

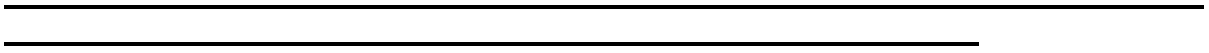
Attachment S
PARENTS' BILL OF RIGHTS
FOR DATA PRIVACY AND SECURITY

To satisfy their responsibilities regarding the provision of education to students in pre-kindergarten through grade twelve, “educational agencies” (as defined below) in the State of New York collect and maintain certain personally identifiable information from the education records of their students. As part of the Common Core Implementation Reform Act, Education Law §2-d requires that each educational agency in the State of New York must develop a Parents’ Bill of Rights for Data Privacy and Security (Parents’ Bill of Rights). The Parents’ Bill of Rights must be published on the website of each educational agency, and must be included with every contract the educational agency enters into with a “third party contractor” (as defined below) where the third party contractor receives student data, or certain protected teacher/principal data related to Annual Professional Performance Reviews that is designated as confidential pursuant to Education Law §3012-c (“APPR data”).

The purpose of the Parents’ Bill of Rights is to inform parents (which also include legal

data, and NYSED make amendments to school or school district records. Schools and school districts are in the best position to make corrections to students' education records.

3. The right to provide written consent before the school discloses personally identifiable information (PII) from the student's education records, except to the extent that FERPA authorizes disclosure without consent (including but not limited to disclosure under specified conditions to: (i) school officials within the school or school district with legitimate educational interests; (ii) officials of another school for purposes of 5 2.(o ())(4.)-Tj3EMC /LBody <</MCID 4 >>BDC (c)4 (11.75n7 (e)4 W)41 (TJ-2 (n)2 (e)-1 (t)



can be accessed at <http://www.dos.ny.gov/coog/shldno1.html>. The Committee on Open Government's address is Committee on Open Government, Department of State, One Commerce Plaza, 99 Washington Avenue, suite 650, Albany, NY 12231, their email address is coog@dos.ny.gov, and their telephone number is (518) 474-2518.

C. Parents' Rights Under Education Law §2-d relating to Unauthorized Release of Personally Identifiable Information

1.

have personal knowledge of the relevant circumstances, to identify the student with

that he or she is in fact the student's parent and is authorized to receive such information pursuant to law.

- (C) State and federal laws protect the confidentiality of PII, 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.

Education Law §2-d also specifically provides certain limitations on the collection of data by educational agencies, including, but not limited to:

- o (not applicable) ~~At a minimum, all data collected by a school district shall only collect PII relating to an educational purpose;~~ (NYSED shall only collect PII relating to an educational purpose;)



When an educational agency enters into a contract with a third party contractor, under which the third party contractor will receive student data, the contract or agreement must include a data security and privacy plan that outlines how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the educational agency's policy on data security and privacy. However, the standards for an educational agency's policy on data security and privacy must be prescribed in Regulations of the Commissioner that have not yet been promulgated. A signed copy of the Parents' Bill of Rights must be included, as well as a requirement that any officers or employees of the third party contractor and its assignees

agency of the breach in the most expedient way possible and without unreasonable delay; (ii) the educational agency must notify the parent in the most expedient way possible and without unreasonable

—

ATTACHMENT

Model Notification of Rights under FERPA for Elementary and Secondary Schools

The Family Educational Rights and Privacy Act (FERPA) affords parents and students who are 18 years of age or older ("eligible students") certain rights with respect to the student's education records. These rights are:

1. The right to inspect and review the student's education records within 45 days after the day the [Name of school ("School")] receives a request for access.

Parents or eligible students should submit to the school principal [or appropriate school official] a written request that identifies the records they wish to inspect. The school official will make arrangements for access and notify the parent or eligible student of the time and place where the records may be inspected.

2. The right to request the amendment of the student's education records that the parent or eligible student believes are inaccurate, misleading, or otherwise in violation of the student's privacy rights under FERPA.

Parents or eligible students who wish to ask the [School] to amend a record11 (r)-1 (e)-10 (cl(cl(diin)

[Optional] Upon request, the school discloses education records without consent to officials of another school district in which a student seeks or intends to enroll, or is already enrolled if the disclosure is for purposes of the student's enrollment or transfer. [NOTE: FERPA requires a school district to make a reasonable attempt to notify the parent or student of the records request unless it states in its annual notification that it intends to forward records on request.]

