

DATA PRIVACY AND SECURITY AGREEMENT

WHEREAS, Discovery Education, Inc., having its principal offices at 4350 Congress Street, Suite 700, Charlotte, North Carolina 28209 (hereinafter “Contractor” or “Discovery”) and the Board of Cooperative Educational Services, Second Supervisory District of Erie, Chautauqua and Cattaraugus Counties, having its offices at 8685 Erie Road, Angola, New York 14006 (hereinafter “E2CCB”), collectively “the Parties,” are parties to an agreement, also referenced herein as the “BOCES Purchase Contract” and attached hereto as Exhibit 2, through which Contractor will provide E2CCB and educational agencies with whom it contracts with access to Discovery Education Streaming Services and related resources; and

WHEREAS, pursuant to that agreement, Contractor will receive student data and/or teacher or principal data in possession of E2CCB and/or its officers, employees, agents, and students, and may also receive student data and/or teacher or principal data of educational agencies within New York State that contract with E2CCB for the use of Contractor’s products and/or services; and

WHEREAS, the Parties enter into this Data Privacy and Security Agreement (hereinafter the “Agreement”) to address the confidentiality and security of student data and/or teacher or principal data received by Contractor, and in conformance with N.Y. Education Law § 2-d and 8 N.Y.C.R.R. § 121.1, *et seq.*

NOW, THEREFORE, the Parties mutually agree as follows:

1. For purposes of this Agreement, terms shall be defined as follows:
 - a. “Breach” means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.
 - b. “Commercial Purpose” or “Marketing Purpose” means the sale of student data; or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly; the use of student data for advertising purposes, or to develop, improve or market products or services to students.
 - c. “Disclose” or “Disclosure” means to permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written, or electronic, whether intended or unintended.
 - d. “Education Records” means an education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
 - e. “Eligible Student” means a student who is eighteen years or older.
 - f. “Encryption” means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of

a technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

- g. "Parent" means a parent, legal guardian, or person in parental relation to a student.
 - h. "Personally Identifiable Information," or "PII" as applied to student data, means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and as applied to teacher and principal data, means personally identifiable information as such term is defined in N.Y. Education Law §3012-c (10).
 - i. "Release" shall have the same meaning as Disclosure or Disclose.
 - j. "Student" means any person attending or seeking to enroll in an educational agency.
 - k. "Student data" means personally identifiable information from the student records of an educational agency. For purposes of this agreement, "student data" includes information made accessible to Contractor by E2CCB, E2CCB officers, E2CCB employees, E2CCB agents, E2CCB students, and/or the officers, employees, agents, and/or students of educational agencies with whom E2CCB contracts.
 - l. "Teacher or principal data" means personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of N.Y. Education Law §§ 3012-c and 3012-d. For purposes of this agreement, "teacher or principal data" includes information made accessible to Contractor by E2CCB, E2CCB officers, E2CCB employees, E2CCB agents, E2CCB students, and/or the officers, employees, agents, and/or students of educational agencies with whom E2CCB contracts.
 - m. "Unauthorized Disclosure" or "Unauthorized Release" means any disclosure or release not permitted by federal or State statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.
2. Contractor agrees that the security, confidentiality, and integrity of student data and/or teacher or principal data shall be maintained in accordance with:
- a. Applicable state and federal laws that protect the confidentiality of personally identifiable information;
 - b. The terms and conditions of this Agreement, including but not limited to the E2CCB Parents Bill of Rights for Data Security and Privacy and the Supplemental

Information to Parents Bill of Rights for Data Privacy and Security, attached hereto as Attachment 1; and

- c. Applicable E2CCB policies, which can be accessed on the E2CCB website at: <https://go.boarddocs.com/ny/e2ccb/Board.nsf/Public>.

3. Contractor will ensure that its personnel and subcontractors that access the student data are informed of the confidential nature of the student data they receive and that they are bound by applicable statutory and/or contractual obligations of confidentiality, as set forth in the Contractor's Student Data Protection Addendum, located at <https://www.discoveryeducation.com/data-protection-addendum/>. Contractor will take all reasonable steps and to ensure the reliability of Contractor personnel and subcontractors that access student data.

4. Contractor agrees that it will disclose student data and/or teacher or principal data only to those officers, employees, agents, subcontractors, and/or assignees who need access to provide the contracted services. Contractor further agrees that any of its officers or employees, and any officers or employees of any assignee or subcontractor of Contractor, who have access to personally identifiable information will receive training on the federal and state laws governing confidentiality of such data prior to receiving access to that data. Employees (including temporary and contract employees) of Contractor are educated and trained on the proper uses and disclosures of PII and the importance of information privacy and security. All Contractor's employees are aware of and work to protect the confidentiality, privacy, and security of PII. Contractor, and its respective personnel do not access PII except to comply with a legal obligation under federal or state law, regulation, subpoena, or if there is legitimate need for the information to maintain data systems or to perform required services under the BOCES Purchase Contract.

