Adopted by CPCS BOE on _____

Bill of Rights for Data Privacy and Security

The Crown Point Central School District is committed to ensuring student and staff privacy in accordance with local, state and federal regulations and district policies. To this end and pursuant to U.S. Department of Education (DOE) regulations (Education Law 3012-c & 3012-d) and Part 121, the district is providing the following Bill of Rights for Data Privacy and Security:

- A student's personally identifiable information cannot be sold or released for any commercial or marketing purposes.

- Parents and/or eligible students have the right to inspect and review the complete contents of their child's education record, including any student data maintained by the Crown Point Central School District. This right of inspection of records is consistent with the federal Family Educational Rights and Privacy Act (FERPA). Under the more recently adopted regulations (Education Law §2-d), the rights of inspection are extended to include data, meaning parents have the right to inspect or receive copies of any data in their child's educational record. The New York State Education Department (SED) will develop further policies and procedures related to these rights in the future.

- State and federal laws protect the confidentiality of personally identifiable information and 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 is available for public review in an Excel file at

http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx.

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 who will make a recommendation to the Commissioner for his/her final determination.

- Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to the Superintendent of Schools. Complaints to SED 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.

- New regulations authorizes teachers, principals and staff of the educational agency to utilize the complaint process when there is an improper disclosure of student data and/or teacher or principal data (such as annual professional performance reviews).

- Also, the new regulations as of this year, enacts that each educational agencies and district will identify a data protection officer that will be responsible for the educational agency's data privacy and security program. In the course of complying with its obligations under this law, CEWW BOCES has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors have access to student data and teacher/principal data, as those terms are defined by law. (see below)

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 4 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.

AMENDMENT TO THE REGULATIONS OF THE COMMISSIONER OF EDUCATION

Pursuant to Education Law sections 2-d, 101, 207 and 305,

a new Part 121 shall be added effective upon adoption to read as follows:

Part 121

Strengthening Data Privacy and Security in NY State Educational Agencies to Protect Personally Identifiable Information

§121.1 Definitions.

As used in this Part, the following terms shall have the following meanings:

(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 other written agreement* means a binding agreement between an educational agency and a third-party, 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) *Disclose* or *Disclosure* mean 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.

(f) *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.

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

(h) *Eligible Student* means a student who is eighteen years or older.

(i) *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.

(j) *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.

(k) *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, Room 148, 89 Washington Avenue, Albany, New York 12234.

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

(m) *Personally Identifiable Information*, 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).

(n) *Release* shall have the same meaning as Disclosure or Disclose.

(o) *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 .

(p) *Student* means any person attending or seeking to enroll in an educational agency.

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

(r) *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.

(s) *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 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.

(t) *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.

§121.2 Educational Agency Data Collection Transparency and Restrictions.

(a) Educational agencies shall not sell personally identifiable information 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) Each educational agency shall take steps to minimize its collection, processing and transmission of personally identifiable information.

(c) Each educational agency shall 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 federal and state law and the educational agency's data security and privacy policy.

(d) Except as required by law or in the case of educational enrollment data, school districts shall not report to the department the following student data elements:

(1) juvenile delinquency records; (2) criminal records; (3) medical and health records; and (4) student biometric information.

§121.3 Bill of Rights for Data Privacy and Security.

(a) Each educational agency shall publish on its website a parents bill of rights for data privacy and security ("bill of rights") that complies with the provisions of Education Law §2-d (3).

(b) The bill of rights shall also be included with every contract an educational agency enters with a third-party contractor that receives personally identifiable information.

(c) The bill of rights shall also include supplemental information for each contract the educational agency enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data. The supplemental information must be developed by the educational agency and include the following information:

(1) the exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;

(2) how the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations (e.g., FERPA; Education Law §2-d);

(3) the duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the educational agency, and/or whether, when and how the data will be destroyed).

(4) 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;

(5) 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 and data security and privacy risks mitigated; and

(6) address how the data will be protected using encryption while in motion and at rest.

(d) Each educational agency shall publish on its website the supplement to the bill of rights for any contract or other written agreement with a third-party contractor that will receive personally identifiable information.

(e) The bill of rights and supplemental information may be redacted to the extent necessary to safeguard the privacy and/or security of the educational agency's data and/or technology infrastructure.

§121.4 Complaints of Breach or Unauthorized Release of Personally Identifiable Information

(a) Each educational agency must establish and communicate to parents, eligible students, teachers, principals or other staff of an educational agency, its procedures for them to file complaints about breaches or unauthorized releases of student data and/or teacher or principal data.

(b) The complaint procedures must require educational agencies to promptly acknowledge receipt of complaints, commence an investigation, and take the necessary precautions to protect personally identifiable information.

(c) Following its investigation of a submitted complaint, the educational agency shall provide the parent or eligible student, teacher, principal or any other staff member of the educational agency who filed a complaint with its findings within a reasonable period but no more than 60 calendar days from the receipt of the complaint by the educational agency. Where the educational agency requires additional time, or where the response may compromise security or impede a law enforcement investigation, the educational agency shall provide the parent, eligible student, teacher, principal or any other staff member of the educational agency who filed a complaint with a written explanation that includes the approximate date when the educational agency anticipates that it will respond to the complaint.

(d) Educational agencies may require complaints to be submitted in writing.

(e) Educational agencies must maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1 (1988; rev. 2004), as set forth in section 185.12, Appendix I of this Title.

§121.5 Data Security and Privacy Standard.

(a) As required by Education Law §2-d (5), the Department adopts the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or NIST CSF) as the standard for data security and privacy for educational agencies.

(b) No later than July 1, 2020, each educational agency shall adopt and publish a data security and privacy policy that implements the requirements of this Part and aligns with the NIST CSF.

(c) Each educational agency's data security and privacy policy must also address the data privacy protections set forth in Education Law §2-d (5)(b)(1) and (2) as follows:

(1) every use and disclosure of personally identifiable information by the educational agency shall benefit students and the educational agency (e.g., improve academic achievement, empower parents and students with information, and/or advance efficient and effective school operations).

(2) personally identifiable information shall not be included in public reports or other documents.

(d) An educational agency's data security and privacy policy shall include all the protections afforded to parents or eligible students, where applicable, under FERPA and the Individuals with Disabilities Education Act (20 U.S.C. 1400 et seq.), and the federal regulations implementing such statutes.

(e) Each educational agency must publish its data security and privacy policy on its website and provide notice of the policy to all its officers and employees.

§121.6 Data Security and Privacy Plan.

(a) Each educational agency that enters into a contract with a third-party contractor shall ensure that the contract includes the third-party contractor's data security and privacy plan that is accepted by the educational agency. The data security and privacy plan shall, at a minimum:

(1) outline how the third-party contractor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy;

(2) specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the contract;

(3) demonstrate that it complies with the requirements of Section 121.3(c) of this Part;

(4) 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 federal and state laws governing confidentiality of such data prior to receiving access;

(5) specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

(6) specify how the third-party contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

(7) describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.

§121.7 Training for Educational Agency Employees.

