Yorktown Central School District

July 1, 2024

The following information has been included as part of a parent bill of rights. The State Education Department (SED), the Common Core Implementation Reform Act, requires educational agencies and BOCES to publish a ”Parents Bill of Rights for Data Privacy and Security” on their website. While awaiting further guidance from the State Education Department, we are responding accordingly until such guidance is provided and shall comply with the law to the extent possible under the circumstances. As a district we may find that communicating this information to stakeholders helpful in fostering an awareness of data privacy and security issues. It is understood that this information regarding the Parents Bill of Rights for Data Privacy and Security will be updated as additional regulatory guidance becomes available from the State Education Department.

The Yorktown Central School District is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with Education Law § 2-d, the District wishes to inform the community of the following.

PARENTS’ BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY MAINTAINING PRIVACY AND SECURITY OF STUDENT DATA

In accordance with the requirements of Section 2-d of the New York Education Law, parents and students are entitled to certain protections regarding confidential student information. The Yorktown Central School District is committed to safeguarding personally identifiable information from unauthorized access or disclosure and herby sets forth the following Parents’ Bill of Rights for Data Privacy and Security below:

1. New York State Education Law Section 2-d (“Section 2-d”) and the Family Educational Rights and Privacy Act (“FERPA”) protect the confidentiality of personally identifiable information. Section 2-d and FERPA assures the confidentiality of records with respect to "third parties," and provides parents with the right to consent to disclosures of personally identifiable information contained in their child’s education records. Exceptions to this include school employees, officials and certain State and Federal officials who have a legitimate educational need to access such records. In addition, the District will, upon request of parents, or adult students, or if otherwise required by law, disclose student records to officials of another school district in which a student seeks to enroll.

2. A student's personally identifiable information cannot be sold or released for any commercial purposes and use of personally identifiable information by the educational agency shall benefit students and the educational agency;

3. Personally identifiable information includes, but is not limited to:
    i. The student's name;
    ii. The name of the student's parent or other family members;

iii. The address of the student or student's family;
iv. A personal identifier, such as the student's social security number, student number, or biometric record;
v. Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
vi. Other information that, alone 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
vii. Information requested by a person who the District reasonably believes knows the identity of the student to whom the education record relates.
viii. As such, PII will not be included in public reports or other documents.

4. Verified parents/guardians have the right to inspect and review the complete contents of their child's education record. The District shall comply with a request for access to records within a reasonable period, but not more than 45 calendar days after receipt of a request.

5. The District is committed to implementing safeguards associated with industry standards and best practices under state and federal laws protecting the confidentiality of personally identifiable information, including, but not limited to, encryption, firewalls, and password protection must be in place when data is stored or transferred.

6. New York State, through the New York State Education Department, collects a number of student data elements for authorized uses. A complete list of all student data elements collected by the State is available for public review, at: NYSED Data Elements List. Parents may also obtain a copy of this list by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, N.Y. 12234.

7. Parents have the right to have complaints about possible breaches of student data or teacher or principal data addressed. Complaints should be submitted in writing to:
   Ms. Jennifer Forsberg, Data Protection Officer
   jforsberg@yorktown.org,
   2725 Crompond Road, Yorktown Heights, NY 10598

   Additionally, parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; the e-mail address is cpo@mail.nysed.gov. SED's complaint process is under development and will be established through regulations from the department's chief privacy officer, who has yet to be appointed.

8. The District contracts with the Lower Hudson Regional Information Center, BOCES and certain third party contractors. For the purposes of further ensuring confidentiality and security of student data, as an appendix to the Parents' Bill of Rights each contract an educational agency enters into with a third party contractor shall include the following supplemental information:

i. the exclusive purposes for which the student data, or teacher or principal data, will be used;

ii. how the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

iii. when the agreement with the third party contractor expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

iv. if and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and

v. where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

vi. How the data will be protected using encryption while in motion and at rest.

9. A parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected by filing a written request with:

   Ms. Jennifer Forsberg, Data Protection Officer
   jforsberg@yorktown.org,
   2725 Crompond Road, Yorktown Heights, NY 10598.