5. Contractor will examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point, to the Contractor's knowledge, a subcontractor fails to materially comply with the requirements of this Agreement, Contractor will: notify E2CCB and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor will follow the Data Breach reporting requirements set forth herein.

6. Contractor is being provided access to personally identifiable information for the sole and exclusive purpose of carrying out the services for which E2CCB has contracted.

7. Student data and/or teacher or principal data received by Contractor, or by any subcontractor or assignee of Contractor, shall not be sold or used for commercial purposes or marketing purposes.

8. The agreement between Contractor and E2CCB for Discovery Education Streaming Services and any related services and/or resources expires on June 30, 2025. Upon expiration of that agreement without a successor agreement in place, Contractor shall thereafter securely delete or otherwise destroy any and all student data and/or teacher or principal data remaining in the possession of Contractor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of such data) as well as any and all student data and/or teacher or principal data maintained on behalf of Contractor in secure data

center facilities. Contractor shall ensure that no copy, summary, or extract of the student data and/or teacher or principal data or any related work papers are retained on any storage medium whatsoever by Contractor, its subcontractors or assignees, or the aforementioned secure data center facilities. Any and all measures related to the deletion, or destruction of student data and/or teacher or principal data will be completed within 60 days of the expiration of the agreement between E2CCB and Contractor, and will be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. To the extent that Contractor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (*i.e.*, data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party. Upon request, Contractor and/or its subcontractors or assignees will provide a certification to E2CCB from an appropriate officer that the requirements of this paragraph have been satisfied in full.

9. In the event that a parent, student, or eligible student wishes to challenge the accuracy of student data concerning that student or eligible student, that challenge shall be processed through the procedures provided by E2CCB or the educational agency that generated the student data for amendment of education records under the Family Educational Rights and Privacy Act (FERPA). In the event that a teacher or principal wishes to challenge the accuracy of the teacher or principal data that is collected, he or she may do so consistent with applicable provisions of 8 N.Y.C.R.R. Part 30 and the applicable educational agency's Annual Professional Performance Review Plan.

10. Student data and/or teacher or principal data transferred to Contractor will be stored in electronic format on systems maintained by Contractor in a secure data center facility located in the United States. In order to protect the privacy and security of student data and/or teacher or principal data stored in that manner, Contractor will take measures aligned with industry best practices and the NIST Cybersecurity Framework Version 1.1 (as acknowledged in Attachment 2). Such measures will include, but are not necessarily be limited to disk encryption, file encryption, firewalls, and password protection.

More specifically, Contractor implements security measures based on the level of risks, capabilities, and operating requirements. These measures include, as appropriate and reasonable, the following safeguards:

- a. Administrative Safeguards:
 - i. Sanctions: Appropriate sanctions against Contractor personnel who fail to comply with Contractor's security policies and procedures.
 - ii. System Monitoring: Procedures to regularly review records of information systems activity, including maintaining access logs, access reports, security incident tracking reports, and periodic access audits.
 - iii. Security Oversight: Assignment of one or more appropriate management-level employees of Contractor to be responsible for developing, implementing, and monitoring of safeguards and security issues.
 - iv. Appropriate Access: Procedures to determine that the access of Contractor personnel to PII is appropriate and meets a legitimate need to support their roles in business or educational operations. Procedures for establishing appropriate authorization and authentication mechanisms for Contractor personnel who have access to PII.
 - v. Employee Supervision: Procedures for regularly monitoring and