Educational agencies shall annually provide data privacy and security awareness training to their officers and employees with access to personally identifiable information. Such training should include but not be limited to training on the state and federal laws that protect personally identifiable information, and how employees can comply with such laws. Such training may be delivered using online training tools and may be included as part of training the educational agency already offers to its workforce.

§121.8 Educational Agency Data Protection Officer

(a) Each educational agency shall designate a Data Protection Officer to be responsible for the implementation of the policies and procedures required in Education Law §2-d and this Part, and to serve as the point of contact for data security and privacy for the educational agency.

(b) Data Protection Officers must have the appropriate knowledge, training and experience to administer the functions described in this Part.

(c) A current employee of an educational agency may perform this function in addition to other job responsibilities.

§121.9 Third Party Contractors

(a) In addition to all other requirements for third-party contractors set forth in this Part, each third-party contractor that will receive student data or teacher or principal data shall:

(1) adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework;

(2) comply with the data security and privacy policy of the educational agency with whom it contracts; Education Law § 2-d; and this Part;

(3) limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;

(4) not use the personally identifiable information for any purpose not explicitly authorized in its contract;

(5) not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student:

(i) 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 state and federal law, regulations and its contract with the educational agency; or

(ii) unless required by statute or court order and the third-party contractor provides a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

(6) maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;

(7) use encryption to protect personally identifiable information in its custody while in motion or at rest; and

(8) not sell personally identifiable information 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) Where a third-party contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

§121.10 Reports and Notifications of Breach and Unauthorized Release

(a) Third-party contractors shall promptly notify each educational agency with which it has a contract of any breach or unauthorized release of personally identifiable information in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of such breach.

(b) Each educational agency shall in turn notify the Chief Privacy Officer of the breach or unauthorized release no more than 10 calendar days after it receives the third-party contractor's notification using a form or format prescribed by the Department.

(c) Third-party contractors must cooperate with educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.

(d) Educational agencies shall report every discovery or report of a breach or unauthorized release of student, teacher or principal data to the Chief Privacy Officer without unreasonable delay, but no more than 10 calendar days after such discovery.

(e) Educational agencies shall 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 by an educational agency or the receipt of a notification of a breach or unauthorized release from a third-party contractor unless that notification would interfere with an ongoing investigation by law enforcement or cause further disclosure of personally identifiable information by disclosing an unfixed security vulnerability. Where notification is delayed under these circumstances, the educational agency shall 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.

(f) Where a breach or unauthorized release is attributed to a third-party contractor, the third-party contractor shall pay for or promptly reimburse the educational agency for the full cost of such notification.

(g) Notifications required by this section shall be clear, concise, use language that is plain and easy to understand, and to the extent available, include: a brief description of the breach or unauthorized release, the dates of the incident and the date of discovery, if known; a description of the types of personally identifiable information affected; an estimate of the number of records affected; a brief description of the educational agency's investigation or plan to investigate; and contact information for representatives who can assist parents or eligible students that have additional questions.

(h) Notification must 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.

(i) Upon the belief that a breach or unauthorized release constitutes criminal conduct, the Chief Privacy Officer shall report such breach and unauthorized release to law enforcement in the most expedient way possible and without unreasonable delay.

§121.11 Third Party Contractor Civil Penalties

(a) Each third party contractor that receives student data or teacher or principal data pursuant to a contract or other written agreement with an educational agency shall be required to notify such educational agency of any breach of security resulting in an unauthorized release of such data by the third party contractor or its assignees in violation of applicable state or federal law, the parents bill of rights for student data privacy and security, the data privacy and security policies of the educational agency and/or binding contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay. Each violation of this paragraph 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).

(b) Except as otherwise provided in subdivision (a) each violation of Education Law §2-d by a third-party contractor or its assignee shall be punishable by a civil penalty of up to $1,000.00; a second violation by the same third party contractor involving the same data shall be punishable by a civil penalty of up to $5,000; any

subsequent violation by the same third party contractor involving the same data shall be punishable by a civil penalty of up to $10,000. Each violation shall be considered a separate violation for purposes of civil penalties and the total penalty shall not exceed the maximum penalty imposed under General Business Law §899-aa (6) (a).

(c) The Chief Privacy Officer shall investigate reports of breaches or unauthorized releases of student data or teacher or principal data by third-party contractors. As part of an investigation, the Chief Privacy Officer may require that the parties submit documentation, provide testimony, and may visit, examine and/or inspect the third-party contractor's facilities and records.

(d) 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.

(e) () If after reviewing the third-party contractor's written response, the Chief Privacy Officer determines the incident to be a violation of Education Law §2-d, the Chief Privacy Officer shall be authorized to:

(1) order the third-party contractor be precluded from accessing personally identifiable information from the affected educational agency for a fixed period of up to five years; and/or

(2) order that a third-party contractor or assignee who knowingly or recklessly allowed for the breach or unauthorized release of student data or teacher

or principal data be precluded from accessing student data or teacher or principal data from any educational agency in the state for a fixed period of up to five years; and/or

(3) order that a third party contractor who knowingly or recklessly allowed for the breach or unauthorized release of student data or teacher or principal data shall not be deemed a responsible bidder or offeror on any contract with an educational agency that involves the sharing of student data or teacher or principal data, as applicable for purposes of the provisions of General Municipal Law §103 or State Finance Law §163(10)(c), as applicable, for a fixed period of up to five years;

(4) require the third-party contractor to provide additional training governing confidentiality of student data and/or teacher or principal data to all its officers and employees with reasonable access to such data and certify that it has been performed, at the contractor's expense. Such additional training must be performed immediately and include a review of federal and state laws, rules, regulations, including Education Law §2-d and this Part.

(f) If the Chief Privacy Officer determines that the breach or unauthorized release of student data or teacher or principal data on the part of the third-party contractor or assignee was inadvertent and done without intent, knowledge, recklessness or gross negligence, the Chief Privacy Officer would make a recommendation to the Commissioner that no penalty be issued upon the third-party contractor. The Commissioner would then make a final determination as to whether the breach or unauthorized release of student data or teacher or principal data on the part of the third-party contractor or assignee was inadvertent and done without intent,

knowledge, recklessness or gross negligence and whether or not a penalty should be issued.

§121.12 Right of Parents and Eligible Students to Inspect and Review Students Education Records

(a) Consistent with the obligations of the educational agency under FERPA, parents and eligible students shall have the right to inspect and review a student's education record by making a request directly to the educational agency in a manner prescribed by the educational agency.

(b) An educational agency shall ensure that only authorized individuals are able to inspect and review student data. To that end, educational agencies shall take steps to verify the identity of parents or eligible students who submit requests to inspect and review an education record and verify the individual's authority to do so.

(c) Requests by a parent or eligible student for access to a student's education records must be directed to an educational agency and not to a third-party contractor. An educational agency may require that requests to inspect and review education records be made in writing.

(d) Educational agencies are required to notify parents annually of their right to request to inspect and review their child's education record including any student data stored or maintained by an educational agency. A notice issued by an educational agency to comply with the FERPA annual notice requirement shall be deemed to satisfy this requirement. Two separate annual notices shall not be required.

(e) Educational agencies 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.

