

DATA SHARING AND CONFIDENTIALITY AGREEMENT

Including Parent's Bill of Rights for Data Privacy and Security and Supplemental Information about a Master Agreement between CPCS and [Name of Vendor]

1. Purpose (a) CPCS (hereinafter "District") and [Name of Vendor] (hereinafter "Vendor") are parties to a contract or other written agreement pursuant to which Vendor will receive student data and/or teacher or principal data that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as "Section 2-d") from the District for purposes of providing certain products or services to the District (the "Master Agreement"). (b) This Exhibit supplements the Master Agreement to which it is attached, to ensure that the Master Agreement conforms to the requirements of Section 2-d. This Exhibit consists of a Data Sharing and Confidentiality Agreement, a copy of the District's Bill of Rights for Data Security and Privacy signed by Vendor, and the Supplemental Information about the Master Agreement between CPCS and [Name of Vendor] that the District is required by Section 2-d to post on its website. (c) In consideration of the mutual promises set forth in the Master Agreement, Vendor agrees that it will comply with all terms set forth in the Master Agreement and this Exhibit. To the extent that any terms contained in the Master Agreement, or any terms contained in any other Exhibit(s) attached to and made a part of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In addition, in the event that Vendor has online or written Privacy Policies or Terms of Service (collectively, "TOS") that would otherwise be applicable to its customers or users of the products or services that are the subject of the Master Agreement between the District and Vendor, to the extent that any terms of the TOS, that are or may be in effect at any time during the term of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.
2. Definitions As used in this Exhibit:
 - a. "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor may receive from the District pursuant to the Master Agreement.
 - b. "Teacher or Principal Data" means personally identifiable information, as defined in Section 2-d, relating to the annual professional performance reviews of classroom teachers or principals that Vendor may receive from the District pursuant to the Master Agreement.
 - c. "Protected Data" means Student Data and/or Teacher or Principal Data, to the extent applicable to the product or service actually being provided to the District by Vendor pursuant to the Master Agreement.
 - d. "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).
3. Confidentiality of Protected Data

- a. Vendor acknowledges that the Protected Data It receives pursuant to the Master Agreement originates from the District and that this Protected Data belongs to and is owned by the District.
 - b. Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and the District's policy on data security and privacy. The District will provide Vendor with a copy of its policy on data security and privacy upon request.
4. Data Security and Privacy Plan As more fully described herein, throughout the term of the Master Agreement, Vendor will have a Data Security and Privacy Plan in place to protect the confidentiality, privacy and security of the Protected Data it receives from the District. Vendor's Plan for protecting the District's Protected Data includes, but is not limited to, its agreement to comply with the terms of the District's Bill of Rights for Data Security and Privacy, a copy of which is set forth below and has been signed by the Vendor. Additional components of Vendor's Data Security and Privacy Plan for protection of the District's Protected Data throughout the term of the Master Agreement are as follows:
 - a. Vendor will implement all state, federal, and local data security and privacy requirements including those contained within the Master Agreement and this Data Sharing and Confidentiality Agreement, consistent with the District's data security and privacy policy.
 - b. Vendor will have specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from the District under the Master Agreement.
 - c. Vendor will comply with all obligations contained within the section set forth in this Exhibit below entitled "Supplemental Information about a Master Agreement between CPCS and [Name of Vendor]." Vendor's obligations described within this section include, but are not limited to:
 - i. its obligation to require subcontractors or other authorized persons or entities to whom it may disclose Protected Data (if any) to execute written agreements acknowledging that the data protection obligations imposed on Vendor by state and federal law and the Master Agreement shall apply to the subcontractor, and
 - ii. its obligation to follow certain procedures for the return, transition, deletion and/or destruction of Protected Data upon termination, expiration or assignment (to the extent authorized) of the Master Agreement.
 - d. Vendor has provided or will provide training on the federal and state laws governing confidentiality of Protected Data for any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who will have access to Protected Data, prior to their receiving access.
 - e. Vendor will manage data security and privacy incidents that implicate Protected Data and will develop and implement plans to identify breaches

and unauthorized disclosures. Vendor will provide prompt notification to the District of any breaches or unauthorized disclosures of Protected Data in accordance with the Data Sharing and Confidentiality Agreement.

