Gaggle

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

CONTRACT ADDENDUM

Protection of Student Personally Identifiable Information

1. Applicability of This Addendum

The Wayne-Finger Lakes BOCES/EduTech) and Gaggle.Net, Inc. **("Vendor")** are parties to a contract dated 2/12/2024 ("the underlying contract") governing the terms under which BOCES accesses, and Vendor provides, Gaggle Safety Management Services ("Product"). Wayne-Finger Lakes BOCES/EduTech use of the Product results in Vendor receiving student personally identifiable information as defined in New York Education Law Section 2-d and this Addendum. The terms of this Addendum shall amend and modify the underlying contract and shall have precedence over terms set forth in the underlying contract and any online Terms of Use or Service published by Vendor.

2. Definitions

2.1. "Protected Information", as applied to student data, means "personally identifiable information" as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act (FERPA) where that information is received by Vendor from BOCES or is created by the Vendor's product or service in the course of being used by BOCES.

2.2. "Vendor" means Gaggle.Net, Inc.

2.3. "Educational Agency" means a school BOCES, board of cooperative educational services, school, or the New York State Education Department; and for purposes of this Contract specifically includes Wayne-Finger Lakes BOCES/EduTech.

2.4. "BOCES" means the Wayne-Finger Lakes BOCES/EduTech.

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

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

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

2.8. "Assignee" and "Subcontractor" shall each mean any person or entity that receives, stores, or processes Protected Information covered by this Contract from Vendor for the purpose of enabling or assisting Vendor to deliver the product or services covered by this Contract.

2.9. "This Contract" means the underlying contract as modified by this Addendum.

3. Vendor Status

Vendor acknowledges that for purposes of New York State Education Law Section 2-d it is a third-party contractor, and that for purposes of any Protected Information that constitutes education records under the Family Educational Rights and Privacy Act (FERPA) it is a school official with a legitimate educational interest in the educational records.

4. Confidentiality of Protected Information

Vendor agrees that the confidentiality of Protected Information that it receives, processes, or stores will be handled in accordance with all state and federal laws that protect the confidentiality of Protected Information, and in accordance with the BOCES Policy on Data Security and Privacy, a copy of which is Attachment B to this Addendum.

5. Vendor EmployeeTraining

Vendor agrees that any of its officers or employees, and any officers or employees of any Assignee of Vendor, who have access to Protected Information will receive training on the federal and state law governing confidentiality of such information prior to receiving access to that information.

6. No Use of Protected Information for Commercial or Marketing Purposes

Vendor warrants that Protected Information received by Vendor from BOCES or by any Assignee of Vendor, shall not be sold or used for any commercial or marketing purposes; shall not be used by Vendor or its Assignees for purposes of receiving remuneration, directly or indirectly; shall not be used by Vendor or its Assignees for advertising purposes; shall not be used by Vendor or its Assignees to develop or improve a product or service; and shall not be used by Vendor or its Assignees to market products or services to students.

7. Ownership and Location of Protected Information

7.1. Ownership of all Protected Information that is disclosed to or held by Vendor shall remain with BOCES. Vendor shall acquire no ownership interest in education records or Protected Information.

7.2. BOCES shall have access to the BOCES's Protected Information at all times through the term of this Contract. BOCES shall have the right to import or export Protected Information in piecemeal or in its entirety at their discretion, without interference from Vendor.

7.3. Vendor is prohibited from data mining, cross tabulating, and monitoring data usage and access by BOCES or its authorized users, or performing any other data analytics other than those required to provide the Product to BOCES. Vendor is allowed to perform industry standard back-ups of Protected Information. Documentation of back-up must be provided to BOCES upon request.

7.4. All Protected Information shall remain in the continental United States (CONUS) or Canada. Any Protected Information stored, or acted upon, must be located solely in data centers in CONUS or Canada. Services which directly or indirectly access Protected Information may only be performed from locations within CONUS or Canada. All helpdesk, online, and support services which access any Protected Information must be performed from within CONUS or Canada.

8. Purpose for Sharing Protected Information

The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to Wayne-Finger Lakes BOCES/EduTech.

9. Downstream Protections

Vendor agrees that, in the event that Vendor subcontracts with or otherwise engages another entity in order to fulfill its obligations under this Contract, including the purchase, lease, or sharing of server space owned by another entity, that entity shall be deemed to be an "Assignee" of Vendor for purposes of Education Law Section 2-d, and Vendor will only share Protected Information with such entities if those entities are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract and all applicable New York State and federal laws.

10. Protected Information and Contract Termination

10.1. The expiration date of this Contract is defined by the underlying contract.

10.2. Upon expiration of this Contract without a successor agreement in place, Vendor shall assist BOCES in exporting all Protected Information previously received from, or then owned by, BOCES.

10.3. Vendor shall thereafter securely delete and overwrite any and all Protected Information 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 of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities.

10.4. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.

10.5. 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 removed) derived from Protected Information, they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10.6. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to BOCES from an appropriate officer that the requirements of this paragraph have been satisfied in full.