- supervising personnel who have access to PII.
 - vi. Access Termination: Procedures for terminating access to PII when employment ends, or when an individual no longer has a legitimate need for access.
- b. Operational Safeguards
 - i. Access to PII: Procedures that grant access to PII by establishing, documenting, reviewing, and modifying a user's right of access to a workstation, software application/transaction, or process.
 - ii. Awareness Training: On-going security awareness through training or other means that provide Contractor personnel (including management) with updates to security procedures and policies (including guarding against, detecting, and reporting malicious software). Awareness training also addresses procedures for monitoring log-in attempts and reporting discrepancies, as well as procedures for safeguarding passwords.
 - iii. Incident Response Plan: Procedures for responding to, documenting, and mitigating where practicable suspected or known incidents involving a possible breach of security and their outcomes.
 - iv. Physical Access: Procedures to limit physical access to PII and the facility or facilities in which they are housed while ensuring that properly authorized access is allowed, including physical barriers that require electronic control validation (e.g., card access systems) or validation by human security personnel.
 - v. Physical Identification Validation: Access is physically safeguarded to prevent tampering and theft, including procedures to address control and validation of a person's access to facilities based on his or her need for access to the PII.
 - vi. Operational Environment: Procedures that specify the proper functions to be performed, the manner in which they are to be performed.
 - vii. Media Movement: Procedures that govern the receipt and removal of hardware and electronic media that contain PII into and out of a facility.
- c. Technical Safeguards
 - i. Data Transmissions: Technical safeguards, including encryption, to ensure PII transmitted over an electronic communications network is not accessed by unauthorized persons or groups.
 - ii. Data Integrity: Procedures that protect PII maintained by Discovery from improper alteration or destruction. These procedures include mechanisms to authenticate records and corroborate that they have not been altered or destroyed in an unauthorized manner.
 - iii. Logging off Inactive Users: Inactive electronic sessions are designed to terminate automatically after a specified period of time.

The Parties agree and acknowledge that Contractor may modify its administrative, operational, and/or technical safeguards, provided that any such changes will not conflict with applicable law, rule, regulation, or local policy, and that such changes will not be less protective of PII than the measures set forth above. Contractor will notify E2CCB in writing of any material changes to its administrative, operational, and/or technical safeguards within 30 days of such changes.

11. Contractor acknowledges that it has the following obligations with respect to any student data and/or teacher or principal data provided pursuant to its agreement with E2CCB, and any failure to fulfill one of these obligations set forth in New York State Education Law § 2-d and/or 8 N.Y.C.R.R. Part 121 shall also constitute a breach of its agreement with E2CCB:

- a. Limit internal access to education records to those individuals that are determined to have legitimate educational reasons within the meaning of § 2-d and the Family Educational Rights and Privacy Act;
- b. Not use education records/and or student data for any purpose other than those explicitly authorized in this Agreement;
- c. Not disclose any personally identifiable information to any other party who is not an authorized representative of Contractor using the information to carry out Contractor's obligations under this Agreement, unless (i) that other party has the prior written consent of the parent or eligible student, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to the source of the information no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;
- d. Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable information in its custody;
- e. 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);
- f. Notify E2CCB of any breach of security resulting in an unauthorized release of student data by Contractor 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 not more than seven (7) calendar days after discovery of the breach;
- g. Where a breach or unauthorized release of personally identifiable information is attributable to Contractor, Contractor will pay or reimburse E2CCB and/or any educational agencies which contract with E2CCB for the provision of Contractor's products or services for the cost of any notifications E2CCB and/or such other educational agencies is/are required to make by applicable law, rule, or regulation; and
- h. Contractor will cooperate with E2CCB and law enforcement to protect the

integrity of investigations into the breach or unauthorized release of personally identifiable information.

- i. In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on Contractor by state and federal law, and by this Agreement, shall apply to the subcontractor.

12. In combination with periodic security risk assessments, Contractor uses a variety of approaches and technologies to make sure that risks and incidents are appropriately detected, assessed and mitigated on an ongoing basis. Contractor also assesses on an ongoing basis whether controls are effective and perform as intended, including intrusion monitoring and data loss prevention. In the event of a data security and/or privacy incident (including but not limited to a breach, unauthorized release, and/or unauthorized disclosure) implicating the personally identifiable information of students, teachers, and/or principals of E2CCB or educational agencies which contract with E2CCB for the provision of Contractor's products or services, Contractor will act in accordance with the following:

- a. Contractor maintains and updates incident response plans that establish procedures in the event a breach occurs. Contractor also identifies individuals responsible for implementing incident response plans should a breach occur. In the event of a data security and/or privacy incident, Contractor will implement the actions set forth in its incident response plan. Contractor keeps PII provided to Contractor secure and uses reasonable administrative, technical, and physical safeguards to do so. Contractor maintains and updates incident response plans that establish procedures in the event a breach occurs. Contractor also identifies individuals responsible for implementing incident response plans should a breach occur.
- b. If E2CCB or Contractor determines that a breach has occurred, when there is a reasonable risk of identity theft or other harm, or where otherwise required by law or this Agreement, Contractor provides any legally required notification to affected parties as promptly as possible, and fully cooperates as needed to ensure compliance with all breach of confidentiality laws.
- c. Contractor reports as promptly as possible to E2CCB and persons responsible for managing its organization's incident response plan any incident or threatened incident involving unauthorized access to or acquisition of PII of which they become aware. Such incidents include, but are not necessarily limited to, any breach or hacking of Contractor's Electronic Data System or any loss or theft of data, other electronic storage, or paper. As used herein, "Electronic Data System" means all information processing and communications hardware and software employed in Contractor's business, whether or not owned by Contractor or operated by its employees or agents in performing work for Contractor.