(f) Educational agencies may provide the records to a parent or eligible student electronically, if the parent consents to such a delivery method. The educational agency must transmit the personally identifiable information in a way that complies with State and federal law and regulations. Safeguards associated with industry standards and best practices, including but not limited to, encryption and password protection, must be in place when education records requested by a parent or eligible student are electronically transmitted.

§121.13 Chief Privacy Officer's Powers

(a) The Chief Privacy Officer shall have the power to access all records, reports, audits, reviews, documents, papers, recommendations, and other materials maintained by an educational agency that relate to student data or teacher or principal data, which shall include but not be limited to records related to any technology product or service that will be utilized to store and/or process personally identifiable information.

(b) Based upon a review of such records, the Chief Privacy Officer may require an educational agency to act to ensure that personally identifiable information is protected in accordance with state and federal law and regulations, including but not limited to requiring an educational agency to perform a privacy impact and security risk assessment.

(c) The Chief Privacy Officer shall also have and exercise any other powers that the commissioner shall deem appropriate.

§ 121.14 Severability.

If any provision of this Part or its application to any person or circumstances is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this Part or their application to other persons and circumstances, and those remaining provisions shall not be affected but shall remain in full force and effect.

Unauthorized Disclosure Complaint Procedure

(please print and return)

Contact info:

Name:

Phone:

Email:

Mailing Address:

Role/Relationship to impacted person:

District Affiliation:

Complaint:

Education Law 2-d & Part 121

Data Protection Officer (DPO)

Tara S. Celotti

Tara.celotti@cpcsteam.org

518-597-3285 ext. 7

See unauthorized disclosure complaint procedure below.

Directory Information

Directory information is information contained in the education records of a student that would not generally be considered harmful or an invasion of privacy if disclosed. Typically, "directory information" includes information such as name, address, telephone listing, date and place of birth, participation in officially recognized activities and sports, and dates of attendance. A school may disclose "directory information" to third parties without consent if it has given public notice of the types of information which it has designated as "directory information," the parent's or eligible student's right to restrict the disclosure of such information, and the period of time within which a parent or eligible student has to notify the school in writing that he or she does not want any or all of those types of information designated as "directory information." 34 CFR § 99.3 and 34 CFR § 99.37 (http://www2.ed.gov/policy/gen/guid/fpco/pdf/ferparegs.pdf).

For more information, see the PTAC publication Protecting Student Privacy While Using Online Educational Services (/node/161/).

RESOURCES

Family Educational Rights and Privacy Act (FERPA) (/node/548/)

Security Best Practices (/node/40/)

Glossary (/glossary)

Letters of Importance (/node/478/)

Historic Findings Letters (/node/542/)

TRAINING

Online Training Modules (/content/online-training-modules)

Guidance Videos (/content/videos)

Recorded Webinars (/content/recorded-webinars)

BROWSE BY AUDIENCE

School Officials K-12 (/audience/school-officials-k-12)

Parents & Students (/audience/parents-and-students)

Postsecondary School Officials (/node/30/)

Early Childhood Educators (/node/59/)

Vendors (/node/32/)

Researchers (/node/58/)

OTHER

FAQs (/frequently-asked-questions)

About (/about)

Contact (/contact)

Subscribe to the Student Privacy Newsletter (/subscribe-student-privacy-newsletter)

Request PTAC Training or Technical Assistance (/request-ptac-training-or-technical-assistance)

Privacy Policy (https://www2.ed.gov/notices/privacy/index.html?src=ft)

(/)

Privacy Technical Assistance Center

For more information, please visit the Privacy Technical Assistance Center: https://studentprivacy.ed.gov

Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices

Overview

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems and other uses of student data. PTAC provides timely information and updated guidance on privacy, confidentiality, and security practices through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of student data systems. More PTAC information is available on https://studentprivacy.ed.gov.

PTAC welcomes input on this document and suggestions for future technical assistance resources relating to student privacy. Comments and suggestions can be sent to PrivacyTA@ed.gov.

Purpose

Recent advances in technology and telecommunications have dramatically changed the landscape of education in the United States. Gone are the days when textbooks, photocopies, and filmstrips supplied the entirety of educational content to a classroom full of students. Today's classrooms increasingly employ on-demand delivery of personalized content, virtual forums for interacting with other students and teachers, and a wealth of other interactive technologies that help foster and enhance the learning process. Online forums help teachers share lesson plans; social media help students collaborate across classrooms; and web-based applications assist teachers in customizing the learning experience for each student to achieve greater learning outcomes.

Early adopters of these technologies have demonstrated their potential to transform the educational process, but they have also called attention to possible challenges. In particular, the information sharing, web-hosting, and telecommunication innovations that have enabled these new education technologies raise questions about how best to protect student privacy during use. This document will address a number of these questions, and present some requirements and best practices to consider, when evaluating the use of online educational services.

What are Online Educational Services?

This document will address privacy and security considerations relating to computer software, mobile applications (apps), and web-based tools provided by a third-party to a school or district that students and/or their parents access via the Internet and use as part of a school activity. Examples include online services that students use to access class readings, to view their learning progression, to watch

video demonstrations, to comment on class activities, or to complete their homework. This document does not address online services or social media that students may use in their personal capacity outside of school, nor does it apply to online services that a school or district may use to which students and/or their parents do not have access (e.g., an online student information system used exclusively by teachers and staff for administrative purposes).

Many different terms are used to describe both the online services discussed in this document (e.g., Ed Tech, educational web services, information and communications technology, etc.) and the companies and other organizations providing these services. This document will use the term "online educational services" to describe this broad category of tools and applications, and the term "provider" to describe the third-party vendors, contractors, and other service providers that make these services available to schools and districts.

Is Student Information Used in Online Educational Services Protected by FERPA?

It depends. Because of the diversity and variety of online educational services, there is no universal answer to this question. The Family Educational Rights and Privacy Act (FERPA) (see 20 U.S.C. § 1232g and 34 CFR Part 99) protects personally identifiable information (PII) from students' education records from unauthorized disclosure. FERPA defines education records as "records that are: (1) directly related to a student; and (2) maintained by an educational agency or institution or by a party acting for the agency or institution" (see 34 CFR § 99.3 definition of "education record"). FERPA also defines the term PII, which includes direct identifiers (such as a student's or other family member's name) and indirect identifiers (such as a student's date of birth, place of birth, or mother's maiden name) (see 34 CFR § 99.3 definition of "personally identifiable information"). For more information about FERPA, please visit the Family Policy Compliance Office's Web site at https://studentprivacy.ed.gov.

Some types of online educational services do use FERPA-protected information. For example, a district may decide to use an online system to allow students (and their parents) to log in and access class materials. In order to create student accounts, the district or school will likely need to give the provider the students' names and contact information from the students' education records, which are protected by FERPA. Conversely, other types of online educational services may not implicate FERPA-protected information. For example, a teacher may have students watch video tutorials or complete interactive exercises offered by a provider that does not require individual students to log in. In these cases, no PII from the students' education records would be disclosed to (or maintained by) the provider.

Online educational services increasingly collect a large amount of contextual or transactional data as part of their operations, often referred to as "metadata." Metadata refer to information that provides meaning and context to other data being collected; for example, information about how long a particular student took to perform an online task has more meaning if the user knows the date and time when the student completed the activity, how many attempts the student made, and how long the student's mouse hovered over an item (potentially indicating indecision).

