERPA) and other applicable laws and regulations.

15. Notices

Unless specified otherwise herein: (a) all notices must be in writing and addressed to the attention of the other party's legal department and primary point of contact; and (b) notice will be deemed given: (i) when

verified by written receipt if sent by personal courier, overnight courier, or when received if sent by mail without verification of receipt; or (ii) when verified by automated receipt or electronic logs if sent by facsimile or email.

16. Indemnity

You agree to indemnify, defend, and hold Gaggle and its respective officers, directors, shareholders, employees, agents, representatives, successors, and assigns (collectively, the "Gaggle Indemnified Persons") harmless from and against any and all third-party claims, liabilities, damages, losses, or expenses (including reasonable attorney's fees and costs) arising out of, based on, or in connection with your access and/or use of Gaggle Services.

Gaggle's indemnification from third-party claims for which we have no control, even when we do our job with 100% professionalism and client satisfaction, is a requirement of our insurance carriers and legal team.

Notwithstanding the foregoing, your indemnification obligations shall be limited to the extent that such claims or demands are the results of Gaggle's breach of contract, gross negligence, or willful misconduct.

17. Taxes

All fees set forth in this Agreement and any invoices shall include all taxes except such "Transaction Taxes" which Gaggle is required by law to invoice and collect from Customer. Transaction Taxes, if any, will be separately stated on the invoice and will be paid by Customer to Gaggle unless Customer provides an exemption certificate to Gaggle or the transaction is statutorily exempt from Transaction Taxes. Gaggle shall be solely responsible for the timely remittance of all Transaction Taxes to the applicable Governmental Authority, and Gaggle shall pay (without reimbursement by Customer), and shall hold Customer harmless against, any penalties, interest, or additional taxes that may be levied or assessed as a result of the failure to invoice or delay of Gaggle to pay any such taxes. "Transaction Taxes" means sales and use taxes, value-added taxes, goods and services taxes, gross receipts taxes, and excise taxes, and excludes any tax on income, real or personal property taxes, or payroll taxes.

18. Trademarks

The trademarks, service marks, logos, slogans, and product designations of Gaggle ("Trademarks") are the property of Gaggle.Net, Inc., and/or their respective owners. You have no right to use any such Trademarks, and nothing contained in Gaggle Services grants any right to use (by license, implication, waiver, estoppel, or otherwise) any Trademarks without the prior written permission of Gaggle or the respective owner.

19. Acknowledgment of Ownership Rights and Disclosure of Deliverables

Gaggle does not convey any ownership in and Gaggle will own in perpetuity all right, title, and interest, worldwide, in and to: (i) any intellectual property or related rights owned or licensed by Gaggle and used in the performance of Gaggle's service hereunder, including Gaggle's Confidential Information, and (ii) the frameworks, methodologies, processes, inventions, analytical tools, and industry data and insights that may be used or developed by Gaggle in the performance of Gaggle's services hereunder along with any and all intellectual property rights in connection with the foregoing (the "Gaggle IP").

20. Choice of Law

This Agreement is made in and shall be interpreted and governed in all respects in accordance with the laws of the State of Delaware without giving effect to any choice of law or conflict of law rules or provisions.

21. Violations

Please report any violations of these Terms & Conditions to Gaggle's Customer Service department at 800-288-7750, via email at support@gaggle.net, or fax to 309-665-0171.

22. General Questions

If you have any questions regarding the Terms & Conditions, please contact Gaggle's Customer Service department at 800-288-7750, via email support@gaggle.net, or fax to 309-665-0171.

Gaggle Student & Staff Data Privacy Notice

Last Updated: January 13, 2022

Gaggle.Net, Inc. (Gaggle) has been working with K-12 schools and school districts since 1998 and has always maintained clear terms regarding how we treat student and staff data. We reinforce our commitment through participation in a pledge created by the Future of Privacy Forum (FPF) and the Software & Information Industry Association (SIIA) to advance data privacy protection regarding the collection, maintenance, and use of personal information.