5. Notification of Breach and Unauthorized Release:

a. Vendor will promptly notify the District of any breach or unauthorized release of Protected Data it has received from the District in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

b. Vendor will provide such notification to the District by contacting Tara Celotti tara.celotti@cpcsteam.org or Brandon Johnson, brandon.johnson@cpcsteam.org both at 518-597-3285.

c. Vendor will cooperate with the District and provide as much information as possible directly to Tara Celotti or Brandon Johnson or his/her designee about the incident, including but not limited to:

d. description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of Protected Data involved, an estimate of the number of records affected, the schools within the District affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

e. Vendor acknowledges that upon initial notification from Vendor, the District, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor agrees not to provide this notification to the CPO directly unless requested by the District or otherwise required by law. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by the District, Vendor will promptly inform the designee.

6. Additional Statutory and Regulatory Obligations 1 Vendor acknowledges that it has the following additional obligations under Section 2-d with respect to any Protected Data received from the District, and that any failure to fulfill one or more of these statutory or regulatory obligations will be deemed a breach of the Master Agreement and the terms of this Data Sharing and Confidentiality Agreement:

a. To limit internal access to Protected Data to only those employees or subcontractors that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act

(FERPA); i.e., they need access in order to assist Vendor in fulfilling one or more of its obligations to the District under the Master Agreement.

b. To not use Protected Data for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement and the Master Agreement to which this Exhibit is attached.

c. To not disclose any Protected Data to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations to the District and in compliance with state and federal law, regulations and the terms of the Master Agreement, unless:

i. the parent or eligible student has provided prior written consent; or
1 Nothing in Education Law Section 2-d or Part 121 specifically requires an educational agency to include within its contracts with third-party contractors this list of obligations that are imposed on third-party contractors by the statute and/or its implementing regulations. However, many school districts and other educational agencies have considered it a best practice to include these statutory and regulatory obligations within their third-party contracts.

ii. the disclosure is required by statute or court order and notice of the disclosure is provided to the District no later than 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 Protected Data in its custody.

e. To use encryption technology to protect Protected Data in its custody while in motion or at rest, using a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

f. To adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.

g. To comply with the District's policy on data security and privacy, Section 2- d and Part 121. (h)

h. To not sell Protected Data 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 another party to do so.

i. To notify the District, in accordance with this Data Sharing and Confidentiality Agreement, of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of applicable state or federal law, the District's Bill of Rights for Data Security and

Privacy, the District's policies on data security and privacy, or other binding obligations relating to data privacy and security contained in the Master Agreement and this Exhibit.

j. To cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.

k. To pay for or promptly reimburse the District for the full cost of notification, in the event the District is required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

Additional student data privacy information

This bill of rights is subject to change based on regulations of the commissioner of education and the SED chief privacy officer, as well as emerging guidance documents from SED.

Also more information is available at:

- **NIST (National Institute of Standards and Technology) Cybersecurity Framework**
 - Standards for educational agencies employees that handle PII (personally identifiable information) receive annual data security and privacy training.
- **New York State Department of Education guidance document** issued on July 29, 2014 (PDF), Proposed Adoption of Part 121 Education Relating to Data Privacy and Security of Students Data and Certain Annual Professional Performance Review Data issued January 29, 2020.
- **U.S. Department of Education press release:** Guidance for Schools Issued on How to Keep Parents Better Informed on the Data they Collect on Students (PDF)
- **Privacy Technical Assistance Center (PTAC):** newly established one-stop resource for education stakeholders to learn about data privacy.