13. Contractor, its employees and representatives shall at all times comply with all

applicable federal, state, and local laws, rules, and regulations.

14. Notwithstanding any conflicting provisions of Contractor's terms of service, privacy policies (including but not limited to its Student Data Protection Addendum), or the BOCES Purchase Contract, the Parties agree and acknowledge that E2CCB bears no responsibility either on its own behalf or on behalf of educational agencies with whom it contracts for complying with the notification and consent requirements that are or may be imposed on "operators" pursuant to Children's Online Privacy Protection Act ("COPPA") and its implementing regulations.

15. This Agreement, together with the signed Parents Bill of Rights for Data Privacy and the Security and Supplemental Information to Parents Bill or Rights for Data Privacy and Security, constitutes the entire understanding of the Parties with respect to the subject matter thereof. The terms of this Agreement, together with the signed Parents Bill of Rights for Data Privacy and the Security and Supplemental Information to Parents Bill or Rights for Data Privacy and Security, shall supersede any conflicting provisions of Contractor's terms of service or privacy policy, or the BOCES Purchase Contract.

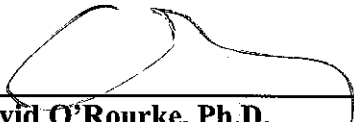
16. If any provision of this Agreement is held to be invalid or unenforceable for any reason, the remaining provisions will continue to be valid and enforceable. If a court finds that any provision to this Agreement is invalid or unenforceable, but that by limiting such provision it would become valid or enforceable, then such provision will be deemed to be written, construed, and enforced as so limited.

17. This Agreement will be binding on any successors of the parties.

18. This Agreement will be governed by the laws of the State of New York. Any action or proceeding arising out of this contract will be brought in the appropriate courts of New York State.

In witness of the foregoing, the duly authorized representatives of the Parties have signed this Memorandum on the date indicated.

FOR THE ERIE 2-CHAUTAUQUA-CATTARAUGUS BOCES:

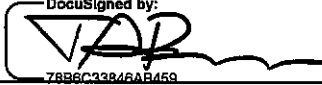


David O'Rourke, Ph.D.
District Superintendent

7/7/22

Date

FOR THE CONTRACTOR:

DocuSigned by:


Travis Barrs
Head of Global Operations

June 9, 2022

Date

KD


ATTACHMENT 1: PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

E2CCB is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, E2CCB wishes to inform the community of the following:

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.
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.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints may be submitted to NYSED at www.nysed.gov/data-privacy-security; 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.

Supplemental Information to Parents Bill or Rights for Data Privacy and Security:

1. Discovery Education (hereinafter "Contractor") is being provided access to personally identifiable information for the sole and exclusive purpose of carrying out the services for which E2CCB has contracted. Student data and/or teacher or principal data received by Contractor, or by any assignee of Contractor, from E2CCB or its employees, officers, agents, and/or students will not be sold or used for commercial purposes or marketing purposes.
2. Contractor agrees that any of its officers or employees, and any officers or employees of any assignee or subcontractor of Contractor, who have access to personally identifiable information will receive training on the federal and state law governing confidentiality of such data prior to receiving access to that data. Contractor will ensure that its personnel and subcontractors that access the student data are informed of the confidential nature of the student data they receive and that they are bound by applicable statutory and/or contractual obligations of confidentiality, as set forth in the Contractor's Student Data Protection Addendum, located at <https://www.discoveryeducation.com/data-protection-addendum/>. Contractor will also take all reasonable steps to ensure the reliability of Contractor personnel and subcontractors that access student data.

3. The agreement between Contractor and E2CCB for Discovery Education Streaming Services and any related services and/or resources expires on June 30, 2025. Upon expiration of that agreement without a successor agreement in place, Contractor will securely delete or otherwise destroy any and all student data and/or teacher or principal data remaining in the possession of Contractor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of such data) as well as any and all student data and/or teacher or principal data maintained on behalf of Contractor in secure data center facilities. Contractor shall ensure that no copy, summary, or extract of the student data and/or teacher or principal data or any related work papers are retained on any storage medium whatsoever by Contractor, its subcontractors or assignees, or the aforementioned secure data center facilities. Any and all measures related to the deletion, or destruction of student data and/or teacher or principal data will be completed within 60 days of the expiration of the agreement between BOCES and Contractor, and will be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. To the extent that Contractor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (*i.e.*, data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party. Upon request, Contractor and/or its subcontractors or assignees will provide a certification to E2CCB from an appropriate officer that the requirements of this paragraph have been satisfied in full.