We will:

- Not sell student or staff information
- Not behaviorally target advertising nor show advertising to any user
- Use data for authorized education purposes only
- Enforce strict limits on data retention
- Support parental access to, and correction of errors in, their children's information
- Provide comprehensive security standards
- Be transparent about the collection and use of data

Definition of Data

Data includes all personally identifiable information (PII) and other non-public information. Data includes, but is not limited to, student data, staff data, metadata, and user content.

Scope of Policy

This Policy describes the types of information we may collect, or that you may provide, when registering with, accessing, or using Gaggle solutions. This Policy does not apply to information we collect offline or on Gaggle websites (such as our [company website here](#)) or to information that you may provide to, or is collected by, third parties.

Purpose of Data Collection and Ownership

We consider all school and district data to be confidential and do not use such data for any purpose other than to provide services on your behalf and as outlined in your service level agreement or contract. Student data is the property of the school or district and remains in the school or district's control throughout the duration of any agreement/contract.

Role of School and School Officials

Although this Policy will focus mainly on what we do, and what we confirm we will not do, with student and staff data, we believe that schools and school officials are critical partners in our collective efforts to protect and ensure only appropriate use of student-related information entrusted to them and us. In that regard, schools and school officials using Gaggle solutions should be mindful that in granting or allowing access to Gaggle solutions, they are controlling who has access to student and staff information. When we reference "granting or allowing access," we are referring to both intentional actions, such as an administrator

authorizing a Gaggle account for a teacher or a student, as well as unintentional actions and consequences that may flow from, for example, a school's failure to maintain sufficient data governance or security practices.

In cases where the Family Educational Rights and Privacy Act (FERPA) applies, access to certain student information remains the legal responsibility of the applicable school. In all situations, it is incumbent upon our customers to make an affirmative determination before furnishing access to anyone that the party has a legitimate need for access to Gaggle solutions and the sensitive information that may be accessible to that party through Gaggle solutions.

Information About Students

FERPA and Education Records

Although FERPA was enacted decades ago, and certainly well before internet-based services became ubiquitous in academic settings, one of its core tenets was and remains the protection of the privacy of PII in students' education records. As defined in FERPA, "education records" are "those records, files, documents, and other materials which (i) contain information directly related to a student; and (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution." PII from education records includes information such as a student's name or identification number, which can be used to distinguish or trace an individual's identity, either directly or indirectly through linkages with other information.

FERPA requires that educational institutions and agencies that receive certain federal funds (for example, public schools) get prior consent from a parent or legal guardian before disclosing any education records regarding that student to a third party. Consequently, before you enter, upload, or access any data concerning a minor student, you must confirm that your agency or institution has (1) obtained appropriate consent from the parent or guardian of that student or (2) determined that one of the limited exceptions to the consent requirement applies.

Gaggle only uses PII from students' education records to enable the use of Gaggle solutions. Unless a school official expressly instructs otherwise, we will not share or reuse PII from education records for any other purpose. While we think those statements are clear, to avoid any doubt, we will not use student PII to target students or their families for advertising or marketing efforts or sell rosters of student PII to third parties.

COPPA and Children Under the Age of 13

The Children's Online Privacy Protection Act (COPPA) is a federal law designed to protect the privacy of children under 13 years old.

Gaggle's services are in compliance with the Children's Online Privacy Protection Act of 1998.

1. Individual children are not allowed to sign up for any Gaggle solutions. The only way a child may obtain access to a Gaggle solution is through their school.
2. Each school is responsible for creating student accounts for any Gaggle solution. For example, schools may choose to list students' full names, grade level, and ID number in the record for each user. Entering data in these fields is optional and is intended for administrative purposes only.

3. The schoolwide data collected by Gaggle is the school's address, grade levels, and other aggregate information about the school's internet connection, computers, and the likelihood of students having devices such as smartphones or tablets.

Disclosure and Retention of PII

Gaggle will not distribute to third parties any staff data or student data without the consent of either a parent/guardian or a qualified educational institution except in cases of Possible Student Situations (PSS), which may be reported to law enforcement.

