# SEXUAL HARRASSMENT GRIEVANCES UNDER TITLE IX

Under federal regulations implementing Title IX, sexual harassment means conduct on the basis of sex that satisfies one or more of the following:

1. A district employee conditioning the provision of an aid, benefit, or service of the district on an individual's participation in unwelcome sexual conduct;
2. Unwelcome conduct determined by a reasonable person to be so severe, pervasive, and objectively offensive that it effectively denies a person equal access to the district's education program or activity; or
3. "Sexual assault" as defined in 20 U.S.C. 1092(f)(6)(A)(v), "dating violence" as defined in 34 U.S.C. 12291(a)(10), "domestic violence" as defined in 34 U.S.C. 12291(a)(8), or "stalking" as defined in 34 U.S.C. 12291(a)(30).

Federal Title IX regulations only address complaints of discrimination or harassment occurring against a person in the United States.

If contacted by a person alleging sexual harassment under Title IX, the Title IX Coordinator will explain the process for filing a formal complaint, which initiates an investigation into the Title IX sexual harassment allegations.

If any district employee is notified of alleged sexual harassment, they must inform the Title IX Coordinator.

Complaints of discrimination on the basis of sex under federal Title IX regulations are addressed in the manner provided by policy 0100, Non-Discrimination and Equal Opportunity. If alleged discrimination or sexual harassment is not covered by Title IX regulations, it may be covered by state laws, addressed in district policies 0100, Non-Discrimination and Equal Opportunity; 0110.2, Sexual Harassment in the Workplace; 0115, Student Harassment and Bullying Prevention and Intervention; and 5300, Code of Conduct.

## Supportive Measures

Once the district has notice of sexual harassment or allegations of sexual harassment, the Title IX Coordinator will promptly contact the complainant of sexual harassment under Title IX and discuss the availability of supportive measures regardless of whether the complainant chooses to file a formal complaint under Title IX or not. Potential supportive measures offered to both complainants and respondents include:

- Counseling,
- Extensions of deadlines or other course-related adjustments,
- Modifications of work or class schedules,
- Campus escort services,
- Mutual restrictions on contact between the parties,
- Changes in work locations,

- Leaves of absence,
- Increased security and monitoring of certain areas.

The Title IX coordinator will discuss and determine the complainant's wishes with respect to supportive measures.

**Formal Complaints**

A formal complaint is a document filed by a complainant or signed by the Title IX Coordinator alleging sexual harassment under Title IX against an individual and requesting that the district investigate the allegation of sexual harassment under Title IX. The formal complaint must be a written document but need not be in any specific form. At the time a formal complaint is filed, the complainant must be participating or attempting to participate in the district's education program or activity.

The formal complaint investigation and process will only be triggered when the complainant files a formal complaint of sexual harassment under Title IX.

The district will investigate the complaint and make determinations regarding a complaint's allegations using a preponderance of evidence standard.

The Title IX Coordinator, investigator, decision-maker or facilitator of an informal resolution process, if applicable, must not have a conflict of interest or bias for or against complainants or respondents. All individuals with conflicts of interest or bias must recuse themselves.

The roles of Title IX Coordinator and investigator will be the Director of HR, and the decision-maker will be the Assistant Superintendent for PPS.

**District Responsibilities**

Throughout the Title IX process the district will, among other things:

- Treat complainants and respondents equitably.
- Perform an objective evaluation of all available evidence.
- Presume that the respondent is not responsible for the alleged conduct until a determination regarding responsibility is made at the conclusion of the grievance process.
- Ensure that no information protected by a legal privilege such as the attorney-client privilege may be used for any purpose or be sought through disclosure unless the person holding the privilege has waived such privilege.

**Timeframes**

- *Written notice of a formal complaint to known parties will be given approximately three (3) calendar days following receipt of a complaint.*

- *Investigations of complaints will begin approximately five (5) calendar days following receipt of a complaint.*
- *Determinations will be made approximately fourteen (14) calendar days following starting an investigation.*
- *Informal resolution will begin approximately seven (7) calendar days following acceptance of both parties in writing, and will conclude in approximately thirty (30) calendar days.*

The district has established reasonably prompt approximate time frames for the conclusion of the grievance process and informal resolution process, unless delayed or extended. The time frames for appeals are set forth in the section below on Appeals.

The district has also established a process that allows for a temporary delay or limited extension of timeframes for good cause with notice to the parties that includes the reason for the delay.

- Good cause may include considerations such as the absence of a party, a party's advisor, or a witness; concurrent law enforcement activity; or the need for language assistance or accommodation of disabilities.
- The Title IX Coordinator will evaluate the request for an extension of timeframes and make a prompt determination to either extend the timeframes, or take or recommend other action to be able to meet the timeframes.
- If an extension is granted, the Title IX Coordinator will notify the parties in writing of the reason(s) for the delay, and the estimated date the stages in the timeframe will be complete.

**Notice**

Upon receipt of a formal complaint of sexual harassment under Title IX, the district will provide written notice to the complainant and respondent(s) in sufficient time to allow the parties who are known to prepare a response before an initial interview.

The notice to the complainant and respondent will include, among other items:

- Information regarding the grievance process and the informal resolution process.
- The conduct allegedly constituting sexual harassment under Title IX, and if known, the identities of the parties involved in the incident, as well as the date and location of the alleged incident.
- A statement that the respondent is presumed not responsible for the alleged conduct until a determination regarding responsibility is made at the conclusion of the grievance process.
- Notification that the parties may inspect and review evidence.

- Policies regarding knowingly making false statements or submitting false information during the grievance process.
- Notification that after commencing an investigation of a formal complaint, the district may decide to also investigate allegations that were not included in the initial notice to the parties. In that case, the district will provide notice of the additional allegations to the parties.

In lieu of resolving a formal complaint through the district's Title IX grievance procedures, at any time prior to reaching a determination of responsibility, the parties may instead elect to participate in a district-facilitated informal resolution process such as mediation, which does not involve a full investigation and determination. The district will obtain the parties' voluntary written consent to the informal resolution process. Informal resolution is not available to resolve a complaint that includes allegations that an employee engaged in sex-based harassment of an elementary school or secondary school student, or when such a process would conflict with Federal, State, or local law.

The district will provide the parties with a written notice of:

- The allegations.
- The requirements of the informal resolution process.
- That at any time prior to agreeing to a resolution, any party has the right to withdraw from the informal resolution process and resume the formal complaint grievance process.
- Any consequences that result from participation in informal resolution, including records that will be maintained or could be shared.

**Investigations**

Upon receipt of a formal complaint of sexual harassment under Title IX, the Title IX Coordinator will assign an investigator. The assigned harassment investigator will:

- Gather additional information through interviews of the complainant, respondent, and witnesses and synthesize the information in a report.
- The investigator has the discretion to determine the relevance of any witness or other evidence and may exclude information in preparing the investigation report if the information is irrelevant, immaterial, or more prejudicial than informative.
- Produce a written report that contains the relevant information and facts learned during the investigation, and may include direct observations and reasonable inferences drawn from the facts and any consistencies or inconsistencies between the various sources of information. The investigator may exclude statements of personal opinion by witnesses and statements as to general reputation for any character trait, including honesty. The investigator will not make a finding or recommended finding of responsibility. The investigator's report will include credibility assessments

based on their experience with the complainant, respondent, and witnesses, as well as the evidence provided.
- The investigator's written report will be provided to both parties and their representatives, if any.