11. Data Subject Request to Amend Protected Information

11.1. In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the BOCES for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

11.2. Vendor will cooperate with BOCES in retrieving and revising Protected Information, but shall not be responsible for responding directly to the data subject.

12. Vendor Data Security and Privacy Plan

12.1. Vendor agrees that for the life of this Contract the Vendor will maintain the administrative, technical, and physical safeguards described in the Data Security and Privacy Plan set forth in Attachment C to this Contract and made a part of this Contract.

12.2. Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:

12.3. align with the NIST Cybersecurity Framework 1.0;

12.4. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;

12.5. outline how the Vendor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the BOCES data security and privacy policy (Attachment B);

12.6. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;

12.7. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;

12.8. specify how officers or employees of the Vendor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

12.9. specify if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;

12.10. specify how the Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify BOCES; and

12.11. describe whether, how and when data will be returned to BOCES, transitioned to a successor contractor, at BOCES's option and direction, deleted or destroyed by the Vendor when the contract is terminated orexpires.

13. Additional VendorResponsibilities

Vendor acknowledges that under Education Law Section 2-d and related regulations it has the following obligations with respect to any Protected Information, and any failure to fulfill one of these statutory obligations shall be a breach of this Contract:

13.1 Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;

13.2 Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract;

13.3 Vendor will not disclose any Protected Information to any party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Contract or to the BOCES unless (1) Vendor has the prior written consent of the parent or eligible student to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to BOCES no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

13.4 Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;

13.5 Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

13.6 Vendor will notify the BOCES of any breach of security resulting in an unauthorized release of student data by the 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 but no more than seven calendar days after the discovery of the breach; and

Where a breach or unauthorized disclosure of Protected Information is attributed to the Vendor, the Vendor shall pay for or promptly reimburse BOCES for the full cost incurred by BOCES to send notifications required by Education Law Section 2-d.

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Signatures

For Wayne-Finger Lakes BOCES/EduTech	**For (Vendor Name)**
Date 2/14/24	**Date** 2/12/2024

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment A – Parent Bill of Rights for Data Security and Privacy

Wayne-Finger Lakes BOCES (EduTech)

Parents' Bill of Rights for Data Privacy and Security

The Wayne-Finger Lakes BOCES (EduTech)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 BOCES and school operations.

The Wayne-Finger Lakes BOCES (EduTech)seeks to insure 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 Wayne-Finger Lakes BOCES (EduTech) 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 Board Policy 5500 entitled Family Educational Rights and Privacy Act (FERPA).
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.nysed.gov/data-privacy-security/student-data-inventory 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 the Chief Privacy Officer, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Revised October 2019

Signatures

For Wayne-Finger Lakes BOCES/EduTech	**For (Vendor Name)**
Date 2/14/24	**Date** 2/12/2024

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment B – Wayne-Finger Lakes BOCES/EduTech Data Privacy and Security Policy

In accordance with New York State Education Law §2-d, the BOCES hereby implements the requirements of Commissioner's regulations (8 NYCRR §121) and aligns its data security and privacy protocols with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or "NIST CSF").

In this regard, every use and disclosure of personally identifiable information (PII) by the BOCES will benefit students and the BOCES (for example, improving academic achievement, empowering parents and students with information, and/or advancing efficient and effective school operations). PII will not be included in public reports or other documents.

The BOCES also complies with the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA). Consistent with FERPA's requirements, unless otherwise permitted by law or regulation, the BOCES will not release PII contained in student education records unless it has received a written consent (signed and dated) from a parent or eligible student. For more details, see Policy 6320 and any applicable administrative regulations.

In addition to the requirements of FERPA, the Individuals with Disabilities Education Act (IDEA) provides additional privacy protections for students who are receiving special education and related services. For example, pursuant to these rules, the BOCES will inform parents of children with disabilities when information is no longer needed and, except for certain permanent record information, that such information will be destroyed at the request of the parents. The BOCES will comply with all such privacy provisions to protect the confidentiality of PII at collection, storage, disclosure, and destruction stages as set forth in federal regulations 34 CFR 300.610 through 300.627.

The Board of Education values the protection of private information of individuals in accordance with applicable law and regulations. Further, the BOCES Director of Educational Technology is required to notify parents, eligible students, teachers and principals when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and Board policy and New York State Education Law §2-d

a) "Private information" shall mean **personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

1. Social security number.
2. Driver's license number or non-driver identification card number; or
3. Account number, credit or debit card number, in combination with any required security code, access code, or password, which would permit access to an individual's financial account.
4. Any additional data as it relates to administrator or teacher evaluation (APPR)

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

**"Personal information" shall mean any information concerning a person, which, because of name, number, symbol, mark or other identifier, can be used to identify that person.

b) Personally Identifiable Information, as applied to student data, means 40 personally identifiable information as defined in section 99.3 of Title 34 of the Code of 41 Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 42 U.S.C 1232-g, and as applied to teacher and principal data, means personally 43 identifying information as such term is defined in Education Law §3012-c(10).

c) Breach means the unauthorized access, use, or disclosure of student data 9 and/or teacher or principal data. Good faith acquisition of personal information by an employee or agent of the BOCES for the purposes of the BOCES is not a breach of the security of the system, provided that private information is not used or subject to unauthorized disclosure.