To protect your school or district against the risks involved in handling sexually explicit content involving minors, Gaggle registers incidents containing explicit videos and images of possible minors with the CyberTipline at the National Center for Missing and Exploited Children (NCMEC). It is NCMEC's mission to prevent the spread of these materials, as well as to prevent the sexual exploitation of children.

We may also disclose student or staff data to comply with a court order, law, or legal process (including a government or regulatory request), but before doing so, we will provide the applicable school with notice of the requirement so that, if the school so chooses, it could seek a protective order or another remedy. If after providing that notice we remain obligated to disclose the demanded student or staff data, we will disclose no more than that portion of data which, on the advice of our legal counsel, the order, law, or process specifically requires us to disclose.

If a third party purchases all or most of our ownership interests or assets, or we merge with another organization, it is possible that we would need to disclose data to the other organization following the transaction; for example, were we to integrate Gaggle with the other organization's product offerings. To the extent any such transaction would alter our practices relative to this Policy, we will give schools or school districts notice of those changes and any choices they may have regarding student or staff data. Notwithstanding the foregoing, in the event of a merger, acquisition, or substantial transfer of assets, we will hold the new entity to its own privacy policy, or give users (or the school or the school district) the option to opt out of their data being included in the transaction.

Finally, although we outlined earlier in this Policy what constitutes student or staff data, we also want to be clear about what information is not student or staff data or PII. Once PII, whether relating to a school or district employee or student, has been de-identified, that information is no longer PII. PII may be de-identified through aggregation or various other means. The U.S. Department of Education has issued [guidance on de-identifying PII in education records](#). In order to allow us to proactively address customer needs, we anticipate using de-identified information to improve Gaggle solutions and services. That said, we would use reasonable de-identification approaches to ensure that, in doing so, we are not compromising the privacy or security of the PII you entrust to us. We will not attempt to re-identify de-identified data and will not transfer de-identified data to any party unless that party agrees not to attempt re-identification.

Data Security and Protection of Data, Including PII

We have implemented measures designed to secure PII from accidental loss and unauthorized access, use, alteration, and disclosure. Among other things, PII is encrypted in transit to and from Gaggle using SSL technology. In addition, all PII is stored in multiple databases with extensive redundancy and failover

maintained at data centers located in two geographically dispersed states, consistent with guidance from the U.S. Department of Education that storing sensitive education records within the United States is a ["best practice."](#) That said, unfortunately, the transmission of information via the internet is not completely secure and, although we do our best to protect PII, neither we nor any other hosted service provider can guarantee the security of all personally identifiable information.

Data integrity and accuracy are achieved through strict restrictions on how data may be accessed and by whom. Audit logs are kept to be able to track data modification. Additional security measures are in place to prevent and identify data tampering. In the extremely rare case of a data breach, we will immediately notify all customers affected using the primary email address specified in their accounts. It is the responsibility of our customers to contact parents or legal guardians regarding a data breach.

Gaggle has completed a SOC 2 Type 2 audit of the Trust Service Principles: Security, Availability, and Privacy. Our assessors' review of our technology and practices resulted in a final SOC 2 report free of any disclosures, which evidences Gaggle's unwavering commitment to information security and keeping our customers' data safe.

According to the American Institute of CPAs:

"A Software-as-a-Service (SaaS) or Cloud Service Organization that offers virtualized computing environments or services for user entities and wishes to assure its customers that the service organization maintains the confidentiality of its customers' information in a secure manner and that the information will be available when it is needed. A SOC 2 report addressing security, availability, and confidentiality provides user entities with a description of the service organization's system and the controls that help achieve those objectives."

Expiration of Agreement and Disposal of Data, Including PII

Upon the expiration or termination of any agreement/contract between a school or school district and Gaggle, we keep customer data for up to 30 days except in cases where state laws require a specific shorter or longer duration.