During the formal complaints process, the parties will have an equal opportunity to:

- Present witnesses and to gather and present relevant evidence.
- Have others present during any grievance proceeding, including the representative of their choice who may be, but is not required to be, an attorney.
- Inspect and review all evidence obtained as part of the investigation that is directly related to the allegations in the complaint and respond to the evidence prior to the conclusion of the investigation. Parties must be given at least ten (10) calendar days to submit a written response that the investigator will consider prior to completing the investigative report.

**Dismissal**

The district must dismiss a formal complaint when the conduct alleged in the formal complaint of sexual harassment under Title IX:

- Would not constitute sexual harassment under Title IX even if proved; or
- Did not occur in the district's education program or activity; or
- Did not occur against a person in the United States.

Such a dismissal does not preclude action under another provision of the district's code of conduct, or another policy adopted pursuant to state law.

The district may dismiss a formal complaint when:

- A complainant notifies the Title IX Coordinator in writing that they would like to withdraw the formal complaint or any of its allegations; or
- The respondent is no longer enrolled or employed by the district; or
- Specific circumstances prevent the district from gathering enough evidence to reach a determination on the formal complaint or its allegations.

If a complaint is dismissed, the decision-maker will send written notice of the dismissal and reason(s) therefore simultaneously to the parties

**Questions**

Prior to issuing a written determination, the decision-maker(s) will afford each party the opportunity to submit written, relevant questions that a party wants to ask of any party or witness, provide each party with the answers, and allow for additional, limited follow-up questions from each party. Questions and evidence about the complainant's sexual predisposition or prior sexual behavior are not relevant, unless

such questions and evidence about the complainant's prior sexual behavior are offered to prove that someone other than the respondent committed the conduct alleged by the complainant, or if the questions and evidence concern specific incidents of the complainant's prior sexual behavior with respect to the respondent and are offered to prove consent. The decision-maker(s) must explain to the party proposing the questions any decision to exclude a question as not relevant.

**Determinations**

Following the question-and-answer process and upon receipt of the investigative report, the decision-maker will issue a written determination. The decision-maker's written determination will address:

- The allegations,
- The procedural steps taken in the case at hand,
- The findings of fact,
- The applicability of code of conduct and local rules to the facts, and
- The result with corresponding rationale for each addressed allegation, including a determination of responsibility, disciplinary sanctions, and whether remedies to restore or preserve access will be provided.

**Disciplinary Sanctions and Remedies**

If the district determines responsibility for sexual harassment, if the decision is not appealed, or if the appeal is dismissed, the district will impose disciplinary sanctions, which may include, but not limited to:

- Student respondents: consequences may include warning, reprimand, detention, in-school suspension, and suspension from school, to be imposed consistent with the district's Code of Conduct and applicable law
- Employee respondents: consequences may include warning, reprimand, mandatory counseling, re-assignment, demotion, suspension, and termination, to be imposed consistently with all applicable contractual and statutory rights.
- Volunteer respondents: consequences may include warning, reprimand, loss of volunteer assignments, and removal from future volunteer opportunities.
- Vendor respondents: consequences may include warning, removal from school property, denial of future access to school property, and denial of future business with the district.
- Other individuals: consequences may include warning, removal from school property, and denial of future access to school property.

The Title IX Coordinator will facilitate the transfer of information and determinations from the Title IX complaint process to the appropriate administrator, to aid in the imposition of disciplinary consequences.

The district may also provide or facilitate remedies, which may include, but not limited to:

- Training of individuals or entire departments, classes, or groups;
- Peer support groups;
- Letters of apology;
- Separation of the parties;
- Additional supervision or mentoring for the respondent; and
- Restitution and restoration.

## Appeals

Following a decision-makers written determination, either party may appeal the written determination or dismissal of the complaint.

An appeal must be submitted to the Title IX Coordinator within seven (7) calendar days of receipt of the determination or dismissal (as applicable) and must identify all information a party wishes to have considered on appeal. Any appeal statement will be shared with the other party, who will have two (2) calendar days to submit a response to the Title IX Coordinator. The appeal and any response will be considered by a decision-maker other than the decision-maker who issued the determination or dismissal that is being appealed.

Grounds for an appeal are limited to the following:

- Procedural irregularity that affected the outcome of the matter; and/or
- New evidence that was not reasonably available at the time determination regarding responsibility or dismissal was made, that could affect the outcome of the matter; and/or
- The Title IX Coordinator, investigator(s), or any decision-maker had a conflict of interest or bias for or against Complainants or Respondents generally or the individual Complainant or Respondent that affected the outcome of the matter; and/or
- The sanction is inappropriate.

A decision responding to the written appeal will be issued to the parties and the Title IX Coordinator within thirty (30) calendar days.

Cross-ref:
0100, Non-Discrimination and Equal Opportunity
0110.2, Sexual Harassment in the Workplace
0115, Student Harassment and Bullying Prevention and Intervention
5300, Code of Conduct

Ref:
20 USC §§1681 et seq.
34 CFR Part 106
First Reading: September 10, 2024
Adoption Date: September 24, 2024
First Reading: September 9, 2025
Adoption date: September 30, 2025

AGENDA ITEM

## HARASSMENT GRIEVANCES UNDER TITLE IX EXIBIT - DEFINITIONS

Definitions of the following terms are based on the federal regulations implementing Title IX (34 CFR §106.2):

*Complainant* means an individual who is alleged to be the victim of conduct that could constitute sexual harassment.

*Formal complaint* means a document filed by a complainant or signed by the Title IX Coordinator alleging sexual harassment against a respondent and requesting that the district investigate the allegation of sexual harassment. At the time of filing a formal complaint, a complainant must be participating in or attempting to participate in the education program or activity of the district with which the formal complaint is filed.

*Respondent* means an individual who has been reported to be the perpetrator of conduct that could constitute sexual harassment.

*Retaliation* means intimidation, threats, coercion, or discrimination against any individual for the purpose of interfering with any right or privilege secured by title IX or this part, or because the individual has made a report or complaint, testified, assisted, or participated or refused to participate in any manner in an investigation, proceeding, or hearing under Title IX regulations.

*Sexual harassment* means conduct on the basis of sex that satisfies one or more of the following:

1. An employee of the district conditioning the provision of an aid, benefit, or service of the district on an individual's participation in unwelcome sexual conduct;
2. Unwelcome conduct determined by a reasonable person to be so severe, pervasive, and objectively offensive that it effectively denies a person equal access to the district's education program or activity; or
3. "Sexual assault" as defined in 20 U.S.C. 1092(f)(6)(A)(v), "dating violence" as defined in 34 U.S.C. 12291(a)(10), "domestic violence" as defined in 34 U.S.C. 12291(a)(8), or "stalking" as defined in 34 U.S.C. 12291(a)(30).