4. In the event that a parent, student, or eligible student wishes to challenge the accuracy of student data concerning that student or eligible student, that challenge shall be processed through the procedures provided by the E2CCB for amendment of education records under the Family Educational Rights and Privacy Act (FERPA). In the event that a teacher or principal wishes to challenge the accuracy of the teacher or principal data that is collected, he or she may do so consistent with applicable provisions of 8 N.Y.C.R.R. Part 30 and the BOCES Annual Professional Performance Review Plan.

5. Student data and/or teacher or principal data transferred to Contractor by E2CCB or E2CCB officers, employees, agents, or students will be stored in electronic format on systems maintained by Contractor in a secure data center facility, or a data facility maintained by a board of cooperative educational services, in the United States. In order to protect the privacy and security of student data and/or teacher or principal data stored in that manner, Contractor will take measures aligned with industry best practices and the NIST Cybersecurity Framework Version 1.1. Such measures include, but are not necessarily limited to disk encryption, file encryption, firewalls, and password protection.

More specifically, Contractor implements security measures based on the level of risks, capabilities, and operating requirements. These measures include, as appropriate and reasonable, the following safeguards:

- a. Administrative Safeguards

- i. Sanctions: Appropriate sanctions against Contractor personnel who fail to comply with Contractor's security policies and procedures.
 - ii. System Monitoring: Procedures to regularly review records of information systems activity, including maintaining access logs, access reports, security incident tracking reports, and periodic access audits.
 - iii. Security Oversight: Assignment of one or more appropriate management-level employees of Contractor to be responsible for developing, implementing, and monitoring of safeguards and security issues.
 - iv. Appropriate Access: Procedures to determine that the access of Contractor personnel to PII is appropriate and meets a legitimate need to support their roles in business or educational operations. Procedures for establishing appropriate authorization and authentication mechanisms for Contractor personnel who have access to PII.
 - v. Employee Supervision: Procedures for regularly monitoring and supervising personnel who have access to PII.
 - vi. Access Termination: Procedures for terminating access to PII when employment ends, or when an individual no longer has a legitimate need for access.
- b. Operational Safeguards
- i. Access to PII: Procedures that grant access to PII by establishing, documenting, reviewing, and modifying a user's right of access to a workstation, software application/transaction, or process.
 - ii. Awareness Training: On-going security awareness through training or other means that provide Contractor personnel (including management) with updates to security procedures and policies (including guarding against, detecting, and reporting malicious software). Awareness training also addresses procedures for monitoring log-in attempts and reporting discrepancies, as well as procedures for safeguarding passwords.
 - iii. Incident Response Plan: Procedures for responding to, documenting, and mitigating where practicable suspected or known incidents involving a possible breach of security and their outcomes.
 - iv. Physical Access: Procedures to limit physical access to PII and the facility or facilities in which they are housed while ensuring that properly authorized access is allowed, including physical barriers that require electronic control validation (e.g., card access systems) or validation by human security personnel.
 - v. Physical Identification Validation: Access is physically safeguarded to prevent tampering and theft, including procedures to address control and validation of a person's access to facilities based on his or her need for access to the PII.
 - vi. Operational Environment: Procedures that specify the proper functions to be performed, the manner in which they are to be performed, and the physical attributes of the surroundings of facilities where PII is stored.

vii. **Media Movement:** Procedures that govern the receipt and removal of hardware and electronic media that contain PII into and out of a facility.

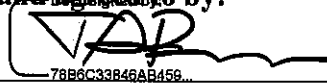
c. **Technical Safeguards**

- i. **Data Transmissions:** Technical safeguards, including encryption, to ensure PII transmitted over an electronic communications network is not accessed by unauthorized persons or groups.
- ii. **Data Integrity:** Procedures that protect PII maintained by Discovery from improper alteration or destruction. These procedures include mechanisms to authenticate records and corroborate that they have not been altered or destroyed in an unauthorized manner.
- iii. **Logging off Inactive Users:** Inactive electronic sessions are designed to terminate automatically after a specified period of time.

6. Any student data and/or teacher or principal data possessed by Contractor will be protected using encryption while in motion and at rest.

Acknowledged and agreed to by:

Signature:


78B6C33B46AB458...

Name:

Travis Barrs

Title:

Head of Global Operations

Date:

June 9, 2022