Any retained data will, of course, remain subject to the restrictions on disclosure and use outlined in this policy for as long as it resides with us.

Correction of Data

We only accept requests to change data from main contacts and administrators. Parents or legal guardians who request changes to student data should go through a school- or district-authorized main contact or administrator.

Focused Collection

- Geolocation data is not collected.
- Gaggle does not collect biometric data.
- No sensitive data is intentionally collected.

Data Collection

- All data is used only for the purpose for which it was collected for product requirements to ensure student safety.
- Gaggle does not combine personally identifiable information except for data produced by the school or district.
- No specific types of personal information are collected.
- No user personal information is acquired from third parties.
- The product does not provide any links to external websites.
- Third parties are not allowed to access user information.

Data Sharing

- No data is shared with unrelated third parties unless requested by a customer or as required by law.
- While aggregate data is maintained, none is shared with unrelated third parties.
- Data is never shared with unrelated third parties for research, although de-identified data is used to improve the product.
- Gaggle does not work with unrelated third-party service providers, nor does Gaggle share data with any such providers.
- Gaggle does not support social or federated logins.
- There is no unrelated third-party access to data and thus no contractual limits are set.

Data Security

- User identity is not linked to other sources, except student information systems as provided by the school or district.
- Third-party contractual protections are not required as there are no third-party agreements.

Data Rights

- Schools and districts operating in loco parentis control all student information and privacy settings.
- Users do not create or upload data on Gaggle but may do so via the platforms being monitored.
- Schools and districts may download data from the system.

Data Sold

- No user data is ever sold to third parties. As such, an opt out is unnecessary.
- User information is never transferred to a third party.
- Data is not shared with third parties for research or product improvement.

Data Safety

- Users cannot communicate with untrusted users via Gaggle. No communication via Gaggle is enabled for Gaggle Safety Management.
- Users do not create profiles on Gaggle, nor do they engage in social interactions in the safety management system.
- No personal information is displayed publicly.
- All user-created data is content filtered and none is displayed publicly.
- All interactions between users, social or otherwise, and administrator activities are logged.

- Users can report abuse or cyberbullying either directly in content, via the SpeakUp for Safety tipline, or by contacting Customer Support.

Ads & Tracking

- No marketing messages are ever sent to end users.
- Gaggle does not engage in sweepstakes, contests, or surveys with end users.
- Gaggle does not engage in contextual or behavioral marketing.

Parental Consent

- Gaggle is only provided to schools and districts operating in loco parentis. Students are subject to the school's acceptable use policy.
- COPPA parental consent is provided via the school or district operating in loco parentis.
- Parental consent with respect to third parties does not apply as there are no third-party relationships and consent is provided by the school or district.
- Parental consent can be withdrawn via arrangements with the school or district.
- Parental consent notice and submission methods are provided via the school or district.

School Purpose

- Gaggle is designed and built for K-12 students, schools, and districts but is not marketed to students.
- Gaggle does not publish or disclose directory information.

Changes to This Policy

We may update this Policy from time to time. If we make material changes, we will post the updated policy on this page (with a notice that the policy has been updated) and notify all customers by email using the primary email address specified in their accounts.

Contact Information

You can, and should, ask questions about this Policy and our privacy practices. You should always feel free to contact us at:

Gaggle.net, Inc.
5050 Quorum Drive
Suite 700
Dallas, TX 75254
Phone: (800) 288-7750
Email: support@gaggle.net



Gaggle Privacy Policy

Last Updated: September 9, 2022

Welcome to the company website of Gaggle.Net, Inc. (Gaggle).

This policy describes the types of information we may collect from you or that you may provide when you visit <http://www.gaggle.net> (the "Company Site") and our practices for collecting, using, maintaining, protecting, and disclosing that information. Please note: The information herein represents only the Company Site at <https://www.gaggle.net> and not Gaggle.Net, Inc. ("Gaggle") Solutions ("Services").