*Supportive measures* means non-disciplinary, non-punitive individualized services offered as appropriate, as reasonably available, and without fee or charge to the complainant or the respondent before or after the filing of a formal complaint or where no formal complaint has been filed. Such measures are designed to restore or preserve equal access to the district's education program or activity without unreasonably burdening the other party, including measures designed to protect the safety of all parties or the district's educational environment, or deter sexual harassment.

First Reading: September 10, 2024
Adoption Date: September 24, 2024
First Reading: September 9, 2025
Adoption Date: September 30, 2025

# STUDENT RECORDS

The Board of Education recognizes its legal responsibility to maintain the confidentiality of student records. As part of this responsibility, the Board will ensure that eligible students and parents/guardians have the right to inspect and review education records, the right to seek to amend education records and the right to have some control over the disclosure of information from the education record. The procedures for ensuring these rights shall be consistent with state and federal law, including the Family Educational Rights and Privacy Act of 1974 (FERPA) and its implementing regulations.

The Board also recognizes its responsibility to ensure the orderly retention and disposition of the district's student records in accordance with Schedule ED-1 as adopted by the Board in policy 1120.

The District will use reasonable methods to provide access to student educational records only to those authorized under the law and to authenticate the identity of the requestor. The district will document requests for and release of records, and retain the documentation in accordance with law. Furthermore, pursuant to Education Law §2-d ("§2-d") and its implementing regulations 8 NYCRR Part 121 ("Part 121"), the district will execute agreements with third-party contractors who collect, process, store, organize, manage or analyze student personally identifiable information (PII) to ensure that the contractors comply with the law in using appropriate means to safeguard the data.

Additionally, pursuant to §2-d and Part 121 the district will only use or disclose student personally identifiable information (including directory information described below) if it benefits students and the district (e.g., improves academic achievement, empowers parents and students with information, and/or advances efficient and effective school operations), except for disclosure required by federal law of the names, addresses and telephone numbers of secondary students to the military and institutions of higher education.

The Superintendent of Schools shall be responsible for ensuring that all requirements under federal statutes and Commissioner's Regulations shall be carried out by the district.

Definitions

*Authorized Representative:* an authorized representative is any individual or entity designated by a State or local educational authority or a Federal agency headed by the Secretary, the Comptroller General or the Attorney General to carry out audits, evaluations, or enforcement or compliance activities relating to educational programs.

*Education Record:* means those records, in any format, directly related to the student and maintained by the district or by a party acting on behalf of the district, except:

(a) records in the sole possession of the individual who made it and not accessible or revealed to any other person except a substitute (e.g. memory joggers);
(b) records of the district's law enforcement unit;
(c) grades on peer-graded papers before they are collected and recorded by a teacher.

*Eligible student:* a student who has reached the age of 18 or is attending postsecondary school.

*Legitimate educational interest*: a school official has a legitimate educational interest if they need to review a student's record in order to fulfill his or her professional responsibilities.

*Personally identifiable information:* is information that alone or in combination, would allow a reasonable person in the school or its community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty. Such data includes, but is not limited to, a student's: name, address, date and place of birth, mother's maiden name, family member's name and address, social security number, student identification number, a biometric record, etc. This term is fully defined in federal regulations at 34 CFR section 99.3. The State Chief Privacy Officer has determined that student and parent phone numbers are considered PII.

*School official*: a person who has a legitimate education interest in a student record who is employed by the district as an administrator, supervisor, instructor or support staff member (including health or medical staff and law enforcement unit personnel); a member of the Board of Education; a person or company with whom the district has contracted to perform a special task (such as attorney, auditor, medical consultant or therapist); or a parent or student serving on an official committee, such as disciplinary or grievance committee, or assisting another school official performing his or her tasks. Volunteers may only access the information necessary for an assignment and must not disclose student information to anyone other than a school official with a legitimate educational interest. The Building Principal shall provide adequate training on confidentiality of student records.

*Third party contractor:* is 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 or audit or evaluation of publicly funded programs.

*Annual Notification*

At the beginning of each school year, the district will publish a notification that informs parents, guardians and students currently in attendance of their rights under

FERPA and New York State Law and the procedures for exercising those rights. ~~A 'Parents' Bill of Rights for Data Privacy and Security' will be posted on the district website and included in any agreements with third-party contractors.(see 5500-E.4)~~ The notice ~~and 'Bill of Rights~~s' may be published in a newspaper, handbook or other school bulletin or publication. The notice ~~and 'Bill of Rights'~~ will also be provided to parents, guardians, and students who enroll during the school year.

The notice ~~and Parents' Bill of Rights~~ must include a statement that the parent or eligible student has a right to:

1. inspect and review the student's education records;
2. request that records be amended to ensure that they are not inaccurate, misleading, or otherwise in violation of the student's privacy or other rights;
3. consent to the disclosure of personally identifiable information contained in the student's educational records, except to the extent that FERPA authorizes disclosure without consent; and
4. file a complaint with the U.S. Department of Education alleging failure of the district to comply with FERPA and its regulations.~~; and/or file a complaint regarding a possible data breach by a third-party contractor with the district and/or the New York State Education Department's Chief Privacy officer for failure to comply with state law.~~

The annual notice ~~and Parents' Bill of Rights~~ will inform parents/guardians and students:

1. that it is the district's policy to disclose personally identifiable information from student records, without consent, to other school officials within the district whom the district has determined to have legitimate educational interests. The notice will define 'school official' and 'legitimate educational interest.'
2. that, upon request, the district will disclose education records without consent to officials of another school district in which a student seeks to or intends to enroll or is actually enrolled.
3. that personally identifiable information will be released to third party authorized representatives for the purposes of educational program audit, evaluation, enforcement or compliance purposes.
4. that the district, at its discretion, releases directory information (see definition below) without prior consent, unless the parent/guardian or eligible student has exercised their right to prohibit release of the information without prior written consent. The district will not sell directory information.
5. that, upon request, the district will disclose a high school student's name, address and telephone number to military recruiters and institutions of higher learning unless the parent or secondary school student exercises their right to prohibit release of the information without prior written consent.
6. of the procedure for exercising the right to inspect, review and request amendment of student records.

7. ~~that the district will provide information as a supplement to the "Parents' Bill of Rights" about third parties with which the district contracts that use or have access to personally identifiable student data.~~

Additionally, the district will include in the annual FERPA notification either its process, or where the process is located, for parents/guardians and eligible students to file complaints about breaches or unauthorized releases of student data required by §2-d and Part 121.

The district may also release student education records, or the personally identifiable information contained within, without consent, where permitted under federal law and regulation. For a complete list of exceptions to FERPA's prior consent requirements see accompanying regulation 5500-R, Section 5.

The district shall effectively notify parents, guardians and students who have a primary or home language other than English.