4. The right to file a complaint with the U.S. Department of Education concerning alleged failures by the [School] to comply with the requirements of FERPA. The

programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs. These entities may make further disclosures of PII to outside entities that are designated by them as their authorized representatives to conduct any audit, evaluation, or enforcement or compliance activity on their behalf. (§§99.31(a)(3) and 99.35)

In connection with financial aid for which the student has applied or which the student has received, if the information is necessary to determine eligibility for the aid, determine the amount of the aid, determine the conditions of the aid, or enforce the terms and conditions of the aid. (§99.31(a)(4))

To State and local officials or authorities to whom information is specifically allowed to be reported or disclosed by a State statute that concerns the juvenile justice system and the system's ability to effectively serve, prior to adjudication, the student whose records were released, subject to §99.38. (§99.31(a)(5))

To organizations conducting studies for, or on behalf of, the school, in order to: (a) develop, validate, or administer predictive tests; (b) administer student aid programs; or (c) improve instruction. (§99.31(a)(6))

To accrediting organizations to carry out their accrediting functions. (§99.31(a)(7))

To parents of an eligible student if the student is a dependent for IRS tax purposes. (§99.31(a)(8))

To comply with a judicial order or lawfully issued subpoena. (§99.31(a)(9))

To appropriate officials in connection with a health or safety emergency, subject to §99.36. (§99.31(a)(10))

Information the school has designated as "directory information" under §99.37. (§99.31(a)(11))

Attachment to Parents' Bill Of Rights
Regarding Disclosure of Certain Personally Identifiable
Information

Attachment
For Contracts Involving

added by Ch. 56 of the Laws of 2014 requires that a Parents' Bill of Rights Education Law 82-d
be attached to every contract with a third-party contractor (as defined in the law) which involves the
disclosure of personally identifiable information (PII) derived from student education
records of Student Data); or certain teacher/principal information regarding annual professional perform
ance evaluations that is confidential pursuant to Education Law 8302(12-c) ("APPR Data"). Each such Contr
act must include this completed Attachment to provide speci
information about the use of such data by the contractor.

Specify whether this contract involves disclosure to the contractor of Student Data
both.

Disclosure of Student Data

Disclosure of APPR Data

Describe the exclusive purposes for which the Student Data or APPR Data will be used in the performance of this contract.

Students (ages 14-21) per year and collect demographic data such as Vendor will identify the
services (Pre-ETS services) received; and any other elements deemed employment transiti

Attachment R

By the expiration date of the Contract, and explain what will happen to the Student Data or APPR Data in the contractor's possession or the possession of any other person/entity described in response to Paragraph 4 upon the expiration or earlier termination of the Contract.

Contract expiration date: 9/30/25

Contractor agrees to retain the Student Data or APPR Data in NYSED consistent with the protocols set forth in Paragraph 4 of the Data Security and Privacy Plan set forth in Attachment R.

Contractor agrees to securely destroy the Student Data or APPR Data consistent with the protocols set forth in Paragraph 4 of the Data Security and Privacy Plan set forth in Attachment R.

Whether the Contractor will be collecting any data from or pertaining to students derived from the student's education record, or pertaining to teachers or principals' annual professional performance evaluation, or any other data, and if so, the Contractor shall ensure that the principal may challenge the accuracy of the Student Data or APPR data that is collected. *ISSEY program office checks appropriate boxes.*

Student Data
 APPR Data
to the accuracy of any of the Student Data or APPR Data shared pursuant to this Contract should be addressed to the school, educational agency or entity which produced, generated or otherwise created such data.

6. Describe where the Student Data or APPR Data will be stored (in a manner that does not jeopardize the security of the data) and the security protections taken to ensure that the data will be protected, including whether such data will be encrypted.

DOE stores on internal server. DOE data centers are state-of-the-art provisioning and de-provisioning technology to ensure that only authorized personnel are provided access. All unauthorized access or download is subject to our defined Security Incident Response Process (SIRP). This includes notification of DOE executives and appropriate notification of law enforcement where necessary and in compliance with applicable laws and regulations.