Metadata that have been stripped of all direct and indirect identifiers are not considered protected information under FERPA because they are not PII. A provider that has been granted access to PII from education records under the school official exception may use any metadata that are not linked to FERPA-protected information for other purposes, unless otherwise prohibited by the terms of their agreement with the school or district.

Schools and districts will typically need to evaluate the use of online educational services on a case-by-case basis to determine if FERPA-protected information (i.e., PII from education records) is implicated. If so, schools and districts must ensure that FERPA requirements are met (as well as the requirements of any other applicable federal, state, tribal, or local laws).

EXAMPLE 1: A district enters into an agreement to use an online tutoring and teaching program and discloses PII from education records needed to establish accounts for individual students using FERPA's school official exception. The provider sends reports on student progress to teachers on a weekly basis, summarizing how each student is progressing. The provider collects metadata about student activity, including time spent online, desktop vs. mobile access, success rates, and keystroke information. If the provider de-identifies these metadata by removing all direct and indirect identifying information about the individual students (including school and most geographic information), the provider can then use this information to develop new personalized learning products and services (unless the district's agreement with the provider precludes this use).

What Does FERPA Require if PII from Students' Education Records is Disclosed to a Provider?

It depends. Because of the diversity and variety of online educational services, there is no universal answer to this question. Subject to exceptions, the general rule under FERPA is that a school or district cannot disclose PII from education records to a provider unless the school or district has first obtained written consent from the parents (or from "eligible students," i.e., those who are 18 years of age or older or attending a postsecondary school). Accordingly, schools and districts must either obtain consent, or ensure that the arrangement with the provider meets one of FERPA's exceptions to the written consent requirement.

While disclosures of PII to create user accounts or to set up individual student profiles may be accomplished under the "directory information" exception, more frequently this type of disclosure will be made under FERPA's school official exception. "Directory information" is information contained in the education records of a student that would not generally be considered harmful or an invasion of privacy if disclosed (see 34 CFR § 99.3 definition of "directory information"). Typical examples of directory information include student name and address. To disclose student information under this exception, individual school districts must establish the specific elements or categories of directory information that they intend to disclose and publish those elements or categories in a public notice. While the directory information exception can seem to be an easy way to share PII from education

records with providers, this approach may be insufficient for several reasons. First, only information specifically identified as directory information in the school's or district's public notice may be disclosed under this exception. Furthermore, parents (and eligible students) generally have the right to "opt out" of disclosures under this exception, thereby precluding the sharing of information about those students with providers. Given the number of parents (and eligible students) who elect to opt out of directory information, schools and districts may not find this exception feasible for disclosing PII from education records to providers to create student accounts or profiles.

The FERPA school official exception is more likely to apply to schools' and districts' use of online educational services. Under the school official exception, schools and districts may disclose PII from students' education records to a provider as long as the provider:

1. Performs an institutional service or function for which the school or district would otherwise use its own employees;

2. Has been determined to meet the criteria set forth in in the school's or district's annual notification of FERPA rights for being a school official with a legitimate educational interest in the education records;

3. Is under the direct control of the school or district with regard to the use and maintenance of education records; and

4. Uses education records only for authorized purposes and may not re-disclose PII from education records to other parties (unless the provider has specific authorization from the school or district to do so and it is otherwise permitted by FERPA).

See 34 CFR § 99.31(a)(1)(i).

Two of these requirements are of particular importance. First, the provider of the service receiving the PII must have been determined to meet the criteria for being a school official with a "legitimate educational interest" as set forth in the school's or district's annual FERPA notification. Second, the framework under which the school or district uses the service must satisfy the "direct control" requirement by restricting the provider from using the PII for unauthorized purposes. While FERPA regulations do not require a written agreement for use in disclosures under the school official exception, in practice, schools and districts wishing to outsource services will usually be able to establish direct control through a contract signed by both the school or district and the provider. In some cases, the "Terms of Service" (TOS) agreed to by the school or district, prior to using the online educational services, may contain all of the necessary legal provisions governing access, use, and protection of the data, and thus may be sufficient to legally bind the provider to terms that are consistent with these direct control requirements.

When disclosing PII from education records to providers under the school official exception, schools and districts should be mindful of FERPA's provisions governing parents' (and eligible students') access to the students' education records. Whenever a provider maintains a student's education records, the

school and district must be able to provide the requesting parent (or eligible student) with access to those records. Schools and districts should ensure that their agreements with providers include provisions to allow for direct or indirect parental access. Under FERPA, a school must comply with a request from a parent or eligible student for access to education records within a reasonable period of time, but not more than 45 days after it has received the request. Some States have laws that require access to education records sooner than 45 days.

Schools and districts are encouraged to remember that FERPA represents a minimum set of requirements to follow. Thus, even when sharing PII from education records under an exception to FERPA's consent requirement, it is considered a best practice to adopt a comprehensive approach to protecting student privacy when using online educational services.

Do FERPA and the Protection of Pupil Rights Amendment (PPRA) Limit What Providers Can Do with the Student Information They Collect or Receive?

On occasion, providers may seek to use the student information they receive or collect through online educational services for other purposes than that for which they received the information, like marketing new products or services to the student, targeting individual students with directed advertisements, or selling the information to a third party. If the school or district has shared information under FERPA's school official exception, however, the provider cannot use the FERPA-protected information for any other purpose than the purpose for which it was disclosed.

Any PII from students' education records that the provider receives under FERPA's school official exception may only be used for the specific purpose for which it was disclosed (i.e., to perform the outsourced institutional service or function, and the school or district must have direct control over the use and maintenance of the PII by the provider receiving the PII). Further, under FERPA's school official exception, the provider may not share (or sell) FERPA-protected information, or re-use it for any other purposes, except as directed by the school or district and as permitted by FERPA.

It is important to remember, however, that student information that has been properly de-identified or that is shared under the "directory information" exception, is not protected by FERPA, and thus is not subject to FERPA's use and re-disclosure limitations.

EXAMPLE 2: A district contracts with a provider to manage its cafeteria account services. Using the school official exception, the district gives the provider student names and other information from school records (not just directory information). The provider sets up an online system that allows the school, parents, and students to access cafeteria information to verify account balances and review the students' meal selections. The provider cannot sell the student roster to a third party, nor can it use PII from education records to target students for advertisements for foods that they often purchase at school under FERPA because the provider would then be using FERPA-protected information for different purposes than those for which the information was shared.

FERPA is not the only statute that limits what providers can do with student information. The Protection of Pupil Rights Amendment (PPRA) provides parents with certain rights with regard to some marketing activities in schools. Specifically, PPRA requires that a school district must, with exceptions, directly notify parents of students who are scheduled to participate in activities involving the collection, disclosure, or use of personal information collected from students for marketing purposes, or to sell or otherwise provide that information to others for marketing purposes, and to give parents the opportunity to opt-out of these activities. 20 U.S.C. § 1232h(c)(2)(C)(i). Subject to the same exceptions, PPRA also requires districts to develop and adopt policies, in consultation with parents, about these activities. 20 U.S.C. § 1232h(c)(1)(E) and (c)(4)(A). PPRA has an important exception, however, as neither parental notice and the opportunity to opt-out nor the development and adoption of policies are required for school districts to use students' personal information that they collect from students for the exclusive purpose of developing, evaluating, or providing educational products or services for students or schools. 20 U.S.C. § 1232h(c)(4)(A).