In the absence of the parent or secondary school student exercising their right to opt out of the release of information to the military, the district is required to, under federal law, release the information indicated in number five (5) above.

*Directory Information*

The district has the option under FERPA of designating certain categories of student information as "directory information." The Board directs that "directory information" include a student's:

- Name
- ID number, user ID, or other unique personal identifier that is either (1) used by a student for purposes of accessing or communicating in electronic systems, or (2) displayed on a student ID badge (But in either case, only if the ID cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the student's identity),
- Address (except information about a homeless student's living situation, as described below)
- Telephone number
- Date and place of birth
- Major course of study
- Participation in school activities or sports
- Weight and height if a member of an athletic team
- Dates of attendance,
- Degrees and awards received
- Most recent school attended
- Grade level
- Photograph

- E-mail address
- Enrollment status

Information about a homeless student's living situation will be treated as a student educational record and will not be deemed directory information. A parent/guardian or eligible student may elect, but cannot be compelled, to consent to the release of a student's address information in the same way they would for other student education records. The district's McKinney-Vento liaison will take reasonable measures to provide homeless students with information on educational, employment, or other postsecondary opportunities and other beneficial activities.

Social security numbers ~~or other personally identifiable information~~ will not be considered directory information.

Students who opt out of having directory information shared are still required to carry and/or display their student ID cards.

The district will notify parents/guardians and eligible students of the types of information designated as directory information, that they have the right to object to (or "opt out" of) any or all of the district's designations for that student, and that they may notify the district at any time during the year that they opt out of a directory information designation. ~~Once the proper FERPA notification is given by the district, a parent/guardian or student will have 14 days to notify the district of any objections they have to any of the "directory information" designations. If no~~ Unless and until an objection is received, the district may release this information without prior approval of the parent/guardian or student for the release, as long as such release is permitted by §2-d and Part 121. Once the student or parent/guardian provides the "opt-out," it will remain in effect after the student is no longer enrolled in the school district.

The district may elect to provide a single notice regarding both directory information and information disclosed to military recruiters and institutions of higher education.

When considering the release of student information, including directory information, the district is required by Law §2-d and Part 121 to further protect student PII. The district will not sell PII, use or disclose PII for marketing or commercial purposes, or facilitate use of disclose by another party for marketing or commercial purposes or permit another party to do so. Any use or release of PII must conform to the requirements of §2-d and Part 121. The district will also publish a Parents Bill of Rights for Data Privacy on its website that includes the elements by law, and supplemental information for third party contractors receiving PII. See policy 8635 and regulation 8635-R for more information.

Cross-ref: 1120, School District Records
4321, Programs for Students with Disabilities Under IDEA and Part 89
4532, School Volunteers
5550, Student Privacy

5151, Homeless Children

Ref. Family Educational Rights and Privacy Act, as amended, 20 USC 1232g; 34 CFR Part 99
Elementary and Secondary Education Act, as amended, 20 USC §7908 (Military Recruiter Access)
10 USC §503 as amended by §544 of the National Defense Reauthorization Act for FY 2002
Education Law §§ 2-a; 2-b; 2-c; 2-d; 225;
Public Officers Law §87(2)(a)
Arts and Cultural Affairs Law, Article 57-A (Local Government Records Law)
8 NYCRR 185.12 (Appendix I) Records Retention and Disposition, Schedule ED-1 for Use by School Districts and BOCES
"Guidance for Reasonable Methods and Written Agreements,"
http://www2.ed.gov/policy/gen/guid/fpco/pdf/reasonablemtd_agreement.pdf
Parents' Bill of Rights for Data Privacy and Security, July 29, 2014: http://www.p12.nysed.gov/docs/parents-bill-of-rights.pdf

Adoption Date: January 22, 2008
First Reading: September 28, 2010
Adoption Date: October 12, 2010
First Reading: July 31, 2012
Adoption Date: August 28, 2012
First Reading: January 7, 2014
Adoption Date: February 11, 2014
First Reading: October 7, 2014
Adoption Date: October 21, 2014
First Reading: June 6, 2017
Adoption Date: June 20, 2017
Frist Reading: May 14, 2024
Adoption Date: May 30, 2024
First Reading: September 30, 2025

AGENDA ITEM

# STUDENT RECORDS REGULATION

It is recognized that the confidentiality of student records must be maintained. The terms used in this regulation are defined in the accompanying policy. The following necessary procedures have been adopted to protect the confidentiality of student records.

## Requirements under FERPA

Section 1 - Pursuant to the Family Educational Rights and Privacy Act (FERPA) and state law it shall be the policy of this school district to permit parents/guardians and eligible students to inspect and review any and all official records, files and data directly related to that student, including all materials that are incorporated into each student's cumulative record folder.

The rights created by FERPA and state law transfer from the parents/guardians to the student once the student attains eligible student status. However, districts can disclose information to parents of eligible students under certain circumstances, including when the student is a dependent under the IRS tax code, when the student has violated a law or the school's rules regarding alcohol or substance abuse (and the student is under 21); when the information is needed to protect the health or safety of the student or other individuals.

Section 2 - Parents/guardians or the eligible student will have an opportunity for a hearing to challenge the content of the student's school records, to insure that the records are not inaccurate, misleading, or otherwise in violation of the privacy or other rights of the student, and to provide an opportunity for the correction or deletion of any such inaccurate, misleading, or otherwise inappropriate data contained therein.

Section 3 - A letter shall be sent annually to parents/guardians of students currently in attendance and students currently in attendance informing them of their rights pursuant to FERPA and state law~~, and will include a Parents' Bill of Rights~~. See Exhibits 5500-E.1 ~~and 5500-E.4~~. The district shall provide translations of this notice, where necessary, to parents/guardians and students in their native language or dominant mode of communication.

Section 4 - To implement the rights provided for in sections 1 and 2, the following procedures are adopted:

1. A parent/guardian or an eligible student who wishes to inspect and review student records shall make a request for access to the student's school records, in writing, to the Building Principal. Upon receipt of such request, arrangements shall be made to provide access to such records within 45 days after the request has been received. If the

record to which access is sought contains information on more than one student, the parent/guardian or eligible student will be allowed to inspect and review only the specific information about the student on whose behalf access is sought.

a. Before providing access to student records, the district will verify the identity of the parent/guardian or students.

b. The district may provide the requested records to the parent/guardian or eligible students electronically, as long as the parent/guardian or eligible student consents. The district will transmit personally identifiable information (PII) electronically in a way that maintains its confidentiality, using safeguards such as encryption and password protection.

2. A parent/guardian or an eligible student who wishes to challenge the contents of the student's school records shall submit a request, in writing, to the Building Principal identifying the record or records which they believe to be inaccurate, misleading or otherwise in violation of the privacy or other rights of the student together with a statement of the reasons for their challenge to the record.

