Eastern Suffolk BOCES
Educational Services That Transform Lives

Education Law §2-d Rider

Board of Cooperative Educational Services
First Supervisory District of Suffolk County
201 Sunrise Highway
Patchogue, New York 11772
(631) 289-2200

New York State Education Law §2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law §2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor signs a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law §2-d, and Gaggle.Net, Inc. (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law §2-d, and notwithstanding any provision of the attached contract between the Board of Cooperative Educational Services, First Supervisory District of Suffolk County ("ESBOCES") and Contractor, including any Agreement to Terms attached thereto, to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that ESBOCES' and/or participating school districts' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time, if applicable.

"**Protected Data**" includes any information rendered confidential by State or federal law, including, but not limited to, student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by ESBOCES and/or participating school districts. Protected Data also includes any information protected under Education Law §2-d, including, but not limited to:

> "Personally identifiable information" from student records of ESBOCES and/or participating school districts as that term is defined in §99.3 of FERPA,
>
> -AND-
>
> Personally identifiable information from the records of ESBOCES and/or participating school districts relating to the annual professional performance reviews of classroom teachers or principals

that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record, or display any Protected Data shall comply with New York State Education Law §2-d. As applicable, Contractor agrees to comply with ESBOCES' policy(ies) on data security and privacy. Contractor shall promptly reimburse ESBOCES and/or participating school districts for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed, or is terminated, Contractor shall return all ESBOCES' and/or participating school districts' data, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record, or display any ESBOCES' and/or participating school districts' Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;

2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;

3. Specifies how officers or employees of the Contractor and its assignees 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;

4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency; and

6. Specifies whether Protected Data will be returned to ESBOCES and/or participating school districts, transitioned to a successor contractor, at ESBOCES' and/or participating school districts' option and direction, deleted or destroyed by the Contractor when the contract and/or the Agreement to Terms is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);

2. Comply with the data security and privacy policy of ESBOCES, Education Law §2-d, and Part 121;

3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;

4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;

5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

    a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or

    b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;

7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and

8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgment, acceptance, and signature of ESBOCES' or participating school district's Parents' Bill of Rights.

NAME OF CONTRACTOR: Gaggle.Net, Inc.

BY: 

DATED: 5/16/2023

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

EASTERN SUFFOLK BOCES
PARENTS' BILL OF RIGHTS
FOR DATA SECURITY AND PRIVACY

Eastern Suffolk BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, parents, legal guardians, and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information. Eastern Suffolk BOCES wishes to inform the school community of the following rights:

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 maintained by Eastern Suffolk BOCES.

3. State and Federal laws protect the confidentiality of personally identifiable information and safeguards associated with industry standards and best practices, including, but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4. A complete list of all student data elements collected by the State is available for public review at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, or, by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Claudy Damus-Makelele
Associate Superintendent for Educational Services
Eastern Suffolk BOCES
201 Sunrise Highway
Patchogue, NY 11772
cdamus@esboces.org

Or in writing to:

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, NY 12234
CPO@mail.nysed.gov.

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services, Eastern Suffolk BOCES has entered into contracts with certain third-party contractors. Pursuant to such contracts, third-party contractors may have access to "student data" and/or "teacher or principal data." Each contract

Eastern Suffolk BOCES enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data will include information addressing the following:

1. The exclusive purposes for which the student data or teacher or principal data will be used;

   Cloud Archiving and Backup services

2. How the third-party contractor will ensure that the subcontractors, persons, or entities with whom the third-party contractor will share the student data or teacher or principal data, if any, will abide by data protection and security requirements;

   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.

   In accordance with FERPA/COPPA and iKeepSafe Harbor® guidelines. Gaggle employees are given extensive security training upon hire, which is repeated annually, with specific PII security training quarterly.

3. When the contract expires and what happens to the student data or teacher or principal data upon expiration of the contract;

   District data will be purged or can be migrated back to the district for an additional fee.

4. If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data collected; and

   Complaints should be directed to: the Associate Superintendent for Curriculum for your district; Or in writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234, CPO@mail.nysed.gov.

5. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security) and the security protections taken to ensure that such data will be protected, including whether such data will be encrypted.

   Gaggle's archiving services are entirely cloud-based. All data is stored within the continental United States. Client data is stored on three separate storage systems in two geographically disparate data centers, providing data redundancy and security.

   Gaggle's data is stored in Amazon Web Services (AWS) and our own dedicated data center. Files are stored in an encrypted format, all communication is over Secure Sockets Layer (SSL), and all passwords are hashed. Data is retained for varying lengths of time depending upon the contract with the customer.

Backups, flat files, and other data at rest is protected via encryption (AES-256 min.)
All internal network traffic, and external network traffic, is performed via encryption (TLS 1.2 min.)
An asset management system is in place to document physical and logical assets
An information and asset disposal policy is in place, strictly adhered to and reviewed annually.

Third-Party Contractors are required to:

1. Provide training on Federal and State law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;

2. Limit internal access to educational records to those individuals who have a legitimate educational interest in such records;

3. Not use educational records for any other purpose than those explicitly authorized in the contract;

4. Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;

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

6. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;

7. Notify Eastern Suffolk BOCES of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;

8. Provide a data security and privacy plan outlining how all State, federal, and local data security and privacy contract requirements will be implemented over the life of the contract; and

9. Provide a signed copy of this Parents' Bill of Rights to Eastern Suffolk BOCES, thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

This Parents' Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

A copy of this signed document must be made a part of Contractor's Data Security and Privacy Plan.

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: Jun 1, 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. PII 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, t**o 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. T**he 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.
- 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**
        a. **AWS (Amazon Web Services) -** for providing servers, databases and network infrastructure for storage, service delivery and other related services.
        b. **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 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