LIBERTY CENTRAL SCHOOL DISTRICT
DISTRICT OFFICE
Stacy Feasel
District Data Coordinator and Privacy Officer

Data Processing Addendum

This Data Processing Addendum ("***Addendum***") is entered into by the Liberty Central School District (the "***District***") and Aperture Education, LLC ("***Contractor***") as of 9/6/2024 (the "***Effective Date***").

WHEREAS, the District is committed to protecting the security and privacy of personally identifiable information ("***PII***") in accordance with all applicable state and federal laws, including but not limited to the Family Educational Rights and Privacy Act ("***FERPA***") and New York State Education Law § 2-d; and

WHEREAS, Contractor has entered into an agreement (the "***Underlying Agreement***" with the District pursuant to which the Contractor may receive PII, including PII of students, teachers and/or principals;

NOW, THEREFORE, the Parties agree as follows:

1. Definitions. All capitalized terms not otherwise defined herein shall have the same definition as used in New York State Education Law § 2-d and/or 8 NYCRR Part 121.

2. Parents Bill of Rights. The District's Parents' Bill of Rights for Data Privacy and Security ("***Parents Bill of Rights***") is attached as Exhibit A and shall be deemed to be expressly appended to and included with the Underlying Agreement.

3. Contractor Responsibilities.

a. Contractor agrees that PII, including Student Data and Teacher or Principal Data, shall be maintained confidentially and in accordance with federal and state law and the District's data security and privacy policies.

b. Contractor may not sell, use or disclose PII for any marketing or commercial purpose or permit another person to do so.

c. Supplemental information concerning Contractor's handling of Student Data and/or Teacher or Principal Data is set forth as Exhibit A-1 to the Parents Bill of Rights.

d. Contractor shall maintain a data security and privacy plan that complies with the District's data security and privacy policies, as well as all legal requirements, including but not limited to the specific requirements set forth in NY Education Law §2-d, 8 NYCRR Part 121, and the National Institute of Standards and Technology ("***NIST***") Cybersecurity Framework. At a minimum, Contractor shall:

i. limit access to PII to only those employees or subcontractors that need access to perform Contractor's obligations under the Underlying Agreement;

ii. not use PII for any purpose not authorized under the Underlying Agreement;

iii. not disclose PII to any person without the prior written consent of the parent or Eligible Student, except to the extent such disclosure is made:

1. to an authorized subcontractor for a purpose necessary to fulfill the Contractor's obligations under the Underlying Agreement; or

2. as required under applicable law;

iv. maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII received pursuant to the Underlying Agreement; and

v. use encryption to protect PII while in motion or at rest.

e. If Contractor uses a third party to perform any of Contractor's obligations under the Underlying Agreement, Contractor shall ensure that the third party complies with all obligations of the Contractor under this Section 3.

4. Breach Notification. Unless otherwise expressly required by law, Contractor agrees to:

a. notify the District promptly, but in no event later than forty-eight (48) hours, after discovery of any data breach or other security incident (collectively, a "***Security Incident***") that is reasonably believed to affect the confidentiality, integrity and/or security of PII, including but not limited to the unauthorized access to or disclosure of such PII;

b. provide the District promptly, but in no event later than five (5) business days, after the notice described in Section 4(a) with a report concerning the known or suspected cause of the Security Incident, the information affected, the steps taken by the Contractor to stop and/or mitigate the Security Incident, and any other information reasonably requested by the District or law enforcement authorities to respond to and/or otherwise recover from the Security Incident; and

c. comply with all other applicable breach notification requirements, including but not limited to those in NY Education Law § 2-d(6) and 8 NYCRR § 121.10.

5. Changes in Applicable Law. PII, including Student Data and Teacher or Principal Data, is subject to rapidly changing laws and regulations. Contractor agrees to work in good faith to execute and implement any additional documents, policies and/or procedures reasonably necessary to comply with any change in applicable law or regulation within thirty (30) days of a request by the District.