3. Upon receipt of a written challenge, the Building Principal shall provide a written response indicating either that he/she:

a. finds the challenged record inaccurate, misleading or otherwise in violation of the student's rights and that the record will be corrected or deleted; or

b. finds no basis for correcting or deleting the record in question, but that the parent/guardian or eligible student will be given an opportunity for a hearing. The written response by the Building Principal shall be provided to the parent/guardian or eligible student within 14 days after receipt of the written challenge. The response shall also outline the procedures to be followed with respect to a hearing regarding the request for amendment.

4. Within 14 days of receipt of the response from the Building Principal, a parent/guardian or eligible student may request, in writing, that a hearing be held to review the determination of the Building Principal.

5. The hearing shall be held within 10 days after the request for the hearing has been received. The hearing will be held by the Superintendent of Schools, unless the Superintendent has a direct interest in the outcome of the hearing, in which case the Superintendent will designate another individual who does not have a direct interest in the outcome of the hearing to hold the hearing.

6. The parent/guardian or eligible student shall be given a full and fair opportunity to present evidence at the hearing. The parent/guardian or eligible student may, at their own expense, be assisted or represented

by one or more individuals of his or her own choice, including an attorney.

7. The Superintendent or other individual designated by the Superintendent will make a decision in writing within 14 days after the hearing.
8. After the hearing, if the Superintendent or the individual designated by the Superintendent decides not to amend the record, the district will inform the parent/guardian or eligible student that they have the right to place a statement in the record commenting on the contested information or stating why he/she disagrees with the decision of the district. Any statement placed in the record will be maintained with the contested part of the student record for as long as the record is maintained. Further, the statement will be disclosed by the district whenever it discloses the portion of the record to which the statement relates.

Section 5 - Except to the extent that FERPA authorizes disclosure of student records without consent, student records, and any material contained therein which is personally identifiable, are confidential and will not be released or made available to persons other than parents/guardians or eligible students without the prior written consent of the parents/guardians or eligible student.

Exceptions to FERPA's prior consent requirement include, but are not limited to disclosure:

1. To other school officials within the district who have been determined to have legitimate educational interests.
2. To officials of another school, school system or post secondary institution where the student seeks or intends to enroll.
3. To authorized representatives of the Comptroller General of the United States, the U.S. Secretary of Education, the U.S. Attorney General or state and local education authorities in connection with an audit or evaluation of a federal- or state-supported education program or in compliance with legal requirements related to those programs.
4. In connection with the student's application for or receipt of financial aid.
5. To state and local officials or authorities in compliance with state law that concerns the juvenile justice system and the system's ability to effectively serve, prior to adjudication, the student whose records are being released.
6. To organizations conducting studies for, or on behalf of, education agencies or institutions, in order to develop tests, administer student aid, or improve instruction.
7. To accrediting organizations to carry out their accrediting functions.
8. To parents of a dependent student, as defined by the Internal Revenue Code.

9. To comply with a judicial order or lawfully issued subpoena, including ex parte court orders under the USA Patriot Act. Prior to complying with a judicial order or subpoena, the district will make a reasonable effort to notify the parent/guardian or eligible student, unless the district has been ordered not to disclose the existence or content of the order or subpoena, or unless the parent is the subject of a court proceeding involving child dependency or child abuse and neglect matters, and the order is issued in context of that proceeding.
10. In connection with a health or safety emergency, the district will disclose information when, taking into account the totality of circumstances, a determination is made that there is an articulable and significant threat to the health or safety of the student or other individuals.
11. To teachers and school officials in other schools who have legitimate educational interests in the behavior or the student when the information concerns disciplinary action taken against the student for conduct that posed a significant risk to the safety or well-being of that student, other students, or other members of the school community.
12. To provide information that the district has designated as "directory information."
13. To provide information from the school's law enforcement unit records.
14. To a court, when the district is involved in legal action against a parent or student, those records necessary to proceed with the legal action.
15. To the U.S. Secretary of Agriculture, its authorized representatives from the Food and Nutrition Service, or contractors acting on its behalf, to monitor, evaluate and measure performance of federally subsidized school food programs, subject to certain privacy protections.
16. To any caseworker or representative of a state or local child welfare agency or tribal organization who has the right to access a student's case plan, where the agency or organization is legally responsible for the care and protection of that student, not to be redisclosed except as permitted by law.

However, even if the district is permitted under FERPA to release student information (including directory information), state Education Law §2-d and regulations 8 NYCRR Part 121 only permit the district to use or disclose student PII if it benefits students and the district (e.g., improves academic achievement, empowers parents and students with information, and/or advances efficient and effective school operations), except for disclosure required by federal law of the names, addresses and telephone numbers of secondary students to the military and institutions of higher education. The Superintendent, the district's Data Protection Officer, and the district's attorney, if necessary will assist in determining whether complying with a request for student PII can be done in conformance with the law.

The District will use reasonable methods to provide access to student educational records to only those authorized under the law and to authenticate the identity of the requestor. The district will use an array of methods to protect records, including

physical controls (such as locked cabinets), technological controls such as role-based access controls for electronic records, password protection, firewalls, encryption, and administrative procedures. The district will document requests for and release of records, and retain the documentation in accordance with law.

~~If the district enters into a contract with a third party that calls for receipt of student PII by the contractor, the agreement shall include a data security and privacy plan that includes a signed copy of the Parents' Bill of Rights and addresses the following, among other contractual elements:~~

~~1. training of vendor employees regarding confidentiality requirements;~~
~~2. limiting access to education records to those individuals who have a legitimate educational interest;~~
~~3. prohibiting the use education records for any other purpose than those authorized under the contract;~~
~~4. maintaining reasonable administrative, technical and physical safeguards to protect PII;~~
~~5. using encryption technology to protect data while in motion or in its custody to prevent unauthorized disclosure;~~
~~6. breach and notification procedures.~~

The district will, via written agreements, designate authorized representatives who have access to educational records. The written agreement will specify how the work falls within the exception, what personally identifiable information is to be disclosed, how the educational record will be used, and that the records will be destroyed by the authorized representative once they are no longer needed for that purpose or the agreement expires.

Section 6 - Whenever a student record or any material contained therein is to be made available to third persons, other than those covered by the exceptions authorized by FERPA, the parent/guardian or eligible student must file a written consent to such action. The written consent must specify the records to be released, the reasons for such release, and to whom. If the parent or eligible student so requests, the district will provide him or her with a copy of the records disclosed. In addition, if the parent of a student who is not an eligible student so requests, the district will provide the student with a copy of the records disclosed.

Section 7 - Unless specifically exempted by FERPA, all persons requesting access to such records will be required to sign a written form which indicates the legitimate educational interest that such person has in inspecting the records. Such form will be kept with the student's file and will be maintained with the student's file as long as the file is maintained.

