PRODUCT: Castle Software

COMPANY: Harris School Solutions

Hamilton Fulton Montgomery Board of Cooperative Educational Services Data Privacy Agreement

1. Definitions

    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. **Chief Privacy Officer** means the Chief Privacy Officer appointed by the Commissioner pursuant to Education Law §2-d.

    c. **Commercial 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.

    d. **Contract or Agreement** means a binding agreement between the District and a third-party contractor, which shall include but not be limited to an agreement created in electronic form and signed with an electronic or digital signature or a click wrap agreement that is used with software licenses, downloaded and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service.

    e. **District** means the Hamilton Fulton Montgomery Board of Cooperative Educational Services, as well as all of its component and subscribing school districts as set forth in Exhibit B.

    f. **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.

    g. **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.

    h. **Educational Agency** means a school district, board of cooperative educational services (BOCES), school, or the Department.

    i. **Eligible Student** means a student who is eighteen years or older.

    j. **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.

    k. **FERPA** means the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.

    l. **NIST Cybersecurity Framework** means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 which is available at the Office of Counsel, State Education Department, State Education Building, 89 Washington Avenue, Room 148, Albany, New York 12234.

    m. **Parent** means a parent, legal guardian, or person in parental relation to a student.

n. **Personally Identifiable Information ("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 Education Law §3012-c(10). And, includes, but is not limited to: name, name of parents or family members, personal identifier such as a social security number, student number, or biometric record, other indirect identifiers, such as the student's date of birth, place of birth and mother's maiden name, other information that, along or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty, or information requested by a person who the educational agency or institution reasonably believes or knows the identity of the student to whom the education record relates.

o. **Release** shall have the same meaning as Disclosure or Disclose.

p. **School** means any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law §3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law §4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.

q. **Student** means any person attending or seeking to enroll in an educational agency.

r. **Student Data** means personally identifiable information from the student records of an educational agency.

s. **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 Education Law §§3012-c and 3012-d.

t. **Third-Party Contractor or Contractor** means any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities pursuant to Education Law §211-e and is not an educational agency, and a not-for-profit corporation or other nonprofit organization, other than an educational agency.

    i. For purposes of this Agreement, "Contractor" shall mean Castle Software, Inc.

u. **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. Under the Agreement between the District and the Contractor ("Agreement"), the Contractor may receive PII regulated by several New York State and federal laws and regulations, including but not limited to, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (15

CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); Personal Privacy Protection Law (PPPL), Article 6-A of the New York Public Officers Law; New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. Contractor agrees that the security, confidentiality, and integrity of student data and/or teacher or principal data shall be maintained in accordance with the foregoing laws and regulations, and any other applicable New York State and federal laws and regulations, as well as:

   a. The terms and conditions of the contract between the District and the Contractor, including but not limited to the 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 and signed by a representative of Contractor and the District; and

   b. Applicable District policies, which can be accessed on the District website at: http://web2.moboces.org/districtpolicies/?public=hfmboces.

3. Contractor has no property or licensing rights or claims of ownership to PII, and shall not use PII for any other reason other than to provide the services outlined in the Agreement between the District and the Contractor. The Contractor shall further not sell PII 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 any other party, employee, subcontractor or other agent of Contractor to do so.

4. Parents, eligible students, teachers, principals, and other staff of District may file a complaint of breach or unauthorized release of PII with the District based on the contract or written agreement with Contractor. All complaints may be filed with David Ziskin, District Superintendent, in writing by email, dziskin@hfmboces.org, or by mail, 2755 State Highway 67 Johnstown, NY 12095.

5. The District understands the Contractor may use subcontractors to fulfill its responsibilities under its contract with the District. Contractor shall manage its relationships with subcontractors, employees, agents, or entities, to ensure the protection of PII consistent with all applicable state and federal law.

   Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this Data Privacy Agreement, Contractor shall: notify the District 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 Data Privacy Agreement. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements as set forth herein.

