CLINTON-ESSEX-WARREN-WASHINTON BOCES

DATA SECURITY AND PRIVACY FAQ

Note: The following is provided for your information and convenience only. This document is not intended to create additional parent and student rights.

What is Personally Identifiable Information (PII)?

PII includes but not limited to:

A. First name and last name
B. Names of parents or family members (including the maiden name of a student's mother)
C. Household address
D. Date or place of birth
E. Social security numbers
F. Student-identification numbers issued by schools or school systems
G. Digital files such as photographs, videos, or audio recordings, among other forms of information that may reveal a specific student's identity
H. Biometric data (e.g., fingerprints or palm prints)
I. Geolocation data (e.g., real-time location data relayed by a smartphone)
J. Metadata (i.e., "data about other data," such as data about image size, resolution, color, or date of creation that are commonly embedded in digital photos)
K. 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

What steps does CVES take to minimize its collection, processing, and transmission of PII?

A. 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 another party to do so.

B. Ensure that it has provisions in its contracts with third-party contractors or in separate data sharing and confidentiality agreements that require the confidentiality of shared student data or teacher or principal data be maintained in accordance with law, regulation, and District policy.

Except as required by law or in the case of educational enrollment data, CVES, identified as the "District" throughout this document, will not report to NYSED the following student data elements:

A. Juvenile delinquency records;

B. Criminal records;

C. Medical and health records; and

D. Student biometric information.

What is the role of the NYS Chief Privacy Officer?

The Commissioner of Education has appointed a Chief Privacy Officer who will report to the Commissioner on matters affecting privacy and the security of student data and teacher and principal data. Among other functions, the Chief Privacy Officer is authorized to provide assistance to educational agencies within the state on minimum standards and best practices associated with privacy and the security of student data and teacher and principal data.

The District will comply with its obligation to report breaches or unauthorized releases of student data or teacher or principal data to the Chief Privacy Officer in accordance with Education Law Section 2-d, its implementing regulations, and this policy.

The Chief Privacy Officer has the power, among others, to:

A. Access all records, reports, audits, reviews, documents, papers, recommendations, and other materials maintained by the District that relate to student data or teacher or principal data, which includes, but is not limited to, records related to any technology product or service that will be utilized to store and/or process PII; and

B. Based upon a review of these records, require the District to act to ensure that PII is protected in accordance with laws and regulations, including but not limited to requiring the District to perform a privacy impact and security risk assessment.

What is the role of the CVES Data Protection Officer?

The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures including those required by Education Law Section 2-d and its implementing regulations, as well as serving as the main point of contact for data privacy and security for the District.

The District will ensure that the Data Protection Officer has the appropriate knowledge, training, and experience to administer these functions. The Data Protection Officer may perform these functions in addition to other job responsibilities.

What cybersecurity framework is CVES utilizing to safeguard its data?

The District will use the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1) (Framework) as the standard for its data privacy and security program. The Framework is a risk-based approach to managing cybersecurity risk and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. The Framework provides a common taxonomy and mechanism for organizations to:

A. Describe their current cybersecurity posture;

B. Describe their target state for cybersecurity;

C. Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;

D. Assess progress toward the target state; and

E. Communicate among internal and external stakeholders about cybersecurity risk.

The District will protect the privacy of PII by:

A. Ensuring that every use and disclosure of PII by the District benefits students and the District by considering, among other criteria, whether the use and/or disclosure will:

    a. Improve academic achievement;

    b. Empower parents and students with information; and/or

    c. Advance efficient and effective school operations.

B. Not including PII in public reports or other public documents.

The District affords all protections under FERPA and the Individuals with Disabilities Education Act and their implementing regulations to parents or eligible students, where applicable.

When a Third-Party Contractor is receiving student, principal and/or teacher PII, what are the district and third-party contractor responsibilities?

District Responsibilities

The District will ensure that whenever it enters into a contract or other written agreement with a third-party contractor under which the third-party contractor will receive student data or teacher or principal data from the District, the contract or written agreement will include provisions requiring that confidentiality of shared student data or teacher or principal data be maintained in accordance with law, regulation, and District policy.