The Company Site is intended for a general audience. Although we may permit educators and parents to access Gaggle solutions through links provided on the Company Site, access to and use of Gaggle solutions is governed by separate agreements with customers and authorized users, including our [Student Data Privacy Notice](#), [Terms & Conditions](#), and [Service Level Agreement](#). In addition, this policy does not apply to information collected by us offline or through any other means or by any third party, including through application or content (including advertising) that may link to or be accessible from or on the Company Site.

Please read this policy carefully to understand our policies and practices regarding your information and how we will treat it. If you do not agree with our policies and practices, your choice is not to use the Company Site. By accessing or using the Company Site, you agree to this privacy policy. This policy may change from time to time (see "Changes to this Privacy Policy"). Your continued use of the Company Site after we make changes is deemed to be acceptance of those changes, so please check the policy periodically for updates.

Children Under the Age of 13 and Student Education Records

The Company Site is not intended for children under 13 years of age or for use in connection with student education records. We do not knowingly collect personal information from children under 13, or information that may comprise student education records, through the Company Site. If you are under 13, do not use or provide any information on the Company Site or on or through any of its features. In addition, regardless of age, you should never provide student education records on or through the Company Site. If we learn we have collected or received personal information from a child under 13 without verification of parental consent or any education records of a minor student through the Company Site, we will delete that information.

To learn more about our practices with respect to student information entered into Gaggle solutions, please refer to our [Student Data Privacy Notice](#).

Information We Collect About You and How We Collect It

We collect several types of information from, and about, users of the Company Site, including information:

- By which you may be personally identified, such as name, employer, job title, postal address, email address, and telephone number ("personal information")
- About your internet connection, the equipment you use to access the Company Site, and other usage details

We collect information:

- Directly from you when you voluntarily provide it to us by completing web forms on the Company Site, such as requests for marketing or other information
- Automatically as you navigate through the Company Site, such as usage details, IP addresses, operating systems, browser types, and information collected through automatic data collection technologies, including cookies, web beacons, and other tracking technologies
- That details your visits to the Company Site, including traffic data, location data, logs, and other communication data, and the resources that you access and use on the Company Site
- Including records and copies of your correspondence (including email addresses), if you choose to contact us
- To help us estimate our audience size and usage patterns
- To recognize you when you return to the Company Site

The technologies we use for this automatic data collection may include:

Cookies (or browser cookies): A cookie is a small file placed on the hard drive of your computer. You may refuse to accept browser cookies by activating the appropriate setting on your browser. However, if you select this setting, you may be unable to access certain parts of the Company Site. Unless you have adjusted your browser setting so that it will refuse cookies, the Company Site will issue cookies when you direct your browser to the Company Site.

Web Beacons: Pages of our Company Site and our emails may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit us, for example, to count users who have visited those pages or opened an email and for other related website statistics (for example, recording the popularity of certain website content and verifying system and server integrity).

Third-Party Use of Tracking Technologies

The Company Site works with third parties when you use the Company Site and to perform services on our behalf. We do not control these third parties' tracking technologies or how they may be used. If you have any questions, you should contact the responsible provider directly.

- **Act-On** allows us to track the activity of anonymous and known prospects coming to the Company Site.
- **AddThis** is a social bookmarking service integrated into the Company Site through the use of a web widget to allow visitors to easily share content.
- **Disqus** is a networked community platform that allows the Company Site to gain a feature-rich comment system complete with social network integration, advanced administration and moderation options, and other extensive community functions.
- **Google Analytics** is a web analysis service provided by Google Inc. ("Google"). Google utilizes the data collected to track and examine the use of the Company Site, prepare reports on its activities, and share them with other Google services.
- **Service Cloud** is a customer service platform that allows the Company Site to create customer relationships that are meaningful, personal, and productive through the use of live chat.