   Contractor also agrees and acknowledges that the data protection obligations imposed on it by state and federal law, as well as the terms of the agreement between the District and the Contractor shall apply to any subcontractor it engages in providing its contracted services to the District.

6. 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, employees, assignees and/or subcontractors, who have access to PII will receive training on the federal and New York State laws and regulations governing confidentiality of such data prior to receiving access to that data.

7. Once the contract between the District and the Contractor is expired and is not being renewed or extended, the Contractor, within ninety (90) days of such expiration date, shall destroy any student data or teacher or principal data or any other PII it received over the course of the agreement from the District. Redaction is specifically excluded as a means of data destruction. With regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Contractor shall provide the District a written certification of the secure deletion and/or destruction of PII held by the Contractor and/or subcontractors. To the extent Contractor and/or its subcontractors remain in possession of any de-identified data, they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

8. Upon request by the District, Contractor shall provide the District with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the District's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the District. Contractor may provide the District with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

9. 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, or a data facility maintained by a Board of Cooperative Educational Services. In order to protect the privacy and security of student data and/or teacher or principal data stored in that manner, Contractor use industry best practices and the NIST Cybersecurity Framework Version 1.1. Such measures shall include, but are not necessarily limited to disk encryption, file encryption, firewalls, and password protection.

10. Contractor shall promptly notify the District of any Breach of PII without unreasonable delay no later than seven (7) calendar days after discovery of the Breach. Notifications required under this paragraph must be in writing, given by personal delivery, email transmission (if contact information is provided for the specific mode of delivery), or by registered or certified mail, and to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and contact information for representatives who can assist the District. Notifications requested under this paragraph must be sent to the District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the District shall be subject to civil penalty pursuant to Education Law 2-d. The Breach of certain PII protected by Education Law 2-d may subject the Contractor to additional penalties.

    Notifications required under this paragraph must be provided to the District at the following address: 2755 State Highway 67 Johnstown, NY 12095 or dziskin@hfmboces.org.

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the District for the full cost of the District's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law 2-d and 8 NYCRR Part 121.

The confidentiality and data security obligations of the Contractor under this Data Privacy Agreement shall survive any termination of the Agreement between the District and the Contractor but shall termination upon Contractor's certifying that it has destroyed all PII.

11. Education Law 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the District. To the extent Student Data is held by Contractor pursuant to the Agreement, Contractor shall respond within thirty (30) calendar days to the District's request for access to Student Data so to allow the District to facilitate same to the Parent or Eligible Student. If a Parent or Eligible Student contacts the Contractor directly, the Contractor will refer same to the District.
12. As required by Education Law 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Agreement is included and incorporated in the Agreement between the District and the Contractor. Contractor shall fill-in and/or provide all necessary information for the Parents Bill of Rights for Data Privacy and Security and the supplemental information before the Agreement is executed.
13. In the event of a conflict between and among the terms and conditions of this Data Privacy Agreement, including the Parents Bill of Rights for Data Security and Privacy and the supplemental information incorporated into the Agreement between the District and the Contractor, the terms and conditions of this Data Privacy Agreement shall govern and prevail, shall survive the termination of the Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

	Mayeau
Hamilton Fulton Montgomery BOCES	Castle Software Representative
	Diva Mayeau, Vice President of Operations
Print Name	_ Print Name
	05/17/2022
Date	Date

EXHIBIT A:

HFM BOCES Parents Bill of Rights For Data Privacy and Security

The Hamilton Fulton Montgomery Board of Cooperative Educational Services ("HFM BOCES" or the "BOCES") is committed to ensuring student privacy in accordance with local state and federal regulations and policies. To this end and pursuant to the New York Education Law §2-d, and it's implementing regulations (Commissioner's regulations Part 121), Parents (including legal guardians or persons in parental relationships) and Eligible Students (student 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) shall not be sold or released for any commercial purposes. PII, as defined by Education Law §2-d and FERPA, includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.4 for a complete definition.