Additional Rights and Responsibilities Under New York State Law Related to the Protection of Student Data by the District and Third Party Contractors

New York State Education Law §2-d and reculations 8 NCRR Part 121 offers parents additional rights beyond FERPA in regard to third party contractors and student PII, and imposes additional responsibilities for the district and third parties to protect student PII. The district shall post on its website ~~and distribute~~ a 'Parents' Bill of Rights for Data Privacy and Security.' The 'Parents' Bill of Rights' ~~shall establish the following~~ will include all elements required by §2-d and Part 121, including supplemental information for contracts with all third parties receiving PII:

- ~~Educational purpose: The use of student personally identifiable information (PII) is for educational or related purposes only.~~
- ~~Transparency: Disclosure of third party contracts and their privacy provisions.~~
- ~~Authorization: Assurance that proper authorization will be secured prior to the release of PII~~
- ~~Security: A description of the measures in place to protect PII, without compromising the security plan.~~
- ~~Data Breach Notification: An explanation of the procedures in the event of a data breach.~~
- ~~Complaint Procedure: The district offers a complaint procedure in the event that a parent suspects a breach of student data by a third party contractor and provides information about lodging a complaint with the New York State Education Department's Chief Privacy Officer.~~

See policy 8635 (and regulation 8635-R), Information and Data Privacy, Security, Breach and Notification for more information on data security and breaches of PII, and 8635-E for the Parent's Bill of Rights for Data Privacy and Security and third-party supplemental information.

Retention and Disposition of Student Records

The Board has adopted the Records Retention and Disposition Schedule issued pursuant to Article 57-A of the Arts and Cultural Affairs Law, which contains the legal minimum retention periods for district records. The Board directs all district officials to adhere to the schedule and all other relevant laws in retaining and disposing of student records. In accordance with Article 57-A, the district will dispose of only those records described in the schedule after they have met the minimum retention periods set forth in the schedule. The district will dispose of only those records that do not have sufficient administrative, fiscal, legal or historical value to merit retention beyond the established legal minimum periods.

Second Reading: October 12, 2010
Amended Date: October 12, 2010
First Reading: January 7, 2014
Second Reading: February 11, 2014
Adoption Date: February 11, 2014
First Reading: October 7, 2014
Second Reading: October 21, 2014
Adoption Date: October 21, 2014
First Reading: May 27, 2025
Adoption Date: June 17, 2025
First Reading: September 30, 2025

# STUDENT PRIVACY

The Board recognizes its responsibility under the federal Protection of Pupil Privacy Rights ~~Act~~ Amendment (PPRA) to enact policies that protect student privacy, in accordance with law. This is particularly relevant in the context of the administration of surveys that collect personal information, the disclosure of personal information for marketing purposes and in conducting physical exams.

For purposes of this policy, "parent/guardian" includes a legal guardian or person standing in loco parentis (such as a grandparent or stepparent with whom the child lives, or a person who is legally responsible for the welfare of the child). Prior written parent/guardian consent for surveys and the right to inspect under this policy transfers to students once they turn 18 years old or are emancipated.

The Board of Education recognizes that student surveys are a valuable tool in determining student needs for educational services. ~~Parents have the right to inspect all instructional material that will be used for a survey, analysis, or evaluation as part of a U.S. Department of Education (DOE) funded program. In addition, no minor student may, without parental consent, take part in a survey, analysis or evaluation funded in whole or in part by the U.S. DOE Education that reveals information concerning:~~ surveys which gather any of the following information are subject to certain parent/guardian notification and consent requirements:

1. political affiliations or beliefs of the student or the student's parent;
2. mental or psychological problems of the student or the student's family;
3. sex behavior or attitudes;
4. illegal, anti-social, self-incriminating or demeaning behavior;
5. critical appraisals of other individuals with whom respondents have close family relationships;
6. legally recognized privileged or analogous relationships, such as those of lawyers, physicians and ministers;
7. religious practices, affiliations or beliefs of the student or the student's parent; or
8. income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).

If the district requires students to submit to such a survey, and the survey is part of a program funded by the U.S. Department of Education, students may not participate unless the parent/guardian provides prior written consent (i.e., "opt in"). If such a survey is funded through other sources, or participation in the survey is voluntary, the

district will administer the survey but give parents/guardians the opportunity to deny participation by the student (i.e., "opt out").

~~In the event that the district plans to survey students to gather information included in the list above, the district will obtain written consent from the parent/guardian in advance of administering the survey.~~

The notification/consent form will also apprise the parent/guardian of their right to inspect the survey prior to their child's participation. In addition, the district will notify parents/guardians that they may inspect any survey created by a third party before the survey is administered or distributed to students. ~~Prior written consent and the right to inspect surveys transfers to students once they turn 18 years old or are emancipated.~~ (except surveys administered to a student in accordance with the Individuals with Disabilities Education Act).

All requests to inspect third party surveys must be made to the Building Principal within 5 days after the notice was sent, or within 3 days prior to the date of the survey.

The district will limit access to information collected by any survey that contains the items listed above to those school officials who have a legitimate educational interest. The terms "school official" and "legitimate educational interest" are defined in district policy 5500, Student Records.

Under state Education Law §2-d and its implementing regulations (8 NYCRR Part 121), the district is prohibited from disclosing or using "personally identifiable information" for marketing or commercial purposes, or selling that information, or providing it to others for that purpose (see district policies 5500 and 8635, and their accompanying administrative regulations, for more information)

~~In the event that such data is collected by the district,~~ All disclosure or use of student personal information will be protected by the district pursuant to the requirements of the Family Educational Rights and Privacy Act (FERPA), Individuals with Disabilities Education *Act (*IDEA), Protection of Pupil Rights Amendment (PPRA), the National School Lunch Act, Children's Online Privacy Protection Act (COPPA), and NY Education Law §2-d [For guidance regarding the disclosure of "directory information," rather than personal student information, see policypolicies 5500, Student Records, and 8635, Information and Data Privacy, Security, Breach and Notification].

Inspection of Instructional Material

Parents/guardians shall have the right to inspect, upon request, any instructional material used as part of the educational curriculum for students. "Instructional material" is defined as: "instructional content that is provided to a student, regardless

of format including printed or representational materials, audio-visual materials, and materials in electronic or digital formats (such as materials accessible through the Internet). It does not include tests or academic assessments." The right to inspect instructional materials transfers to students once they turn 18 years old or are emancipated.

A parent/guardian (or student who is at least 18 years old or is emancipated) who wishes to inspect and review such instructional material must submit a request in writing to the Building Principal. Upon receipt of such request, arrangements shall be made to the district will provide access to such material within 30 calendar days after the request has been received.

Invasive Physical Examinations

~~The law also requires each school district to state its policy on the administration of physical examinations or screenings that the school may administer to a student, but this does not apply to physical examinations or screenings permitted or required by state law. If the district administers other physical exams, that should either be included here or cross-referenced to the appropriate policy.~~

Prior to the administration of any non-emergency, invasive physical examination or screening that is required as a condition of attendance, administered by the school and scheduled by the school in advance, which are not necessary to protect the immediate health or safety of the student or other students and not otherwise permitted or required by state law, a student's parent/guardian will be notified and given an opportunity to opt their child out of the exam.

"Invasive physical examination" is defined in federal law as any medical examination that involves the exposure of private body parts, or any act during such examination that includes incision, insertion, or injection into the body. Hearing, vision and scoliosis screenings are not included in this definition and are not subject to prior notification, nor are any physical examinations that are permitted or required by state law, including those which are permitted without parent/guardian notification.