In addition, the District will ensure that the contract or written agreement includes the third-party contractor's data privacy and security plan that has been accepted by the District.

The third-party contractor's data privacy and security plan must, at a minimum:

A. Outline how the third-party contractor will implement all state, federal, and local data privacy and security contract requirements over the life of the contract, consistent with District policy;

B. Specify the administrative, operational, and technical safeguards and practices the third-party contractor has in place to protect PII that it will receive under the contract;

C. Demonstrate that the third-party contractor complies with the requirements of 8 NYCRR Section 121.3(c);

D. Specify how officers or employees of the third-party contractor and its assignees who have access to student data or teacher or principal data receive or will receive training on the laws governing confidentiality of this data prior to receiving access;

    a. Specify if the third-party contractor will utilize subcontractors and how it will manage those relationships and contracts to ensure PII is protected;

    b. Specify how the third-party contractor will manage data privacy and security incidents that implicate PII including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the District;

E. Describe whether, how, and when data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires; and

F. Include a signed copy of the Parents' Bill of Rights for Data Privacy and Security.

Third-Party Contractor Responsibilities

Each third-party contractor, that enters into a contract or other written agreement with the District under which the third-party contractor will receive student data or teacher or principal data from the District, is required to:

A. Adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework;

B. Comply with District policy and Education Law Section 2-d and its implementing regulations;

C. Limit internal access to PII to only those employees or subcontractors that have legitimate educational interests (i.e., they need access to provide the contracted services);

D. Not use the PII for any purpose not explicitly authorized in its contract;

E. Not disclose any PII to any other party without the prior written consent of the parent or eligible student:

   a. Except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with law, regulation, and its contract with the District; or

   b. Unless required by law or court order and the third-party contractor provides a notice of the disclosure to NYSED, the Board, or the institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by law or court order;

F. Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of PII in its custody;

G. Use encryption to protect PII in its custody while in motion or at rest; and

H. 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 another party to do so.

Where a third-party contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by law and contract apply to the subcontractor.

What are Click-Wrap Agreements?

Periodically, District staff may wish to use software, applications, or other technologies in which the user must "click" a button or box to agree to certain online terms of service prior to using the software, application, or other technology. These are known as "click-wrap agreements" and are considered legally binding "contracts or other written agreements" under Education Law Section 2-d and its implementing regulations.

District staff are prohibited from using software, applications, or other technologies pursuant to a click-wrap agreement in which the third-party contractor receives student data or teacher or principal data from the District unless they have received prior approval from the District's Data Privacy Officer or designee.

The District will develop and implement procedures requiring prior review and approval for staff use of any software, applications, or other technologies pursuant to click-wrap agreements.

Where can one access the CVES Parents' Bill of Rights for Data Privacy and Security?

The CVES Parents' Bill of Rights for Data Privacy and Security (Bill of Rights) is posted on the CVES website (https://www.cves.org/wp-content/uploads/2016/11/5512-Parents-Bill-of-Rights-Relating-to-Student-Data-March-2015.pdf). Additionally, the District will include the Bill of Rights with every contract or other written agreement it enters into with a third-party contractor under which the third-party contractor will receive student data or teacher or principal data from the District.

How does one file a complaint of a possible breach or unauthorized release of student data and/or teacher or principal data?

CVES has established the following procedures for parents, eligible students, teachers, principals, and other District staff to file complaints with the district about breaches or unauthorized releases of student data and/or teacher or principal data:

A. All complaints must be submitted to the District's Data Protection Officer in writing.

B. Upon receipt of a complaint, the district will promptly acknowledge receipt of the complaint, commence an investigation, and take the necessary precautions to protect PII.

C. Following the investigation of a submitted complaint, the district will provide the individual who filed the complaint with its findings. This will be completed within a reasonable period of time, but no more than 60 calendar days from the receipt of the complaint by the district.