6. Termination of Underlying Agreement. Notwithstanding any other provision of the Underlying Agreement, the District may terminate the Underlying Agreement without penalty if (a) Contractor fails and/or refuses to comply with its obligations under this Addendum or (b) the parties are unable to reach agreement on an amendment to this Addendum required by changes in applicable law. At the District's written request, whether upon termination or at any other time, Contractor shall return, de-identify and/or delete all PII in its possession, custody or control. Notwithstanding the foregoing, Contractor shall be entitled to retain (a) archive copies required to be retained (i) by law, (ii) as part of Contractor's business record-keeping (such as without limitation for dispute resolution such as to establish or defend against claims) or (iii) for compliance purposes (such as without limitation audit, tax, privacy or other compliance requirements) or (b) back-up or log files that are not accessible in the ordinary course and deleted on a standard schedule (other than ad hoc back-ups that are deleted outside standard retention windows).

7. Interpretation. In the event of a conflict between the terms of this Addendum (including the attached Parents Bill of Rights) and the Underlying Agreement, the terms of this Addendum and the Parents Bill of Rights shall control notwithstanding any language in the Underlying Agreement to the contrary.

8. Counterparts. This Addendum may be executed in counterparts, each of which shall be deemed an original. Each counterpart may be executed and/or exchanged by electronic means.

IN WITNESS WHEREOF, the Parties agree to be bound by the terms of this Addendum as of the Effective Date:

Liberty Central School District:

By: Stacy Feasel

Signature: Stacy Feasel

Title: District Privacy Officer

Date: 9/6/24

Contractor: Aperture Education, LLC

By: Scott E. Olson

Signature: Scott E. Olson

Title: Funding and Proposal Manager

Date: 9/17/24

Exhibit A

Liberty Central School District

Parents Bill of Rights for Data Privacy and Security

The Liberty Central School District, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. The Liberty Central District establishes the following parental bill of rights:

- Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.

- The district and its schools, and third-party contractors and subcontractors, will not sell student PII or use or disclose it for any marketing or commercial purposes or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so;

- Parents have the right to inspect and review the complete contents of their child's education record (for more information about how to exercise this right, see 5500-R);

- State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. 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;

- A complete list of all student data elements collected by the State Education Department is available for public review at http://nysed.gov/data-privacy-security/student-data-inventory or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234

- Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to the District Security and Privacy Officer, the Assistant Superintendent at 845-292-6171 by mail to 115 Buckley Street, Liberty NY 12754 or by email to tdefrank@libertyk12.org. Complaints can also be directed to the New York State Education Department online at http://nysed.gov/data-privacy-security/report-improper-disclosure, by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to privacy@nysed.gov or by telephone at 518-474-0937.

- Parents have the right to be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.

- All district and school employees and officers with access to PII will receive annual training on applicable federal and state laws, regulations, district and school policies and safeguards which will be in alignment with industry standards and best practices to protect PII.

- In the event that the district engages a third party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting (Complaints should be directed to the District Security and Privacy Officer, the Assistant Superintendent at 845-292-6171 by mail to 115 Buckley Street, Liberty NY 12754 or by email to tdefrank@libertyk12.org or can access the information on the district's website www.libertyk12.org

Exhibit A-1

Liberty Central School District

Supplemental Information Relating to Underlying Agreement

Pursuant to New York Education Law §2-d(c) and 8 NYCRR § 121.3(c), the following additional information is provided with respect to processing of Student Data and/or Teacher or Principal Data for the Underlying Agreement between the District and Contractor:

(1) The exclusive purposes for which the Student Data or Teacher or Principal Data will be used are **described here**:

DESSA Comprehensive Social and Emotional Learning Assessment System, an online platform used for measuring student social and emotional competence and which includes resources for teaching social and emotional skills.

(2) Contractor will ensure that the subcontractors, persons or entities that Contractor will share the Student Data or Teacher or Principal Data with, if any, will abide by data protection and security requirements by **methods described in the attached DATA SECURITY AND PRIVACY PLAN.**

(3) The Underlying Agreement expires as set forth in the applicable ordering document. Upon expiration of the Underlying Agreement, and upon written request from the District, Student Data, Teacher or Principal Data will be deleted, and a certification of deletion will be provided to the District upon written request.

(4) A parent, eligible student, teacher or principal may challenge the accuracy of the Student Data or Teacher or Principal Data that is collected by contacting the District's Data Protection Officer.

(5) Student Data or Teacher or Principal Data will be stored **at the location described here**: : in United States based Microsoft Azure data centers that maintain their own rigorous industry standard certifications and compliance offerings.