While FERPA protects PII from education records maintained by a school or district, PPRA is invoked when personal information is collected from the student. The use of online educational services may give rise to situations where the school or district provides FERPA-protected data to open accounts for students, and subsequent information gathered through the student's interaction with the online educational service may implicate PPRA. Student information collected or maintained as part of an online educational service may be protected under FERPA, under PPRA, under both statutes, or not protected by either. Which statute applies depends on the content of the information, how it is collected or disclosed, and the purposes for which it is used.

It is important to remember that even though PPRA only applies to K-12 institutions, there is no time-limit on the limitations governing the use of personal information collected from students for marketing purposes. So, for example, while PPRA would not limit the use of information collected from college students for marketing, it would restrict the use of information collected from students while they were still in high school (if no notice or opportunity to opt-out was provided) even after those students graduate.

EXAMPLE 3: A district contracts with an online tutoring service using the school official exception. As part of the service, the provider uses data about individual students to personalize learning modules for the district's students. This does not implicate the PPRA because the activity falls under the PPRA exception for educational services and products. This use of data about individual students is similarly permissible under FERPA because the provider is only using any FERPA-protected information for the purposes for which it was shared.

EXAMPLE 4: A district contracts under the school official exception with a provider for basic productivity applications to help educate students: email, calendaring, web-search, and document collaboration software. The district sets up the user accounts, using basic enrollment information (name, grade, etc.) from student records. Under FERPA, the provider may not use data about individual student preferences gleaned from scanning student content to target ads to individual students for clothing or toys, because using the data for these purposes was not authorized by the district and does not constitute a legitimate educational interest as specified in the district's annual notification of FERPA rights.

PPRA would similarly prohibit targeted ads for clothing or toys, unless the district had a policy addressing this and parents were notified and given the opportunity to opt-out of such marketing. In spite of these limitations, however, the provider may use data (even in individually identifiable form) to improve its delivery of these applications, including spam filtering and usage monitoring. The provider may also use any non-PII data, such as metadata with all direct and indirect identifiers removed, to create new products and services that the provider could market to schools and districts.

Schools and districts should be aware that neither FERPA nor the PPRA absolutely prohibits them from allowing providers to serve generalized, non-targeted advertisements. FERPA would not prohibit, for example, a school from selling space on billboards on the football field, nor would it prohibit a school or district from allowing a provider acting as a school official from serving ads to all students in email or other online services.

Finally, schools and districts should remember their important role in setting policies to protect student privacy. While FERPA and PPRA provide important protections for student information, additional use or disclosure restrictions may be advisable depending on the situation and the sensitivity of the information. Any additional protections that a school or district would like to require should be documented in the written agreement (the contract or TOS) with the provider.

What are Some Other Best Practices for Protecting Student Privacy When Using Online Educational Services?

Regardless of whether FERPA or PPRA applies to a school's or district's proposed use of online educational services, the Department recommends that schools and districts follow privacy, security, and transparency best practices, such as:

- **Maintain awareness of other relevant federal, state, tribal, or local laws.**

  FERPA and PPRA are not the only laws that protect student information. Other federal, state, tribal, or local laws may apply to online educational services, and may limit the information that can be shared with providers. In particular, schools and districts should be aware of and

consider the requirements of the Children's Online Privacy and Protection Act (COPPA) before using online educational services for children under age 13. In general, COPPA applies to commercial Web sites and online services directed to children and those Web sites and services with actual knowledge that they have collected personal information from children. Absent an exception, these sites must obtain verifiable parental consent prior to collecting personal information from children. The Federal Trade Commission (FTC) has interpreted COPPA to allow schools to exercise consent on behalf of parents in certain, limited circumstances (see http://www.business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions#Schools).

- **Be aware of which online educational services are currently being used in your district.**

  Conduct an inventory of the online educational services currently being used within your school or district. Not only will this help assess the scope and range of student information being shared with providers, but having a master list of online educational services will help school officials to collaboratively evaluate which services are most effective, and help foster informed communication with parents.

- **Have policies and procedures to evaluate and approve proposed online educational services.**

  Establish and enforce school and district-wide policies for evaluating and approving online educational services prior to implementation. Schools and districts should be clear with both teachers and administrators about how proposed online educational services can be approved, and who has the authority to enter into agreements with providers. This is true not only for formal contracts, but also for consumer-oriented "Click-Wrap" software that is acquired simply by clicking "accept" to the provider's TOS. With Click-Wrap agreements, the act of clicking a button to accept the TOS serves to enter the provider and the end-user (in this case, the school or district) into a contractual relationship akin to signing a contract.

  Most schools or districts already have processes in place for evaluating vendor contracts for privacy and security considerations; using these established procedures may be the most effective way to evaluate proposed online educational services. It is particularly important that teachers and staff not bypass internal controls in the acquisition process when deciding to use free online educational services. To ensure that privacy and security concerns relating to these free services are adequately considered, the Department recommends that free online educational services go through the same (or a similar) approval process as paid educational services to ensure that they do not present a risk to the privacy or security of students' data or to the schools and district's IT systems. Following standard internal controls, including testing, will also enable the schools and district's IT personnel to assist in the implementation process. Simple and more streamlined processes will, of course, generate greater compliance.

- **When possible, use a written contract or legal agreement.**

  As mentioned above, the use of online educational services usually involves some form of a

contract or legal agreement between the school and the provider. Having a written contract or legal agreement helps schools and districts maintain the required "direct control" over the use and maintenance of student data. Even when FERPA is not implicated, the Department recommends using written agreements as a best practice. When drafting and reviewing these contracts, the Department recommends the inclusion of certain provisions:

- Security and Data Stewardship Provisions. Make clear whether the data collected belongs to the school/district or the provider, describe each party's responsibilities in the event of a data breach (see PTAC's Data Breach Response Checklist), and, when appropriate, establish minimum security controls that must be met and allow for a security audit.

- Collection Provisions. Be specific about the information the provider will collect (e.g., forms, logs, cookies, tracking pixels, etc.).

- Data Use, Retention, Disclosure, and Destruction Provisions. Define the specific purposes for which the provider may use student information, and bind the provider to only those approved uses. If student information is being shared under the school official exception to consent in FERPA, then it would also be a best practice to specify in the agreement how the school or district will be exercising "direct control" over the third party provider's use and maintenance of the data. Specify with whom the provider may share (re-disclose) student information, and if PII from students' education records is involved, ensure that these provisions are consistent with FERPA. Include data archival and destruction requirements to ensure student information is no longer residing on the provider's systems after the contract period is complete. When appropriate, define what disclosure avoidance procedures must be performed to de-identify student information before the provider may retain it, share it with other parties, or use it for other purposes.

