06/21/2023

Addendum "A"

DATA PRIVACY PLAN AND PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

Pursuant to Section 2-d of the Education Law, agreements entered between the District and a third-party contractor which require the disclosure of student data and/or teacher or principal data that contains personally identifiable information ("**PII**") to the contractor, must include a data security and privacy plan and must ensure that all contracts with third-party contractors incorporate the District's Parents' Bill of Rights for Data Security and Privacy (Attachment A).

As such, Oxford University Press USA ("**Contractor**") agrees that the following terms shall be incorporated into the licensing agreement for services ("**the Agreement**") and it shall adhere to the following:

1. The Contactor's storage, use and transmission of student and teacher/principal PII shall be consistent with the District's Data Security and Privacy Policy available here: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.capitalregionboces.org/wp-content/uploads/2023/05/5676-CRB-Privacy-and-Security-for-StudentTeacher-and-Principal-Data-Policy-3-30-20.pdf

2. Contractor shall not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or permit another party to do so.

3. The exclusive purposes for which the student data or teacher or principal data will be used under the Agreement are set forth in Paragraph 2 of the Agreement only for the term of the Agreement as set forth in Paragraph 1.

4. The Agreement shall maintain the following administrative, operational and technical safeguards and practices in place to protect PII, which shall align with the NIST Cybersecurity Framework, including:

    a. PII data will be protected using encryption while in motion and at rest by using 256-bit encryption to protect personal identifiable information (PII) both when it is being transmitted (in transit) and when it is stored (at rest).

    b. PII will be stored in a manner as to protect its security and to mitigate any potential security risks. Specifically, all student data and/or teacher or principal data will be stored by implementing secure data storage protocols, such as encryption and access controls. The security of this data will be ensured by implementing a range of security safeguards, including but not limited to, firewalls, intrusion detection and prevention systems, regular security audits, and ongoing staff training on data protection and cybersecurity best practices.

Attachment "A"
PARENTS' BILL OF RIGHTS FOR STUDENT DATA PRIVACY AND SECURITY

Capital Region BOCES, 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. BOCES 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.

- A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes by BOCES or any a third party contractor. BOCES will not sell student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by BOCES in accordance with BOCES policy;

- 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 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 Data Protection Officer, (518) 464-5139, DPO@neric.org, Capital Region BOCES, 900 Watervliet-Shaker Rd., Albany NY 12205. Complaints can also be directed to the New York State Education Department online at http://nysed.gov/data-privacy-security by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to privacy@mail.nysed.gov or by telephone at 518-474-0937.

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

- Parents can expect that educational agency workers who handle PII will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect PII.

- In the event that BOCES 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 the Data Protection Officer, (518)-464-5139, DPO@neric.org, 900 Watervliet-Shaker Rd., Albany NY 12205, or can access the information on BOCES' website https://www.capitalregionboces.org/.