D. If the district requires additional time, or where the response may compromise security or impede a law enforcement investigation, the district will provide the individual who filed the complaint with a written explanation that includes the approximate date when the District anticipates that it will respond to the complaint.

These procedures will be disseminated to parents, eligible students, teachers, principals, and other district staff.

How will CVES notify NYS Chief Privacy Officer of a breach or unauthorized release?

The District will report every discovery or report of a breach or unauthorized release of student data or teacher or principal data within the District to the Chief Privacy Officer without unreasonable delay, but no more than ten calendar days after the discovery.

Each third-party contractor that receives student data or teacher or principal data pursuant to a contract or other written agreement entered into with the District will be required to promptly notify the District of any breach of security resulting in an unauthorized release of the data by the third-party contractor or its assignees in violation of applicable laws and regulations, the Parents' Bill of Rights for Student Data Privacy and Security, District policy, and/or binding contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay, but no more than seven calendar days after the discovery of the breach.

In the event of notification from a third-party contractor, the District will in turn notify the Chief Privacy Officer of the breach or unauthorized release of student data or teacher or principal data no more than ten calendar days after it receives the third-party contractor's notification using a form or format prescribed by NYSED.

How will CVES notify affected parents, students, teachers and/or principals of a breach or unauthorized release?

CVES will notify affected parents, eligible students, teachers, and/or principals in the most expedient way possible and without unreasonable delay, but no more than 60 calendar days after the discovery of a breach or unauthorized release of PII by the CVES or the receipt of a notification of a breach or unauthorized release of PII from a third-party contractor unless that notification would interfere with an ongoing investigation by law enforcement or cause further disclosure of PII by disclosing an unfixed security vulnerability. Where notification is delayed under these circumstances, CVES will notify parents, eligible students, teachers, and/or principals within seven calendar days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends.

Notifications will be clear, concise, use language that is plain and easy to understand, and to the extent available, include:

A. A brief description of the breach or unauthorized release, the dates of the incident and the date of discovery, if known;

B. A description of the types of PII affected;

C. An estimate of the number of records affected;

D. A brief description of the District's investigation or plan to investigate; and

E. Contact information for representatives who can assist parents or eligible students that have additional questions.

Notification will be directly provided to the affected parent, eligible student, teacher, or principal by first-class mail to their last known address, by email, or by telephone.

Where a breach or unauthorized release is attributed to a third-party contractor, the third-party contractor is required to pay for or promptly reimburse the District for the full cost of this notification.

How often will CVES provide annual data privacy and security training for employees?

CVES will annually provide data privacy and security awareness training to its officers and staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations. CVES may deliver this training using online training tools. Additionally, this training may be included as part of the training that CVES already offers to its workforce.

Definitions

As provided in Education Law Section 2-d and/or its implementing regulations, the following terms, as used in this policy, will mean:

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 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. "Contract or other written agreement" means a binding agreement between an educational agency and a third-party, which includes, but is not 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.

D. "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.

E. "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 42 USC Section 17932(h)(2).

F. "FERPA" means the Family Educational Rights and Privacy Act and its implementing regulations, 20 USC Section 1232g and 34 CFR Part 99, respectively.

G. "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). A copy of the NIST Cybersecurity Framework is available at the Office of Counsel, State Education Department, State Education Building, Room 148, 89 Washington Avenue, Albany, New York 12234.

H. "Parent" means a parent, legal guardian, or person in parental relation to a student.

I. "Personally identifiable information (PII)," as applied to student data, means personally identifiable information as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act, 20 USC Section 1232g, and, as applied to teacher or principal data, means personally identifying information as this term is defined in Education Law Section 3012-c(10).

J. "Release" has the same meaning as disclosure or disclose.

K. "Student data" means personally identifiable information from the student records of an educational agency.

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 Education Law Sections 3012-c and 3012-d.

M. "Third-party 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 the educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of the educational agency, or audit or evaluation of publicly funded programs. This term will 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 Section 211-e and is not an educational agency, and a not-for-profit corporation or other nonprofit organization, other than an educational agency.

N. “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.

Acknowledged By Board 6/10/20