- Data Access Provisions. Specify whether the school, district and/or parents (or eligible students) will be permitted to access the data (and if so, to which data) and explain the process for obtaining access. This is especially important if the online educational services will be creating new education records that will be maintained by the provider on behalf of the school or district, as FERPA's requirements regarding parental (or eligible students') access will then apply. To avoid the challenges involved in proper authentication of students' parents by the provider, the Department recommends that the school or district serve as the intermediary for these requests, wherein the parent requests access to any education records created and maintained by the provider directly from the school or district, and the school or district then obtains the records from the provider to give back to the parent.

- Modification, Duration, and Termination Provisions. Establish how long the agreement will be in force, what the procedures will be for modifying the terms of the agreement

(mutual consent to any changes is a best practice), and what both parties' responsibilities will be upon termination of the agreement, particularly regarding disposition of student information maintained by the provider.

- Indemnification and Warranty Provisions. Carefully assess the need for and legality of any such provisions and determine whether applicable state or tribal law prohibits or limits the school's or district's ability to indemnify a provider. Analyze whether there should be indemnification provisions in which the provider agrees to indemnify the school or district, particularly relating to a school's or district's potential liabilities resulting from a provider's failure to comply with applicable federal, state, or tribal laws. Given that the Department looks to schools and districts to comply with FERPA and PPRA, be specific about what you will require the provider to do in order to comply with applicable state and federal laws, such as FERPA and PPRA, and what the provider agrees to do to remedy a violation of these requirements and compensate the school or district for damages resulting from the provider's violation.

- **Extra steps are necessary when accepting Click-Wrap licenses for consumer apps.**

  Schools and districts sometimes can't negotiate agreements with providers of consumer apps, and are faced with a choice to accept the providers' TOS or not use the app. Extra caution and extra steps are warranted before employing Click-Wrap consumer apps:

  - Check Amendment Provisions. In addition to reviewing for the above terms, you should review the TOS to determine if the provider has retained the right to amend the TOS without notice. If the provider will be using FERPA-protected information, schools and districts should exercise caution when entering into Click-Wrap agreements that allow for amendment without notice, given FERPA's requirement to maintain "direct control" over the use and maintenance of the information under the school official exception. It is a best practice to review these agreements regularly to determine if any provisions have changed, and if so, to re-evaluate whether to continue using the service.

  - Print or Save the TOS. When accepting a Click-Wrap agreement, you should save a copy of the TOS that you have agreed to. You can either download and save a digital copy, or print and file a copy.

  - Limit Authority to Accept TOS. One potential issue with Click-Wrap agreements is that they can be easily accepted, without going through normal district or school approval channels. Individual teachers may not understand the specifics of how the provider will use and secure student data. Districts or schools should develop policies outlining when individual teachers may download and use Click-Wrap software.

EXAMPLE 5: A teacher who has many remote students wants to foster increased collaboration and socialization among her students. Pursuant to her district's policy, she selects a service from a district-approved list of providers, and accepts the provider's Click-Wrap agreement before creating the user accounts for all students (including those who opted out of directory information). Her students successfully participate in a students-only social collaboration space.

EXAMPLE 6: A teacher wants students to be able to share photographs and videos online and identifies an app that will allow this sharing. He creates user accounts for all students (including those who opted out of directory information) and accepts the app's Click-Wrap agreement without reading it. The TOS allow the provider to use the information for a variety of non-educational purposes, including selling merchandise. The district discovers that this service is being used and determines that the TOS violate FERPA. The district proceeds to block access to the service from district computers, and begins negotiations with the provider to delete the user accounts and any information attached to them.

- **Be transparent with parents and students.**

  The Department encourages schools and districts to be as transparent as possible with parents and students about how the school or district collects, shares, protects, and uses student data. FERPA requires that schools and districts issue an annual notification to parents and eligible students explaining their rights under FERPA (34 CFR § 99.7), and many schools and districts elect to combine their directory information policy public notice, required pursuant to §99.37 of the regulations, with their annual notice of rights. PPRA also requires schools and districts to provide parents and students with effective notice of their PPRA rights, to provide notice to parents of district policies (developed and adopted in consultation with parents) regarding specific activities, and to notify them of the dates of specific events and the opportunity to opt out of participating in those events. Beyond FERPA and PPRA compliance, however, the Department recommends that schools and districts clearly explain on their Web sites how and with whom they share student data, and that they post any school and district policies on outsourcing of school functions, including online educational services. Schools and districts may also want to post copies of the privacy and security provisions of important third party contracts.

  With online educational services, it can often be unclear what information is being collected while students are using the technology. Even when this information is not protected by FERPA or other privacy laws, it is a best practice to inform students and their parents of what information is being collected and how it will be used. When appropriate, the Department recommends that schools or districts develop an education technology plan that addresses student privacy and information security issues, and solicit feedback from parents about the plan prior to its implementation or the adoption of new online education services.

Transparency provides parents, students, and the general public with important information about how the school or district protects the privacy of student data. Greater transparency enables parents, students, and the public to develop informed opinions about the benefits and risks of using education technology and helps alleviate confusion and misunderstandings about what data will be shared and how they will be used.

- **Consider that parental consent may be appropriate.**

  Even in instances where FERPA does not require parental consent, schools and districts should consider whether consent is appropriate. These are individual determinations that should be made on a case-by-case basis.

Additional Resources

Materials below include links to resources that provide additional best practice recommendations and guidance relating to use of online educational services. Please note that these resources do not necessarily address the particular legal requirements, including FERPA, that your school and district need to meet when collecting, storing, disseminating, or releasing education records to a provider. It is always a best practice to consult legal counsel to determine the applicable federal, state, tribal, and local requirements prior to entering into contractual agreements with providers. Some resources prepared by third-party experts are included as well.

- Family Policy Compliance Office, U.S. Department of Education, *Model Notice for Directory Information:* https://studentprivacy.ed.gov/resources/model-notice-directory-information
- National Institute of Standards and Technology, Computer Security Resource Center: http://csrc.nist.gov/publications/
- National Institute of Standards and Technology, *Guidelines on Security and Privacy in Public Cloud Computing* (2011): http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf
- National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems, Federal Information Processing Standards Publications (FIPS) 199* (2004): http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- Privacy Technical Assistance Center, U.S. Department of Education: https://studentpriavcy.ed.gov
- Privacy Technical Assistance Center, U.S. Department of Education, *Checklist – Data Breach Response* (2012): https://studentprivacy.ed.gov/resources/data-breach-response-checklist
- Privacy Technical Assistance Center, U.S. Department of Education, *Written Agreement Checklist* (2012): https://studentpriavcy.ed.gov/resources/written-agreement-checklist
- U.S. Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions - COPPA AND SCHOOLS* (2013): http://www.business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions#Schools
- U.S. Federal Trade Commission, *FTC Strengthens Kid's Privacy, Gives Parents Greater Control Over Their Information By Amending Children's Online Protection Rule* (2012): http://www.ftc.gov/opa/2012/12/coppa.shtm

Glossary

Directory Information is information contained in the education records of a student that would not generally be considered harmful or an invasion of privacy if disclosed. Typically, "directory information" includes information such as name, address, telephone listing, date and place of birth, participation in officially recognized activities and sports, and dates of attendance. A school may disclose "directory information" to third parties without consent if it has given public notice of the types of information which it has designated as "directory information," the parent's or eligible student's right to restrict the disclosure of such information, and the period of time within which a parent or eligible student has to notify the school in writing that he or she does not want any or all of those types of information designated as "directory information." 34 CFR § 99.3 and 34 CFR § 99.37.