How We Use Your Information

We use information that we collect about you, or that you provide to us while visiting the Company Site, including any personal information:

- To present the Company Site and its contents to you
- To provide you with information about solutions or services that you request from us or that may be relevant to you
- To fulfill any other purpose for which you provide it
- To carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including for billing and collection
- To notify you about changes to the Company Site or any of our solutions or services
- In any other way that we may describe when you provide the information
- For any other purpose with your consent

Disclosure of Your Information

We may disclose aggregated information about our visitors to the Company Site, and information that does not identify any individual, without restriction. Unless otherwise stated herein, we will not disclose to any third party personal information that we collect or that you provide unless you provide consent to do so. We may disclose your personal information:

- To a buyer or other successor in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of the Company's assets
- To comply with any court order, law, or legal process, including responding to any government or regulatory request
- To enforce or apply our Terms & Conditions or Service Level Agreement
- If we believe disclosure is necessary or appropriate to protect the rights, property, or safety of our company, our customers, or others

Choice/Opt Out

The Company Site gives users the following options for removing their information from our database to not receive future communications or to no longer receive our service:

- You can send an email to support@gaggle.net
- You can send mail to the following postal address: P.O. Box 735566, Dallas, TX 75373-5566
- You can call the following telephone number: 800-288-7750

Correcting and Updating Information

The Company Site gives users the following options for changing and modifying information previously provided:

- You can send an email to support@gaggle.net
- You can send mail to the following postal address: P.O. Box 735566, Dallas, TX 75373-5566
- You can call the following telephone number: 800-288-7750

Telephone Calls

Telephone calls to and from Gaggle may be recorded for training or monitoring purposes only.

Trademarks

All trademarks, service marks, trade names, logos, and graphics (“Marks”) indicated on this site are registered trademarks of Gaggle, its affiliates, and/or licensors in the United States and other countries. You may not make any use of Gaggle Marks without the prior written consent of Gaggle.Net, Inc.

The company, solutions, and service names used on this website are for identification purposes only. All trademarks and registered trademarks are the properties of their respective owners.

Changes to This Policy

It is our policy to post any changes we make to our privacy policy on this page. If we make material changes to how we treat our users’ personal information, we will notify you via a notice on the Company Site home page. The date the privacy policy was last revised is identified at the top of the page. You are responsible for periodically visiting the Company Site and this privacy policy to check for any changes.

Contact Information

You can, and should, ask questions about this policy and our privacy practices, or feel free to report complaints. You should always feel free to contact us at:

Gaggle.net, Inc.
5050 Quorum Drive
Suite 700
Dallas, TX 75254
Phone: (800) 288-7750
Email: support@gaggle.net



ATTACHMENT 1 - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	We consider all school and district data to be confidential and is not used for any purpose other than to provide services on your behalf and as outlined in your service level agreement or contract. Student data is the property of the school or district and remains in the school or district's control throughout the duration of any agreement/contract.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Gaggle utilizes a multi-tiered security solution to protect the host environment. Gaggle utilizes NIST operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are in place and certified in Gaggle's SOC2 Audit. Gaggle restricts physical access to facilities and protected information assets. Access rules are created and maintained by information security personnel during the application development process. Access to data is restricted to authorized applications through access control software. Access rules are created and maintained by information security personnel during the application development process.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the	In accordance with FERPA/COPPA and iKeepSafe Harbor [®] guidelines. Gaggle

	Contract on the federal and state laws that govern the confidentiality of PII.	employees are given extensive security training upon hire, which is repeated annually, with specific PII security training quarterly.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	All FTEs, contractors and external collaborators sign defined scope of work prior to engagement, and an NDA is signed.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	Gaggle has an extensive, proprietary disaster and security response plan that was evaluated during our SOC2 audit. Here is a summary from our Identify scope of impact, including affected system(s) and data. Limit scope of impact. Establish a secure restore point for any lost hardware or software endpoints. Restore servers, services and applications in order of criticality per I.T Systems details, utilizing backups if necessary. Per Gaggle's Security Incident Response Policy In the extremely rare case of a data breach, we will notify all customers affected using the primary email address specified in their accounts, within 24 hours of confirmed breach.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Data is always the property of the District. If archival services are enabled data will be purged within 30 days or the agreed upon retention period as outlined in your service level agreement or contract.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Data disposal occurs in accordance with prescribed retention policies (see: GSM Retention Policies as outlined in your service level agreement or contract), at the end of a customer engagement, or upon an official and acknowledged request for data destruction from an authorized customer contact. Exceptions to policies regarding the retention of confidential or sensitive