(6) Contractor will use the security protections **described in the attached Application Security in Brief for the Aperture SEL System.**

(7) Data will be protected using encryption while in motion and at rest.

DATA SECURITY AND PRIVACY PLAN

Last Updated 6/8/2020

This Data Security and Privacy Plan (this "Plan") has been implemented and will be maintained by APERTURE in compliance with all applicable laws, including the New York Education Law §2-d and regulations promulgated thereunder.

APERTURE will undertake industry standard practices, including physical controls, firewalls, and password protection, to protect the privacy and security of Client Data received under this Agreement, including compliance with the requirements of National Institute for Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. Physical controls include change control, physical access controls that prevent removal of Client Data from the production data center, physical security controls, and a hardware destruction process that follows NIST SP 800-88.

APERTURE shall inform Client in the event that any student data ("**Student Data**") it stores or maintains pursuant to this Agreement, including such data as may be stored or maintained by a third party cloud provider on APERTURE's behalf, is requested by law enforcement authorities or otherwise sought by subpoena or court order.

APERTURE will keep confidential all Student Data to which it has access in the performance of this Agreement.

In addition to the above requirements, for Student Data:

1) APERTURE shall maintain the confidentiality of the Student Data in accordance with applicable state and federal law.

2) APERTURE shall implement all state, federal and local data security and privacy contract requirements during the term of this Agreement, as follows:

   APERTURE has designated a privacy officer responsible for information security governance and maintains privacy policies and practices that support compliance with FERPA. Client Data will be housed in United States based Microsoft Azure data centers that maintain their own rigorous industry standard certifications and compliance offerings.

3) APERTURE's data security and privacy Plan includes the Parents Bill of Rights for data privacy and security (a copy of which is attached hereto and incorporated into this Agreement**).**

4) APERTURE agrees that any of its officers or employees, and any officers or employees of any subcontractor or assignee of APERTURE, who will have access to Student Data, have received or will receive training on the federal and state law governing confidentiality of such data prior to receiving the data or access to the data.

5) The exclusive purposes for which APERTURE is being provided access to the Client Data is:

   Providing products and services related to the hosting of Client Data.

6) APERTURE will ensure that it will only share Client Data with additional third parties if those third parties are contractually bound to observe equally stringent obligations to maintain data privacy and security as required by APERTURE pursuant to this Plan.

7) In the event that a parent or eligible student wishes to challenge the accuracy of any Student Data that is maintained by APERTURE, that challenge may be processed through the procedures provided by Client for amendment of education records under the Family Educational Rights and Privacy Act (FERPA). APERTURE will be notified by Client of the outcome of any such challenges and immediately correct any inaccurate data it or its subcontractors or assignees maintain.

8) APERTURE acknowledges that it has the following additional obligations under NYS Education Law 2-d with respect to any Student Data received from Client, and agrees that any failure to fulfill one or more of these statutory obligations shall be deemed a breach of this Agreement, as well as subject APERTURE to various penalties under Section 2-d, including but not limited to civil penalties:

   a. To limit internal access to education records and Student Data to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and FERPA; e.g., the individual needs access to the Student Data in order to fulfill his or her responsibilities in performing the Services;

   b. To not use education records or Student Data for any purpose(s) other than those explicitly authorized in this Agreement;

   c. To not disclose any personally identifiable information to any other party who is not an authorized representative of APERTURE using the information to carry out APERTURE's obligations under this Agreement, unless:

      i. the parent or eligible student has provided prior written consent, or
      ii. the disclosure is required by statute or court order, and notice of the disclosure is provided to Client prior to the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

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

   e. To use encryption technology and other suitable means to protect data while in its custody while in motion or at rest.

   f. To notify Client of any breach of security resulting in an unauthorized release of such data by APERTURE or its subcontractors or assignees in violation of applicable state or federal law, the Parents Bill of Rights for student data privacy and security, and obligations relating to data privacy and security within this Agreement in the most expedient way possible and without unreasonable delay.

   g. To return, delete or destroy Client Data when this Agreement terminates or expires as specified in this Agreement and/or APERTURE's privacy policy.

9) The parties acknowledge that an Addendum to this Agreement may be necessary to ensure compliance with Section 2-d following the promulgation of applicable regulations and/or the issuance of further guidance by the New York State Education Department subsequent to the execution of the Agreement. The parties agree to act in good faith to take such additional steps to amend this Agreement as may be necessary at that time.

