DATA SECURITY AND PRIVACY PLAN

WHEREAS, the Liverpool Central School District (hereinafter "School District") and GeoGebra GmbH (hereinafter "Contractor") entered into an agreement dated 04/24/2024 (hereinafter "Agreement") for GeoGebra (hereinafter "Services").

WHEREAS, pursuant to the requirements under 8 NYCRR 121, Contractor maintains the data security and privacy plan described herein in connection with the Services provided to the School District.

1. During the term of the Agreement, Contractor will implement all state, federal and local data security and privacy requirements, consistent with the School District's Data Security and Privacy Policy in the following way(s

Physical security:
○ Access control: access for employees to data is password protected
○ Individuals are required to sign in/out for installation and removal of equipment
○ Data is hosted on Amazon Web Services (AWS). Backups for the servers, on which the data resides, are provided by Amazon RDS automated backups (https://aws.amazon.com/rds/details/backup/). The physical security for AWS is managed by Amazon RDS.

2. Contractor has in place the following administrative, operational and technical safeguards and practices to protect personally identifiable information that it will receive under the Agreement:

Technical security:
○ Our system employs encryption technologies when transmitting sensitive information (SSL/TLS, VPN) over the network.
○ If users have a GeoGebra account, passwords are encrypted by PHP's crypt function, using the Blowfish algorithm with a 16-character salt value.
○ We are utilizing a web application firewall (WAF) (managed by Amazon VPC)

3. Contractor shall comply with 8 NYCRR 121 in that it acknowledges that it has reviewed the School District's Parents Bill of Rights for Data Privacy and Security and will comply with same.

a. Contractor will use the student data or teacher or principal data only for the exclusive purposes defined in the Agreement.

b. Contractor will ensure that the subcontractor(s) or other authorized persons or entities to whom Contractor will disclose the student data or teacher and principal data, if any, will abide by all applicable data protection and security requirements as described in the "Supplemental Information" appended to the Agreement.

c. At the end of the term of the Agreement, Contractor will destroy, transition or return, at the direction of the School District, all student data and all teacher and principal data in accordance with the "Supplemental Information" appended to the Agreement.

d. Student data and teacher and principal data will be stored in accordance with the "Supplemental Information" appended to the Agreement.

e. Student data and teacher and principal data in motion and at rest will be protected using an encryption method that meets the standards described in 8 NYCRR 121.

4. Prior to receiving access to student data and/or teacher and principal data, officer(s) and employee(s) of Contractor and any assignees who will have access to student data or teacher or principal data shall receive training on the federal and state laws governing confidentiality of such data. Such training shall be provided:
Specify date of each training

All GeoGebra employees, with legitimate access to PII, receive twice a year updates regarding best privacy and security practices.

5. Subcontractors (select one): b. Contractor shall utilize subcontractors

a. Contractor shall not utilize subcontractors.

b. Contractor shall utilize subcontractors. Contractor shall manage the relationships and contracts with such subcontractors in the following ways in order to ensure personally identifiable information is protected:

For hosting our
web applications and data we use AWS (Amazon Web Services). AWS, our subcontractor, has one of the highest
privacy and security standards in place. It is compliant with GDPR, FERPA, NIST, ISO/IEC 27001:2013, etc.

6. Contractor has the following procedures, plans or protocols in place to manage data security and privacy incidents that implicate personally identifiable information:
Procedures, plans or protocols must, at a minimum, specify plans to identify breaches and unauthorized disclosures, and to promptly notify the School District.

If you become aware of a data breach please notify GeoGebra by writing an email to office@geogebra.org. We will try to remediate the issues as soon as possible.In case GeoGebra becomes aware of a data or security breach,it will either notify the educational institution with whom we have privacy agreements in place or the user directly and try to fix the issues as soon as possible.

7. Termination of Agreement.

a. Within 30 days of termination of the Agreement, Contractor shall delete or destroy all student data or teacher or principal data in its possession; AND

b. [x] Within 20 days of termination of the Agreement, Contractor shall Return all data to the School District using email; OR

☐ Transition all data to a successor contractor designated by the School District in writing using_____.

8. In the event of a conflict between the terms of this Data Security and Privacy Plan and the terms of the Agreement, the terms of this Data Security and Privacy Plan shall control. All of the defined terms in the Agreement shall have the same definitions in the Data Security and Privacy Plan, unless otherwise defined herein. Except as expressly set forth in this Data Security and Privacy Plan, the terms and conditions of the Agreement shall remain unmodified and in full force and effect.