		information assets (for example, litigation holds) are handled on a case-by-case basis by operational and executive management.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Gaggle agrees to abide by the rules and regulations outlined by COPPA and FERPA. Gaggle utilizes NIST operational requirements that support the achievement of security commitments, relevant laws and regulations. Such requirements are in place and certified in Gaggle's SOC2 Audit.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

ATTACHMENT 1(a) - NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	An asset management system is in place, cataloging all physical devices and systems. The location and scope of confidential information is documented. Mobile device management is in place and configurations are centrally managed All physical systems (both workstations and servers) are inventoried, and that all assets are assigned an owner. Software platforms and applications within the organization are inventoried.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this	Gaggle's role in the supply chain (position within customer mail flow) is clearly documented and communicated. Clear descriptions of Gaggle's product offerings are available on the company website, and detailed documentation is provided to

Function	Category	Contractor Response
	information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	customers prior to engagement. A Disaster Recovery Plan is in place and is tested at least annually to ensure fitness and efficacy.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Detailed cybersecurity policies are in place and revised annually (eg Security Awareness Training, Acceptable Use, Data Classification) All facets of information security are considered during the development of and reflected by the presence of comprehensive internal and external information security policies.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	A comprehensive Risk Assessment Policy is in place to assess vulnerabilities within the system. Risk assessments are performed annually, assessing and documenting risks and their mitigation efforts. The Risk Assessment Policy includes a Vendor Risk Assessment Policy to assess risk associated with third-party applications and services used in support of the system at least annually, and prior to engagement. The Risk Assessment Policy includes an assessment of risks associated with internal and external fraud.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	The Risk Assessment Policy includes a threat and risk matrix, documenting the business impact and likelihood of specific events and any associated mitigation efforts. The Risk Assessment Policy includes a Vendor Risk Assessment Policy to assess risk associated with third-party applications and services used in support of the system at least annually, and prior to engagement.
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	The Risk Assessment Policy includes a Vendor Risk Assessment Policy to assess risk associated with third-party applications and services used in support of the system at least annually, and prior to engagement. A Disaster Recovery Plan is in place and is tested at least annually to ensure fitness and efficacy.
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	An Access Control policy is in effect and maintained, reviewed at least annually. Role-based access is in effect, with regular (at least quarterly) access reviews. All production systems of record are included within quarterly access reviews. Physical security to the environments is maintained by third-party data center and cloud providers. Third-party attestation reports (ie, SOC) are reviewed annually to ensure control adherence and efficacy.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	Role-based access is utilized, with regular (at least quarterly) access reviews, following the least level of privilege model. Clearly-defined job descriptions and scorecards exist for roles requiring privileged access, and are available for review on an internal wiki. All contractors or external collaborators sign defined scope of work prior to engagement, and an NDA is signed.