Notification

The district will notify parents/guardians and eligible students who are at least 18 years old or who are emancipated shall be notified at least annually, at the beginning of the school year, and when enrolling students for the first time in district schools, of their rights under this policy, and the specific or approximate dates that the activities described in this policy are scheduled or expected to be scheduled. The school district

shall also notify parents/guardians within a reasonable period of time after any substantive change to this policy.

Cross-ref:
5420, Student Health Services
5500, Student Records
8635, Information and Data Privacy, Security, Breach and Notification

Ref: 20 USC §1232h (No Child Left Behind Act)
34 CFR Part 98
Education Law §903

AGENDA ITEM

First Reading: June 10, 2008
Adoption date: June 24, 2008
First Reading: May 27, 2025
Adoption Date: June 17,2025
First Reading: September 30, 2025

# PARENTS' BILL OF RIGHTS FOR STUDENT DATA PRIVACY AND SECURITY

~~The Deer Park School District, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. The Deer Park School District establishes the following parental bill of rights:~~

- ~~Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.~~

- ~~The district and its schools, and third-party contractors and subcontractors, will not sell student PII or use or disclose it for any marketing or commercial purposes or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so;~~

- ~~Parents have the right to inspect and review the complete contents of their child's education record (for more information about how to exercise this right, see 5500-R);~~

- ~~State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. Safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred;~~

- ~~A complete list of all student data elements collected by the State Education Department is available for public review at http://nysed.gov/data-privacy-security/student-data-inventory or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234~~

- ~~Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to Jay Murphy, District Administrator for Instructional Technology, (631) 274-4380, murphy.j@deerparkschools.org. Complaints can also be directed to the New York State Education Department online at http://nysed.gov/data-privacy-security/report-improper-disclosure, by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to privacy@nysed.gov or by telephone at 518-474-0937.~~

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

- ~~All district and school employees and officers with access to PII will receive annual training on applicable federal and state laws, regulations, district and school policies and safeguards which will be in alignment with industry standards and best practices to protect PII~~

- ~~In the event that the District engages a third party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by accessing the information on the district's website at www.deerparkschools.org.~~

~~**PARENT BILL OF RIGHTS FOR STUDENT DATA PRIVACY AND SECURITY THIRD PARTY CONTRACTOR SUPPLEMENT**~~

~~The (*insert name of contractor*) has been engaged by the Deer Park School District to provide services. In this capacity, the company may collect, process, manage, store or analyze student or teacher/principal personally identifiable information (PII).~~

~~The (*insert name of contractor*) will provide the district with (*describe specific purpose for which the PII will be used*).~~

~~The (*insert the name of contractor*) will ensure that subcontractors or others that the company shares PII will abide by data protection and security requirements of district policy, and state and federal law and regulations by (*describe methods/procedures to safeguard data use by subcontractors*).~~

~~PII will be stored (*describe the location in a manner that protects data security*).~~

~~Parents may challenge the accuracy of PII held by (*insert name of contractor*) by contacting (*insert contact information, including title, phone number, mailing address and email address*).~~

~~The (*insert name of contractor*) will take reasonable measures to ensure the confidentiality of PII by implementing the following (*describe the following, as applicable*):~~

- ~~Password protections~~
- ~~Administrative procedures~~
- ~~Encryption while PII is in motion and at rest~~
- ~~Firewalls~~

~~The contractor's agreement with the district begins on (*insert date*) and ends on (*insert date*). Once the contractor has completed its service to the district, records containing student PII will be (*select one*: destroyed or returned) by (*insert date*) via the following (insert method if destroyed or format if returned).~~

The Board of Education acknowledges the heightened concern regarding the rise in identity theft and the need for secure networks and prompt notification when security breaches occur. The Board adopts the National Institute for Standards and Technology Cybersecurity Framework Version ***select as applicable***: 1.1 or 2] (NIST CSF) for data security and protection. The district's Executive Director for Instructional Technology is responsible for ensuring the district's systems follow NIST CSF and adopt technologies, safeguards and practices which align with it. This will include an assessment of the district's current cybersecurity state, their

target future cybersecurity state, opportunities for improvement, progress toward the target state, and communication about cyber security risk.

The Board will designate a Data Protection Officer to be responsible for the implementation of the policies and procedures required in Education Law §2-d and its accompanying regulations, and to serve as the point of contact for data security and privacy for the district. *optional language:* This appointment will be made at the annual organizational meeting]

The Board directs the Superintendent of Schools, in accordance with appropriate business and technology personnel, and the Data Protection Officer (where applicable) to establish regulations which address:

- the protections of "personally identifiable information" of student and teachers/principal under Education Law §2-d and Part 121 of the Commissioner of Education;
- the protections of "private information" under State Technology Law §208 and the NY SHIELD Act; and
- procedures to notify persons affected by breaches or unauthorized access of protected information.

**Student and Teacher/Principal "Personally Identifiable Information" under Education Law §2-d**

A. General Provisions

*PII* as applied to student data is as defined in Family Educational Rights and Privacy Act (Policy 5500), which includes certain types of information that could identify a student, and is listed in the accompanying regulation 8635-R. PII as applied to teacher and principal data, means results of Annual Professional Performance Reviews that identify the individual teachers and principals, which are confidential under Education Law §§3012-c and 3012-d, except where required to be disclosed under state law and regulations.

The Data Protection Officer will see that every use and disclosure of personally identifiable information (PII) by the district benefits students and the district (e.g., improve academic achievement, empower parents and students with information, and/or advance efficient and effective school operations). However, PII will not be included in public reports or other documents.

The district will protect the confidentiality of student and teacher/principal PII while stored or transferred using industry standard safeguards and best practices, such as encryption, firewalls, and passwords. The district will monitor its data systems, develop incident response plans, limit access to PII to district employees and third-party contractors who need such access to fulfill their professional responsibilities or contractual obligations, and destroy PII when it is no longer needed.

Certain federal laws and regulations provide additional rights regarding confidentiality of and access to student records, as well as permitted disclosures without consent, which are addressed in policy and regulation 5500, Student Records.

Under no circumstances will the district sell PII. It will not disclose PII for any marketing or commercial purpose, facilitate its use or disclosure by any other party for any marketing or commercial purpose, or permit another party to do so. Further, the district will take steps to minimize the collection, processing, and transmission of PII.

Except as required by law or in the case of enrollment data, the district will not report the following student data to the State Education Department:

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

The district has created and adopted a Parent's Bill of Rights for Data Privacy and Security (see Exhibit 8635-E). It has been published on the district's website at *www.deerparkschools.org* and can be requested from the district clerk.

- Student PII cannot be sold or released for any commercial purposes;
- Parents/guardians have the right to inspect and review the complete contents of their child's education record;
- State and federal laws protect the confidentiality of PII, and that safeguards (such as encryption, firewalls, and passwords) will 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 viewing, and the web address or mailing address for doing so; and
- Parents/guardians have the right to have complaints about possible breaches of student data addressed, and the contact information to direct those complaints.