Notification Requirements
Methods of Notification

The required notice shall be directly provided to the affected persons and/or their guardians by one of the following methods:

a) Written notice;

b) Secure electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and a log of each such notification is kept by the BOCES when notifying affected persons in electronic form. However, in no case shall the BOCES require a person to consent to accepting such notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;

Regardless of the method by which notice is provided, the notice shall include contact information for the notifying BOCES and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired. This notice shall take place 60 days of the initial discovery.

In the event that any residents are to be notified, the BOCES shall notify the New York State Chief Privacy Officer, the New York State Cyber Incident Response Team, the office of Homeland Security, and New York State Chief Security Officer as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected residents.
The Superintendent or his/her designee will establish and communicate procedures for parents, eligible students, and employees to file complaints about breaches or unauthorized releases of student, teacher or principal data (as set forth in 8 NYCRR §121.4). The Superintendent is also authorized to promulgate any and all other regulations necessary and proper to implement this policy.

Data Protection Officer

The BOCES has designated a BOCES employee to serve as the BOCES's Data Protection Officer.

The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures including those required by Education Law Section 2-d and its implementing regulations, as well as serving as the main point of contact for data privacy and security for the BOCES.

The BOCES will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1 (1988; rev. 2004).

Annual Data Privacy and Security Training

The BOCES will annually provide data privacy and security awareness training to its officers and staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations.

References:

Education Law §2-d

8 NYCRR §121

Family Educational Rights and Privacy Act of 1974, 20 USC §1232(g), 34 CFR 99

Individuals with Disabilities Education Act (IDEA), 20 USC §1400 et seq., 34 CFR 300.610–300.627

www.gaggle.net | P 800-288-7750 | F 309-665-0171
5050 Quorum Drive, Suite 700, Dallas, TX 75254

Gaggle Student & Staff Data Privacy Notice

Last Updated: July 17, 2023

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. See Data Collection section for specific data types.

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) 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, 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 to promote school safety and the physical security of students. 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.**

FERPA (§ 99.31(a)(1)(i)(B)) permits schools to outsource institutional services or functions that involve the disclosure of education records to contractors, consultants, volunteers, or other third parties provided that the outside party: Performs an institutional service or function for which the agency or institution would otherwise use employees; Is under the direct control of the agency or institution with respect to the use and maintenance of education records; Is subject to the requirements in § 99.33(a) that the personally identifiable information (PII) from education records may be used only for the purposes for which the disclosure was made, e.g., to promote school safety and the physical security of students, and governing the redisclosure of PII from education records; and Meets the criteria specified in the school or local educational agency's (LEA's) annual notification of FERPA rights for being a school official with a legitimate educational interest in the education records.

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. Gaggle Services participates in the iKeepSafe Safe Harbor program. If you have any questions or need to file a complaint related to our privacy policy and practices, please do not hesitate to contact the iKeepSafe Safe Harbor program at COPPAprivacy@ikeepsafe.org

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 students, the school or the 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 provide you with notice within thirty (30) days following the completion of such a transaction, by posting on our homepage and by email to your email address that you provided to us. If you do not consent to the use of

your information by such a successor company, subject to applicable law, you may request its deletion from the company.

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

- Types of Data we can collect: Student first and last name, Student Physical Address, Student ID, Parent/Guardian First and last name, Parent/Guardian Physical address, Parent/Guardian Phone/Mobile Number, Parent/Guardian Email Address. While Gaggle can collect this data if provided by the district, the student email is the only required data point for Gaggle Services to be enabled.
- Gaggle does not combine personally identifiable information except for data produced by the school or district.
- All data collected will be used solely for the stated purpose of ensuring student safety as required by the product. All data is used only for the purpose for which it was collected for product requirements to ensure student safety.
- 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.
- All data collected will be used solely for the stated purpose of ensuring student safety as required by the product.
- Data is never shared with unrelated third parties for research, although de-identified data is used to improve the product.

Data Storage

- While aggregate data is maintained, none is shared with unrelated third parties.

- **Third-Party Subprocessors**
  - **AWS (Amazon Web Services)** - for providing servers, databases and network infrastructure for storage, service delivery and other related services.
  - **Quadranet** - Physical Data Center that houses IT infrastructure for delivering applications and services. This location/Infrastructure is also used as a failsafe to provide 24/7 security and access control to our services.

Data Security

- User identity is not linked to other sources, except student information systems as provided by the school or district.
- Gaggle and our sub processing partners have completed a SOC 2 Type 2 audit of the Trust Service Principles: Security, Availability, and Privacy of all services and systems.

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 the 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, within 30 days 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

STUDENT PRIVACY PLEDGE SIGNATORY