Function	Category	Contractor Response
		<p>Customers are asked to sign a master services agreement prior to start of services.</p> <p>Information security policies are made available for public review on the corporate website.</p>
	<p>Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.</p>	<p>Backups, flat files, and other data at rest is protected via encryption (AES-256 min.)</p> <p>All internal network traffic, and external network traffic, is performed via encryption (TLS 1.2 min.)</p> <p>An asset management system is in place to document physical and logical assets</p> <p>An information and asset disposal policy is in place, strictly adhered to and reviewed annually.</p>
	<p>Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.</p>	<p>A System Configuration Policy is in effect and maintained, reviewed at least annually and containing guidelines for best practices and system configurations.</p> <p>An Access Control policy is in effect and maintained, reviewed at least annually.</p> <p>Configuration management software is used to inform system configurations.</p>
	<p>Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.</p>	<p>A Change Management policy is in effect and reviewed at least annually. Changes to critical production systems require review and approval prior to implementation.</p> <p>Role-based access is in effect, with regular (at least quarterly) access reviews.</p> <p>An Access Control policy is in effect and maintained, reviewed at least annually.</p> <p>A Remote Access policy is in effect and maintained, reviewed at least annually.</p>
	<p>Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</p>	<p>Audit logging is enabled on the production environment, and is reviewed regularly.</p> <p>Tools are in place to automatically analyze audit logs and surface abnormalities for review.</p> <p>Tools are in place (access rules, IPS/IDS, FIM, HBIPS, configurations, etc.) to protect communications and control networks from unauthorized access.</p> <p>Multi-factor authentication is used to protect access to communication systems and control networks.</p> <p>Abnormalities or malicious behaviors are detected and prevented in real time</p>
<p>DETECT (DE)</p>	<p>Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.</p>	<p>Systems are in place to monitor system performance and detect and alert upon any deviations.</p> <p>Intrusion detection and prevention technology is in place to detect, analyze, and mitigate cybersecurity incidents.</p> <p>Data flow diagrams are maintained, detailing the flow of information throughout the system. A comprehensive Security Incident Response Policy is in place and reviewed at least annually.</p> <p>Intrusion detection and prevention technology is in place to detect, analyze, and mitigate cybersecurity incidents. A Root</p>

Function	Category	Contractor Response
		Cause Analysis is performed following any security event, and includes an analysis of impact.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	<p>Systems are in place to monitor system performance and detect and alert upon any deviations.</p> <p>Intrusion detection and prevention technology is in place to detect, analyze, and mitigate</p> <p>Physical security to the environments is maintained by third-party data center and cloud providers. Third-party attestation reports (ie, SOC) are reviewed annually to ensure control adherence and efficacy.</p> <p>File integrity monitoring is in place, with alerting upon changes enabled</p> <p>A version tracking system is in place, requiring approval prior to system changes. Changes are clearly documented and communicated prior to implementation.</p> <p>Security controls are embedded within the development process to detect any malicious code prior to deployment.</p> <p>Intrusion detection and prevention technology is in place to detect, analyze, and mitigate cybersecurity incidents.</p> <p>Authentication systems detect abnormal login attempts and require administrator intervention to permit access.</p> <p>Devices accessing the system are cataloged and logs are available for review during any security event.</p> <p>IDS/IPS software is configured to proactively defend against malicious activity. Penetration testing is conducted at least annually, and results are communicated to operational and executive management.</p>
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	<p>Detection practices and policies are in keeping with industry-recognized information security frameworks, and are tested at least annually. Penetration testing is conducted at least annually, and results are communicated to operational and executive management.</p>
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	<p>A comprehensive Security Incident Response Policy is in place, and reviewed annually.</p> <p>A root cause analysis is conducted after significant system incidents and the results shared via internal wiki.</p> <p>A Disaster Recovery Plan is in place to inform recovery from critical system events.</p>
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	<p>A comprehensive Security Incident Response Policy is in effect and maintained, and contains policies regarding external communication of any security events.</p>
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	<p>Notifications from detection systems are investigated.</p> <p>The impact of the incident is understood. Forensics are performed. Incidents are categorized consistent with response plans. Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources.</p>
	Mitigation (RS.MI): Activities are performed to prevent expansion of an	<p>Incidents are contained and mitigated. Newly identified vulnerabilities are mitigated.</p>

Function	Category	Contractor Response
	event, mitigate its effects, and resolve the incident.	
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	A comprehensive Security Incident Response Policy is in place, and reviewed at least annually.
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	A Root Cause Analysis is performed following any security event, and includes recommendations for environmental improvements. Response plans incorporate lessons learned and strategies are updated
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	A comprehensive Security Incident Response Policy is in place, and reviewed at least annually. Incident Retrospectives for the year are included.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	A comprehensive Incident Response Policy is in effect and maintained, and contains policies regarding both internal and external communication of any security events.