2. The right to inspect and review the complete contents of their child's education record stored or maintained by an educational agency, and may do so by contacting Dr. Aaron Bochniak, Assistant Superintendent, at (518) 736-4305 or abochniak@hfmboces.org. This right may not apply to parents of an Eligible Student.

3. State and federal laws such as Education Law §2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 123h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of student's personally identifiable information.

4. 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.

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

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. Complaints may be submitted to NYSED at http://www.nysed.gov/data-privacysecurity/report-improper-disclosure, or by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234; or by email to: privacy@nysed.gov. Complaints may also be directed to David Ziskin, Ed. D., District Superintendent, at 518-736-4681 or dziskin@hfmboces.org.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

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

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

10. Specify whether this Agreement involves disclosure to the Contractor of Student Data, APPR Data or both.

___x__ Disclosure of Student Data

______ Disclosure of APPR Data

11. The exclusive purposes for which Student Data or APPR Data may be used by the third-party contractor in the performance of this Agreement is to allow student to use self-directed activities, hints and explanations and progress reports aligned to state standards to increase student knowledge.

12. Identify any subcontractors or other persons/entities with whom the Contractor will share the Student Data or APPR Data in the performance of this Agreement and describe how the Contractor will ensure that persons/entities will abide by the data protection and security requirements of the Agreement.

In the event the Contractor engages a Subcontractor or otherwise shares Student Data or APPR Data with any other entity, Contractor acknowledges and agrees that before any such data is shared with a Contractor or other entity, such party must agree in writing to be bound by the confidentiality and data protection provisions set forth in this Agreement, including, but not limited to, the District's Policy for Data Security and Privacy. Upon termination of the agreement between the Contractor and a Subcontractor or other entity, Contractor acknowledges and agrees that it is responsible for ensuring that all Student Data or APPR Data shared by the Contractor must be returned to the Contractor or otherwise destroyed.

13. Specify the expiration date of the Contract and explain what will happen to the Student Data or APPR Data in the Contractor's possession, or in the possession of any person/entity described in response to Paragraph 12, upon the expiration or earlier termination of the Agreement.

Contract Expiration Date: June 30, 2023

_____ Contractor agrees to return the Student Data or APPR Data to the District consistent with the protocols set forth in the Data Privacy Agreement.

_____ Contractor agrees to securely destroy the Student Data or APPR Data consistent with the protocols set forth in the Data Privacy Agreement

14. A parent, student, eligible student (student eighteen years or older), teacher or principal may challenge the accuracy of the Student Data or APPR Data that is collected by contacting the District which produced the challenged record or data or otherwise created such data.

15. The third party contractor shall protect all student data or teacher principal data through security protections consistent with the industry standards. The third party contractor shall store any student data or teacher or principal data using HTTPS/SSL encryption protocols on a secure Rackspace server and shall ensure such data will be protected and data security and privacy risks are mitigated, and shall use encryption protections on such data while in motion and at rest.

	Mayeau
Hamilton Fulton Montgomery BOCES	Castle Software Representative
	Diva Mayeau - Vice President of Operations
Print Name	Print Name
	5/17/2022
Date	Date

EXHIBIT B:

List of Component and Subscribed School Districts of the Hamilton Fulton Montgomery BOCES for Services

Component School Districts	Other Subscribing School Districts
Greater Amsterdam School District	
Broadalbin-Perth Central School District	
Canajoharie Central School District	
Edinburg Common School District	
Fonda-Fultonville Central School District	
Fort Plain Central School District	
Gloversville Enlarged School District	
Greater Johnstown School District	
Lake Pleasant Central School District	
Mayfield Central School District	
Northville Central School District	
Oppenheim-Ephratah-St. Johnsville Central School District	
Piseco Common School District	
Wells Central School District	
Wheelerville Union Free School District	
Fulton Montgomery Community College	