10. In addition, the Data Protection Officer, with input from parents and other education and expert stakeholders, is required to develop additional elements of the Parents' Bill of Rights to be prescribed in the Regulations of the Commissioner. This Bill of Rights is subject to change based on guidance received from the Chief Privacy Officer, the Commissioner of Education and New York State Education Department.

SUPPLEMENTAL INFORMATION AND DATA PRIVACY AGREEMENT
FOR THIRD PARTY CONTRACTORS

The Yorktown Central School District provides certain student data to the following third party contractors:

CONTRACTOR	[Vendor Name]
PRODUCT	[Product Name]
PURPOSE	The student data,or teacher or principal data collection will be used for: [insert the purpose of the use of the the data, for example,“Independent Assessment And Ongoing Practice of Math Skills.”]
SUBCONTRACTOR	This contractor is prohibited from further sharing any student data to subcontractors, research institutions, persons or entities that are not directly an employee or department/office within this contractor’s organization, unless written consent is included with any contract. This includes sharing of any database, spreadsheet, word processing, csv, html or text files or providing credentials to access the data via the contracted software. This does not pertain to the actual storage of the data on physical hard drives or solid state drives of a data center. This contractor shall only disclose personally identifiable student data (as well as personally identifiable teacher and principal data protected by Education Law 2-d) to this contractor’s employees and subcontractors who need to know such personally identifiable data in order to provide the contracted services to the DISTRICT and the disclosure of such personally identifiable data shall be limited to the extent necessary to provide such services. This contractor must ensure that each subcontractor receiving or having access to any of the DISTRICT’s personally identifiable student data (as well as personally identifiable teacher and principal data protected by Education Law 2-d) is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this Supplemental Information and Data Security and Privacy Plan for Third Party Contractors (“DPA”).
CONTRACT DURATION AND DATA DESTRUCTION	The agreement expires June 30, annually. Upon expiration of this Contract without a successor agreement in place, Vendor shall assist DISTRICT in exporting all Protected Information previously received from, or then owned by, DISTRICT. Upon expiration of this Contract with a successor agreement in place, Vendor will cooperate with the DISTRICT as necessary to transition protected data to the successor vendor prior to deletion. Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities. All student data shall be

	deleted (within 90 days) in accordance with the National Institute of Standards and Technology (NIST) standard 800-88.
DATA ACCURACY	In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the DISTRICT for amendment of education records under the Family Education Rights and Privacy Act. In the event that a teacher or principal seeks to challenge the accuracy of teacher or principal data pertaining to the particular teacher or principal, that challenge will be processed in accordance with the procedures the DISTRICT has established for challenging annual professional performance review ("APPR") data.
CONTRACTOR / SUBCONTRACTOR TRAINING	The contractor/subcontractor will provide annual training on data privacy and security awareness to all employees who have access to student and classroom teacher/building principal PII.
SECURITY PRACTICES	The data is stored in the continental United States (CONUS) or Canada. Vendor will maintain administrative, technical, and physical safeguards that equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection, and that align with the NIST Cybersecurity Framework 2.0. Vendor will 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). This contractor shall promptly notify the DISTRICT of any breach or unauthorized disclosure of the DISTRICT's personally identifiable student data (as well as personally identifiable teacher and principal data protected by Education Law 2-d) without unreasonable delay no later than seven (7) business days after discovery of any such breach or unauthorized disclosure.
Contractor penalties for unauthorized release of student, teacher, or principal data:	Each breach or unauthorized release of student data or teacher or principal data by a third-party contractor shall be punishable by a civil penalty of the greater of $5,000 or up to $10 per student, teacher, and principal whose data was released, provided that the latter amount shall not exceed the maximum penalty imposed under General Business Law §899-aa (6) (a). Upon conclusion of an investigation, if the Chief Privacy Officer determines that a third-party contractor has through its actions or omissions caused student data or teacher or principal data to be breached or released to any person or entity not authorized by law to receive such data in violation of applicable state or federal law, the data and security policies of the educational agency, and/or any binding contractual obligations, the Chief Privacy Officer shall notify the third-party contractor of such finding and give the third-party contractor no more than 30 days to submit a written response.

Vendor Address:

Vendor Phone:

Vendor Email:

Name: Title:

Signature: _____ Date: _____