IN WITNESS WHEREOF, the Contractor hereto has executed this Data Security and Privacy Plan as of 04/24/2024.

Contractor: GeoGebra GmbH

Title: Chief Executive Officer

Date: 04/24/2024

Parents Bill of Rights
Liverpool Central School District

The Liverpool School District is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, parents and eligible students can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency.

3. State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, that protect the confidentiality of a student's PII, 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 NYSED is available for public review and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

5. The right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints may be submitted to NYSED online, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234, by email to privacy@nysed.gov, or by telephone at 518-474-0937.

6. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.

7. Educational agency workers that handle PII will receive training on applicable state and federal laws, the educational agency's policies, and safeguards associated with industry standards and best practices that protect PII.

8. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

APPENDIX

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Liverpool School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

1. The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;

2. How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);

3. The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);

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 that is collected;

5. Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and

6. Address how the data will be protected using encryption while in motion and at rest.

Daniel P Farsaci

Liverpool Administrator Signature

Daniel Farsaci

Liverpool Administrator Printed Name

04/24/2024

Date

Markus Hohenwarter

Representative Signature

Markus Hohenwarter

Representative Printed Name

04/24/2024

Date

GeoGebra Data Privacy and Security Plan

It's important to remember that students **do not need to register** or sign in to the GeoGebra Website in order to use the GeoGebra software, access millions of GeoGebra resources or participate in a real-time collaboration in a GeoGebra Classroom.

Protecting the privacy of **young children** is especially important. If GeoGebra learns that personally identifiable information of children has been collected on the Website without parental consent, then GeoGebra will take the appropriate steps to delete this information. If you are a parent or legal guardian and discover that your child has a registered account with the Website without your consent, then you may alert GeoGebra at office@geogebra.org and request that GeoGebra delete that child's personal information from its systems.

GeoGebra **never shares** personal information of any user with **third parties**.
A parent or a legal guardian of a student under 18, can **inspect and edit** at any time the data associated with the student's account by visiting the account settings page.

GeoGebra uses certain physical, managerial, and technical **safeguards** designed to preserve the integrity and security of users' personal information.

- Physical security:
  - Access control: access for employees to data is password protected
  - Individuals are required to sign in/out for installation and removal of equipment
  - Data is hosted on Amazon Web Services (AWS). Backups for the servers, on which the data resides, are provided by Amazon RDS automated backups (https://aws.amazon.com/rds/details/backup/). The physical security for AWS is managed by Amazon RDS.

- Technical security:
  - Our system employs encryption technologies when transmitting sensitive information (SSL/TLS, VPN) over the network.
  - If users have a GeoGebra account, passwords are encrypted by PHP's crypt function, using the Blowfish algorithm with a 16-character salt value.
  - We are utilizing a web application firewall (WAF) (managed by Amazon VPC)

- Organizational security:
  - Only GeoGebra employees have access to AWS and the used services. Access is password secured.
  - Remote Access: GeoGebra employees can work remotely, but only via VPN.
  - As part of GeoGebra's hiring process, the background and CV of our employees is checked.

All GeoGebra employees, with legitimate access to PII, receive twice a year **updates regarding best privacy and security practices.** This also include updates on the following laws:

- General Data Protection Regulation (“GDPR”)
- Family Educational Rights and Privacy Act ("FERPA")
- Children's Online Privacy Protection Act ("COPPA")
- New York Education Law Section 2-d

If you become aware of a **data breach** please notify GeoGebra by writing an email to office@geogebra.org. We will try to remediate the issues as soon as possible. In case GeoGebra becomes aware of a data or security breach, it will either notify the educational institution with whom we have privacy agreements in place or the user directly and try to fix the issues as soon as possible.

GeoGebra is an international company with headquarters in Austria, Europe. For hosting our web applications and data we use AWS (Amazon Web Services). All our data (including user data) is stored in secure data centers within the European Union, mostly Ireland. We do not transfer any data outside the European Union. AWS, our **subcontractor,** has one of the highest privacy and security standards in place. It is compliant with GDPR, FERPA, NIST, ISO/IEC 27001:2013, etc.

Each user can view/edit his/her personal information on the account settings page. On the same page students can also permanently **delete their account**. GeoGebra keeps a copy of deletion for one year.

Upon **expiration or termination** of a privacy agreement with an educational institution, nothing happens by default with the students data. The educational institution can write us an email at office@geogebra.org to either transfer student data back and/or permanently remove it from our systems.

For further information please visit our Privacy Policy and Terms of Service.