APERTURE EDUCATION

BRINGING THE WHOLE CHILD INTO FOCUS

APERTURE EDUCATION
BRINGING THE WHOLE CHILD INTO FOCUS

Purpose

The purpose of this document is to provide insight into the security posture of the Aperture System. This document is not intended to be an exhaustive representation of all attributes of Information Security and Privacy at Aperture Education but provide a general understanding of the awareness, strategies, design decisions, and other ingredients that comprise boundaries of Information Security.

APERTURE EDUCATION
BRINGING THE WHOLE CHILD INTO FOCUS

Approach

The Aperture Education security approach is fundamentally implemented by utilizing a top tier vendor for hosting our cloud-based solutions. The application, its data, and supporting infrastructure reside in a segregated environment to ensure flexibility in responding to customer needs without having to weigh unrelated enterprise needs. Aperture Education takes seriously its obligation to protect customer assets by conforming to the best available standards for infrastructure, data governance, architecture and design practices, and quality assurance practices.

Aperture's Education's Aperture System is hosted in the Google Cloud Platform. The data centers are geographically dispersed throughout the United States and comply with key industry standards for security, reliability, and availability.

The data center's infrastructure undergoes exhaustive third-party auditing to ensure continued compliance to the most stringent policies, procedures, standards, and regulatory requirements across a broad scope of industries. Third party systems or services integrated with Aperture Education's core cloud infrastructure are also subject to the same audit and baseline guidelines of the security policies.

Google employs an extremely high standard of security at its data centers. As a leader in the cloud infrastructure industry, Google has adopted many stringent security methods to ensure compliance for its customers, such as:

- Data redundancy to ensure high availability, disaster recovery, business continuity, and reliability and consistency of customer data.
- Physical access to all assets are secured and restricted to only authorized personnel
- Data center facilities are continually monitored and constrained to only authorized employees.
- Advanced fire suppression systems
- Redundant environmental controls
- A redundant uninterruptable power supply with diesel generators is employed at all data center facilities.

To leverage this infrastructure to its fullest, the Aperture Education cloud development team operates separate from the internal corporate intranet. This allows Aperture Education to quickly respond to the rapidly changing security landscape and fully leverage all that the Google cloud environment has to offer in terms of security. Aperture integrates with this environment by employing infrastructure segregation and other security practices, such as:

- Continuous and consistent data backups to a disparate data repository, maintained for a 30-day window
- Clients' personally identifiable data is automatically de-identified after 90 days of subscription expiration
- All staff are trained and bound to policies and procedures for secure handling of sensitive data
- Security controls are individually managed on each environment including code delivery, code storage, data storage, data access
    - Production data is never replicated or used outside of our production environment

Aperture Education employs industry best-practice Information Security Policies for handling, storing, and disposing of sensitive data, including but not limited to:

- Strong password policy
- Encrypted hard drives for employees who are likely to encounter Client's personally identifiable data
- Application vulnerability and penetration testing done at least biannually and more frequently as required
- 24/7/365 Application Intrusion Detection and Threat Detection management
- PCs are continually scanned for malware and anti-virus software is run continually and updated at a minimum of 12-hour intervals.
- Employees (full time and contractors) are subject to federal background checks and federal sex offender registry checks and are contractually responsible to comply with all Aperture Education security policies and procedures. Employees who leave the Aperture Education development team have security access de-provisioned in a timely manner.
- Created and maintains a data disposition process with accompanying documentation

APERTURE EDUCATION
BRINGING THE WHOLE CHILD INTO FOCUS

Continual Improvement

Aperture Education's commitment to security means that we keep tabs on news threats as they emerge in the industry.

