LIVERPOOL CENTRAL SCHOOL DISTRICT
Preparing our Students for Tomorrow... Today

DATA SECURITY AND PRIVACY PLAN

WHEREAS, the Liverpool Central School District (hereinafter "School District") and MajorClarity, Inc. (hereinafter "Contractor") entered into an agreement dated 5/12/22 (hereinafter "Agreement") for Career and College Exploration Platform (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):

MajorClarity is compliant with FERPA. MajorClarity does not sell data and is a member of the Student Privacy Pledge. Data will only be used for the purposes covered by the subscription agreement for software and services. Industry standard data security practices are in place as described below. MajorClarity does not retain district data after termination of an agreement. MajorClarity's privacy policy can be found here: https://majorclarity.com/privacy-policy

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:

Accounts and authentication: Secure authentication and passwords, password hashing, forced log-outs, log-in attempt limits, role-based permissions
Data Security and Infrastructure: Data encrypted at rest and in transit, SFTP with 256- bit SSL encryption, IP whitelisting, Data access by MajorClarity only permitted on secured and encrypted company devices, Hosting via Amazon Web Services (AWS) highly secure and redundant environment, regular penetration testing and AWS security testing, code audits, automated testing, and full SDLC process

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 MajorClarity employees who require access to student or educator data are trained on data security and privacy at the time of onboarding, and also receive training annually.

5. Subcontractors (check one):

☑ Contractor shall not utilize subcontractors.

☐ 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:

MajorClarity does not use subcontractors. Any leased or other non-W2 employees are subject to the same committments and requirements for data privacy and security.

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.

In the event of a data breach, MajorClarity will notify the school district within 48 hours. Per MajorClarity's data breach policy, MajorClarity's COO is responsible for the investigation of the breach, including assessing risk and scope, and ensuring communication with any affected district.

7. Termination of Agreement.

a. Within 45 days of termination of the Agreement, Contractor shall delete or destroy all student data or teacher or principal data in its possession; AND

b. ☑ Within 45 days of termination of the Agreement, Contractor shall Return all data to the School District using csv export; 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 5/12/22.

CONTRACTOR:

By: DocuSigned by: Lauren Conroy 0D103E007678418...
Title: Lauren Conroy
COO

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;

   To provide software and services for the Career and College Exploration and Planning platform.

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);

   All MajorClarity employees who require access to student or educator data are trained on data security and privacy at the time of onboarding, and also receive training annually.

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);

   The contract begins on 7/1/22, and ends on 6/30/23. If the contract is not renewed, upon termination the student and educator data will be retrieved by the district via export within 45 days. After this time data will be destroyed from within MajorClarity systems.

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;

   All data that is collected is provided either directly from the district SIS or by input from an educator, parent, or student. If there is an issue, the data should be corrected via those sources first. If an issue remains, MajorClarity will review the issue and provide recommended solutions.

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 Data is stored on AWS servers located in the US. Security includes:

   Secure authentication and passwords, password hashing in the database, forced log-outs and log-in attempt limits, role-based permissions, physical device security and encryptions, regular penetration testing, AWS security testing, code audits, automated testing

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

   Data encrypted at rest and in transit, SFTP with 256- bit SSL encryption

_____	DocuSigned by: Lauren Conroy 0D103E007678418...
Liverpool Administrator Signature	Representative Signature
_____	Lauren Conroy
Liverpool Administrator Printed Name	Representative Printed Name
_____	5/12/2022
Date	Date