Education records means records that are directly related to a student and are maintained by an educational agency or institution or by a party acting for the agency or institution. For more information, see the Family Educational Rights and Privacy Act regulations. 34 CFR § 99.3.

Eligible Student means a student to whom FERPA rights have transferred upon turning 18 years of age, or upon enrolling in a post-secondary institution at any age. 34 CFR § 99.3.

Personally identifiable information (PII) is a FERPA term referring to identifiable information that is maintained in education records and includes direct identifiers, such as a student's name or identification number, indirect identifiers, such as a student's date of birth, or other information which can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. See Family Educational Rights and Privacy Act regulations, 34 CFR § 99.3, for a complete definition of PII specific to education records and for examples of other data elements that are defined to constitute PII.

Personal Information Collected from Students is a PPRA term referring to individually identifiable information including a student or parent's first and last name; a home or other physical address (including street name and the name of the city or town); a telephone number; or a Social Security identification number collected from any elementary or secondary school student. 20 U.S.C. § 1232h(c)(6)(E).

School Official means any employee, including teacher, that the school or district has determined to have a "legitimate educational interest" in the personally identifiable information from an education record of a student. School officials may also include third party contractors, consultants, volunteers, service providers, or other party with whom the school or district has outsourced institutional services or functions for which the school or district would otherwise use employees under the school official exception in FERPA. 34 CFR § 99.31(a)(1).

Family Educational Rights and Privacy Act (FERPA)

Get the Latest on FERPA at https://studentprivacy.ed.gov/ (https://studentprivacy.ed.gov/?src=fpco)

- **Frequently Asked Questions** (https://studentprivacy.ed.gov/frequently-asked-questions)
- FERPA for **parents and students** (https://studentprivacy.ed.gov/audience/parents-and-students), **K12 school officials** (https://studentprivacy.ed.gov/audience/school-officials-k-12) and **Postsecondary school officials** (https://studentprivacy.ed.gov/audience/school-officials-post-secondary)
- Protection of Pupil Rights Amendment (**PPRA**) (https://studentprivacy.ed.gov/content/ppra)
- **Guidance** (https://studentprivacy.ed.gov/guidance) and **Notices** (https://studentprivacy.ed.gov/annual-notices)
- **Filing a complaint under FERPA or PPRA** (https://studentprivacy.ed.gov/file-a-complaint)

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.
- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.
- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):
    - School officials with legitimate educational interest;
    - Other schools to which a student is transferring;
    - Specified officials for audit or evaluation purposes;
    - Appropriate parties in connection with financial aid to a student;
    - Organizations conducting certain studies for or on behalf of the school;
    - Accrediting organizations;

- To comply with a judicial order or lawfully issued subpoena;
- Appropriate officials in cases of health and safety emergencies; and
- State and local authorities, within a juvenile justice system, pursuant to specific State law.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

Printable view
(/print/policy/gen/guid/fpco/ferpa/index.html)

Last Modified: 08/25/2021

How Do I Find...

- Student loans, forgiveness (/fund/grants-college.html?src=rn)
- Higher Education Rulemaking (https://www2.ed.gov/policy/highered/reg/hearulemaking/2021/index.html?src=rn)
- College accreditation (https://www.ed.gov/accreditation?src=rn)
- Every Student Succeeds Act (ESSA) (https://www.ed.gov/essa?src=rn)
- FERPA (http://studentprivacy.ed.gov?src=rn)
- FAFSA (https://fafsa.gov/?src=edgov-rn)
- 1098, tax forms (https://www.ed.gov/1098-e?src=rn)

More > (/about/top-tasks.html?src=rn)

Information About...

- Elevating Teaching (https://www.ed.gov/teaching?src=rn)
- Early Learning (/about/inits/ed/earlylearning/index.html?src=rn)
- Engage Every Student (https://www.ed.gov/ost?src=rn)
- Unlocking Career Success (https://cte.ed.gov/unlocking-career-success/)
- Cybersecurity (https://tech.ed.gov/cyberhelp/)

Student Loans

(/fund/grants-college.html?src=ft)

Repaying Loans (https://studentaid.gov/manage-loans/repayment?src=ft)

Defaulted Loans (https://studentaid.gov/manage-loans/default?src=ft)

Loan Forgiveness (https://studentaid.gov/manage-loans/forgiveness-cancellation?src=ft)

Loan Servicers (https://studentaid.gov/manage-loans/repayment/servicers?src=ft#who-is-my-loan-servicer)

Grants & Programs

(/fund/grants-apply.html?src=ft)

PPRA

34 CFR PART 98—PROTECTION OF PUPIL RIGHTS AMENDMENT

Below are the regulations at 34 CFR Part 98 implementing section 445 of the General Education Provisions Act (GEPA)(20 U.S.C. 1232h), which is commonly referred to as the Protection of Pupil Rights Amendment (PPRA). These regulations can also be found at the Electronic Code of Federal Regulations: Title 34, Part 98--Protection of Pupil Rights Amendment (https://www.ecfr.gov/cgi-bin/text-idx?SID=c372efef49f7659ea9397da901b0ab0a&mc=true&node=pt34.1.98&rgn=div5).

Since the enactment of these regulations in September 1984, there have been significant amendments to section 445 of GEPA by the *No Child Left Behind Act of 2001* (NCLB) passed in 2002, Pub. L. 107-110, and by *Goals 2000: Educate America Act*, Pub. L. 103-227, passed in 1994. The regulations do not reflect these most recent amendments to PPRA, and certain provisions in the current regulations are superseded by these statutory amendments. The current statute can be found at https://www.govinfo.gov/content/pkg/USCODE-2010-title20/pdf/USCODE-2010-title20-chap31-subchapIII-part4-sec1232h.pdf (https://www.govinfo.gov/content/pkg/USCODE-2010-title20/pdf/USCODE-2010-title20-chap31-subchapIII-part4-sec1232h.pdf)

To learn more about PPRA, please refer to the PPRA General Guidance (https://studentprivacy.ed.gov/resources/protection-pupil-rights-amendment-ppra-general-guidance).

Parents and eligible students who wish to file a complaint under PPRA may do so on the File a Complaint (https://studentprivacy.ed.gov/file-a-complaint) page.

Contents

Back to Top

§98.1 Applicability of part.

This part applies to any program administered by the Secretary of Education that:

(a)(1) Was transferred to the Department by the Department of Education Organization Act (DEOA); and

(2) Was administered by the Education Division of the Department of Health, Education, and Welfare on the day before the effective date of the DEOA; or

(b) Was enacted after the effective date of the DEOA, unless the law enacting the new Federal program has the effect of making section 439 of the General Education Provisions Act inapplicable.

(c) The following chart lists the funded programs to which part 98 does not apply as of February 16, 1984.