- Aperture Education maintains an ongoing review of industry alerts, with a goal to implement / modify practices based on new knowledge
- Aperture Education maintains a strong relationship with our customer's needs for security and gives high priority to any specific security needs a customer may request
- Aperture Education monitors industry security trends and can mitigate emerging security threats
- Patch and vulnerability updates are applied using a risk-based approach to maintain business continuity and minimal disruption
- A program for monitoring critical systems and notifying appropriate personnel is employed
- Policies and procedures are updated based on emerging risks and vulnerabilities
- Quality assurance is performed using automated and manual testing for all deployments. Regression testing is performed for all application functionality to verify all established security measures are met

APERTURE EDUCATION
BRINGING THE WHOLE CHILD INTO FOCUS

Assessments

Aperture Education's Aperture System is subjected to third party risk assessment as well as penetration and security testing on at least an annual basis. The following list contains

the testing parameters and general security aspects of the application that are employed, measured, and verified by a third party:

- Application requires authentication for access to data
- Access to application is through individually identifiable means (no shared logins)
- Application utilizes PKI, and a public, well-trusted Certificate Authority
- Administrative logins to application are required to have strong passwords
- Application user IDs are unique
- Every login is tied to a real, specific human; no shared logins
- Data center infrastructure has been evaluated against ISO 27001
- Data center infrastructure has undergone an SAS 70 Type II or SSAE 16 review
- Evaluation against NIST SP 800-53
- OWASP or OSSTMM guidelines/methodology
- Application supports role-based access
- The application process runs only with privileges necessary for proper operation (for example, root or administrator privileges are only used for specific required operations, while in normal mode the application runs as a user without administrative privileges)
- A data backup/restore plan exists for this application
- Secure Software Development Life Cycle (SSDLC) in place that includes peer code review and developer security training
- A code promotion/release management strategy is in place (if applicable)
- One designated accountable party (e.g., Information Security Officer) responsible for all aspects of information security about this service/application
- Vendor has a documented Information Security Management Program
- Vendor has technology capable of and agrees to cooperate with forensic imaging requests in the event of a security incident
- Vendor regularly monitors vulnerabilities in underlying products (e.g., GCP, databases) and patches all critical vulnerabilities within 30 days
- Vendor monitors 3rd party consultants/contractors' access to vendors data and requires an NDA (nondisclosure agreement) where applicable
- Service Level Agreement
- Assessed Element
- Vendor has Service Level Agreement that sets expected availability targets and penalties for noncompliance.
- Vendor has Service Level Agreement that includes targets for initial response time to reports of breach of confidentiality or integrity and penalties for noncompliance.

APERTURE EDUCATION
BRINGING THE WHOLE CHILD INTO FOCUS

Data Protection

The following Data Protection elements are employed and verified by a third party:

- Sensitive application data (including student or employee data and any PII or PHI) is encrypted at rest.
- Sensitive application data (including student or employee data and any PII or PHI) is encrypted in transit.
- User credentials are encrypted at rest.
- User credentials are encrypted in transit.
- Encryption keys are never stored in cleartext such as in configuration files.
- Cryptographic modules are FIPS-140-compliant using the National Institute of Standards and Technology's FIPS 140-1 and FIPS 140-2
- Database and other application interface credentials are encrypted at rest.
- Database and other application interface credentials are encrypted in transit.
- Connection to database is encrypted.
- Database tables/fields are protected using FIPS-140-compliant encryption for all tables/fields containing sensitive data.

Audits

The following audit protections and mechanisms are employed and verified by a third party:

- Application logs security-relevant events. Each log entry must contain, at minimum:
    - User or process ID of user or process causing the event
    - Success or Failure of attempt to access security file
    - Date/time of event
    - Type of event
    - Success or Failure of event
    - Seriousness of event violation Examples of log entries:
    - Success or Failure of login attempt
- Denial of access resulting from excessive number of login attempts
- Blocking or blacklisting of user ID, terminal, or access port, and reason for the action
- Activities that might modify, bypass, or negate security safeguards controlled by the application
- Application logs all access to student or employee data and any PII or PHI in an individually identifiable way.
- Application server is time-synchronized to a known source (e.g., NTP, NIST).
- A process exists to ensure that application log files are retained for at least one year.

APERTURE EDUCATION
BRINGING THE WHOLE CHILD INTO FOCUS

Application Network Architecture, Configuration and Authorization

The following Application Network Architecture, Configuration, and Authorization mechanisms are employed by the application and verified by a third party:

- Application/system uses secure protocols for administration (e.g., SSH, encrypted RDP) and not Telnet or unencrypted PCA/RDP/VNC
- Application/system uses secure protocols for file/data transfer (e.g., SSL, SCP) and not FTP, CIFS, etc.
- Application users can explicitly terminate a session (logout)
- The application validates user inputs before processing them