Name of program	Authorizing statute	Implementing regulations
1. High School Equivalency Program and College Assistance Migrant Program	Section 418A of the Higher Education Act of 1965 as amended by the Education Amendments of 1980 (Pub. L. 96-374) 20 U.S.C. 1070d-2)	part 206.
2. Programs administered by the Commissioner of the Rehabilitative Services Administration	The Rehabilitation Act of 1973 as amended by Pub. L. 95-602 (29 U.S.C. 700, et seq.)	parts 351-356, 361, 362, 365, 366, 369-375, 378, 379, 385-390, and 395.
3. College housing	Title IV of the Housing Act of 1950 as amended (12 U.S.C. 1749, et seq.)	part 614.

(Authority: 20 U.S.C. 1221e-3(a)(1), 1230, 1232h, 3487, 3507)

return arrow Back to Top

§98.2 Definitions.

(a) The following terms used in this part are defined in 34 CFR part 77; "Department," "Recipient," "Secretary."

(b) The following definitions apply to this part:

Act means the General Education Provisions Act.

Office means the information and investigation office specified in §98.5.

(Authority: 20 U.S.C. 1221e-3(a)(1))

return arrow Back to Top

§98.3 Access to instructional material used in a research or experimentation program.

(a) All instructional material—including teachers' manuals, films, tapes, or other supplementary instructional material—which will be used in connection with any research or experimentation program or project shall be available for inspection by the parents or guardians of the children engaged in such program or project.

(b) For the purpose of this part research or experimentation program or project means any program or project in any program under §98.1 (a) or (b) that is designed to explore or develop new or unproven teaching methods or techniques.

(c) For the purpose of the section children means persons not above age 21 who are enrolled in a program under §98.1 (a) or (b) not above the elementary or secondary education level, as determined under State law.

(Authority: 20 U.S.C. 1221e-3(a)(1), 1232h(a))

return arrow Back to Top

§98.4 Protection of students' privacy in examination, testing, or treatment.

(a) No student shall be required, as part of any program specified in §98.1 (a) or (b), to submit without prior consent to psychiatric examination, testing, or treatment, or psychological examination, testing, or treatment, in which the primary purpose is to reveal information concerning one or more of the following:

(1) Political affiliations;

(2) Mental and psychological problems potentially embarrassing to the student or his or her family;

(3) Sex behavior and attitudes;

(4) Illegal, anti-social, self-incriminating and demeaning behavior;

(5) Critical appraisals of other individuals with whom the student has close family relationships;

(6) Legally recognized privileged and analogous relationships, such as those of lawyers, physicians, and ministers; or

(7) Income, other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under a program.

(b) As used in paragraph (a) of this section, prior consent means:

(1) Prior consent of the student, if the student is an adult or emancipated minor; or

(2) Prior written consent of the parent or guardian, if the student is an unemancipated minor.

(c) As used in paragraph (a) of this section:

(1) Psychiatric or psychological examination or test means a method of obtaining information, including a group activity, that is not directly related to academic instruction and that is designed to elicit information about attitudes, habits, traits, opinions, beliefs or feelings; and

(2) Psychiatric or psychological treatment means an activity involving the planned, systematic use of methods or techniques that are not directly related to academic instruction and that is designed to affect behavioral, emotional, or attitudinal characteristics of an individual or group.

(Authority: 20 U.S.C. 1232h(b))

return arrow Back to Top

§98.5 Information and investigation office.

(a) The Secretary has designated an office to provide information about the requirements of section 439 of the Act, and to investigate, process, and review complaints that may be filed concerning alleged violations of the provisions of the section.

(b) The following is the name and address of the office designated under paragraph (a) of this section: Family Educational Rights and Privacy Act Office, U.S. Department of Education, 400 Maryland Avenue, SW., Washington, DC 20202.

(Authority: 20 U.S.C. 1231e-3(a)(1), 1232h)

return arrow Back to Top

§98.6 Reports.

The Secretary may require the recipient to submit reports containing information necessary to resolve complaints under section 439 of the Act and the regulations in this part.

(Authority: 20 U.S.C. 1221e-3(a)(1), 1232h)

return arrow Back to Top

§98.7 Filing a complaint.

(a) Only a student or a parent or guardian of a student directly affected by a violation under Section 439 of the Act may file a complaint under this part. The complaint must be submitted in writing to the Office.

(b) The complaint filed under paragraph (a) of this section must—

(1) Contain specific allegations of fact giving reasonable cause to believe that a violation of either §98.3 or §98.4 exists; and

(2) Include evidence of attempted resolution of the complaint at the local level (and at the State level if a State complaint resolution process exists), including the names of local and State officials contacted and significant dates in the attempted resolution process.

(c) The Office investigates each complaint which the Office receives that meets the requirements of this section to determine whether the recipient or contractor failed to comply with the provisions of section 439 of the Act.

(Approved by the Office of Management and Budget under control number 1880-0507)

(Authority: 20 U.S.C. 1221e-3(a)(1), 1232h)

return arrow Back to Top

§98.8 Notice of the complaint.

(a) If the Office receives a complaint that meets the requirements of §98.7, it provides written notification to the complainant and the recipient or contractor against which the violation has been alleged that the complaint has been received.

(b) The notice to the recipient or contractor under paragraph (a) of this section must:

(1) Include the substance of the alleged violation; and

(2) Inform the recipient or contractor that the Office will investigate the complaint and that the recipient or contractor may submit a written response to the complaint.

(Authority: 20 U.S.C. 1221e-3(A)(1), 1232h)

return arrow Back to Top

§98.9 Investigation and findings.

(a) The Office may permit the parties to submit further written or oral arguments or information.

(b) Following its investigations, the Office provides to the complainant and recipient or contractor written notice of its findings and the basis for its findings.

(c) If the Office finds that the recipient or contractor has not complied with section 439 of the Act, the Office includes in its notice under paragraph (b) of this section:

(1) A statement of the specific steps that the Secretary recommends the recipient or contractor take to comply; and

(2) Provides a reasonable period of time, given all of the circumstances of the case, during which the recipient or contractor may comply voluntarily.

(Authority: 20 U.S.C. 1221e-3(a)(1), 1232h)

return arrow Back to Top

§98.10 Enforcement of the findings.

(a) If the recipient or contractor does not comply during the period of time set under §98.9(c), the Secretary may either:

(1) For a recipient, take an action authorized under 34 CFR part 78, including:

(i) Issuing a notice of intent to terminate funds under 34 CFR 78.21;

(ii) Issuing a notice to withhold funds under 34 CFR 78.21, 200.94(b), or 298.45(b), depending upon the applicable program under which the notice is issued; or

(iii) Issuing a notice to cease and desist under 34 CFR 78.31, 200.94(c) or 298.45(c), depending upon the program under which the notice is issued; or

(2) For a contractor, direct the contracting officer to take an appropriate action authorized under the Federal Acquisition Regulations, including either:

(i) Issuing a notice to suspend operations under 48 CFR 12.5; or

(ii) Issuing a notice to terminate for default, either in whole or in part under 48 CFR 49.102.

(b) If, after an investigation under §98.9, the Secretary finds that a recipient or contractor has complied voluntarily with section 439 of the Act, the Secretary provides the complainant and the recipient or contractor written notice of the decision and the basis for the decision.

(Authority: 20 U.S.C. 1221e-3(a)(1), 1232h)

Back to Top