For each contract with a third party contractor that receives PII, the Parents Bill of Rights will include the following supplemental information will include:

- The exclusive purposes for which the PII will be used;
- How the contractor will ensure that subcontractors and/or authorized users will abide by data protection and security requirements;
- The end date of the contract, and what happens to the PII when the contract ends;
- If and how parents/guardians, students, eligible students, teachers or principals may challenge the accuracy of the PII collected;

- Where the PII will be stored (described without compromising data security) and the security measures taken to protect the PII and mitigate security and privacy risks; and
- How the data will be protected using encryption while in motion and at rest.

B. Third-party Contractors

The district will ensure that contracts with third-party contractors reflect that confidentiality of any student and/or teacher or principal PII be maintained in accordance with federal and state law and the district's data security and privacy policy.

Each third-party contractor that will receive student data or teacher or principal data must:

1. adopt technologies, safeguards and practices that align with the NIST CSF;
2. comply with the district's data security and privacy policy and applicable laws impacting the district;
3. limit internal access to PII to only those employees or sub-contractors that need access to provide the contracted services;
4. not use the PII for any purpose not explicitly authorized in its contract;
5. not disclose any PII to any other party without the prior written consent of the parent or eligible student (i.e., students who are eighteen years old or older):
    a. except for authorized representatives of the third-party contractor to the extent they are carrying out the contract; or
    b. unless required by statute or court order and the third party contractor provides notice of disclosure to the district, unless expressly prohibited.
6. maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody;
7. use encryption to protect PII in its custody; and
8. not sell, use, or disclose PII for any marketing or commercial purpose, facilitate its use or disclosure by others for marketing or commercial purpose, or permit another party to do so.

Third party contractors may release PII to subcontractors engaged to perform the contractor's obligations, but such subcontractors must abide by data protection obligations of state and federal law, and the contract with the district.

If the third-party contractor has a breach or unauthorized release of PII, it will promptly notify the district in the most expedient way possible without unreasonable delay but no more than seven calendar days after the breach's discovery.

C. Third-Party Contractors' Data Security and Privacy Plan

The district will ensure that contracts with all third-party contractors include the third-party contractor's data security and privacy plan. This plan must be accepted by the district.

At a minimum, each plan will:

1. outline how all state, federal, and local data security and privacy contract requirements over the life of the contract will be met, consistent with this policy;
2. specify the administrative, operational and technical safeguards and practices it has in place to protect PII;
3. demonstrate that it complies with the requirements of 8 NYCRR Section 121.3(c) (the Parent's Bill of Rights for Data Privacy and Security);
4. specify how those who have access to student and/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 district;
7. describe if, how and when data will be returned to the district, transitioned to a successor contractor, at the district's direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.

D. Training

The district will provide annual training on data privacy and security awareness to all employees who have access to student and teacher/principal PII.

E. Reporting

Any breach of the district's information storage or computerized data which compromises the security, confidentiality, or integrity of student or teacher/principal PII maintained by the district will be promptly reported to the Data Protection Officer, the Superintendent and the Board of Education.

F. Notifications

The Data Protection Officer *or insert appropriate title* will report every discovery or report of a breach or unauthorized release of student, teacher or principal PII to the State's Chief Privacy Officer without unreasonable delay, but no more than 10 calendar days after such discovery.

The district will notify affected parents, eligible students, teachers and/or principals in the most expedient way possible and without unreasonable delay, but no more than 60 calendar days after the discovery of a breach or unauthorized release or third-party contractor notification.

However, if notification would interfere with an ongoing law enforcement investigation, or cause further disclosure of PII by disclosing an unfixed security vulnerability, the district will notify parents, eligible students, teachers and/or principals within seven calendar days after the security vulnerability has been remedied, or the risk of interference with the law enforcement investigation ends.

The Superintendent *or insert appropriate title*, in consultation with the Data Protection Officer, will establish procedures to provide notification of a breach or unauthorized release of student, teacher or principal PII, and establish and communicate to parents, eligible students, and district staff a process for filing complaints about breaches or unauthorized releases of student and teacher/principal PII.

**"Private Information" under State Technology Law §208**

"Private information" is defined in State Technology Law §208, and includes certain types of information, outlined in the accompanying regulation, which would put an individual at risk for identity theft or permit access to private accounts. "Private information" does not include information that can lawfully be made available to the general public pursuant to federal or state law or regulation.

Any breach of the district's information storage or computerized data which compromises the security, confidentiality, or integrity of "private information" maintained by the district must be promptly reported to the Superintendent and the Board of Education.

The Board directs the Superintendent of Schools, in accordance with appropriate business and technology personnel, to establish regulations which:

- Identify and/or define the types of private information that is to be kept secure;
- Include procedures to identify any breaches of security that result in the release of private information; and
- Include procedures to notify persons affected by the security breach as required by law.

**Employee "Personal Identifying Information" under Labor Law § 203-d**

Pursuant to Labor Law §203-d, the district will not communicate employee "personal identifying information" to the general public. This includes:

1. social security number;
2. home address or telephone number;

3. personal email address;
4. Internet identification name or password;
5. parent's surname prior to marriage; and
6. drivers' license number.

In addition, the district will protect employee social security numbers in that such numbers will not be:

1. publicly posted or displayed;
2. visibly printed on any ID badge, card or time card;
3. placed in files with unrestricted access; or
4. used for occupational licensing purposes.

Employees with access to such information will be notified of these prohibitions and their obligations.



First Reading: November 15, 2022
Adoption Date: November 29, 2022
First Reading: September 30, 2025

# INFORMATION AND DATA SECURITY BREACH AND NOTIFICATION REGULATION

~~Definitions~~

~~"Private information" shall mean personal information (i.e., information such as name, number, symbol, mark or other identifier which can be used to identify a person) in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:~~

- ~~Social security number;~~
- ~~Driver's license number or non-driver identification card number or;~~
- ~~Account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.~~

~~Note: "Private information" does not include publicly available information that is lawfully made available to the general public pursuant to state or federal law or regulation.~~

~~"Breach of the security of the system" shall mean unauthorized acquisition or acquisition without valid authorization of physical or computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the district. Good faith acquisition of personal information by an officer or employee or agent of the district for the purposes of the district is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.~~

~~Procedure for Identifying Security Breaches~~

~~In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, the district shall consider:~~

~~1. indications that the information is in the physical possession and control of an unauthorized person, such as removal of hard copies, a lost or stolen computer, or other device containing information;~~

~~2. indications that the information has been downloaded or copied;~~

~~3. indications that the information was used by an unauthorized person, such as fraudulent accounts, opened or instances of identity theft reported; and/~~

~~4. any other factors which the district shall deem appropriate and relevant to such determination.~~

~~Security Breaches – Procedures and Methods for Notification~~

~~Once it has been determined that a security breach has occurred, the following steps shall be taken:~~

~~1. If the breach involved hard copy or computerized data *owned or licensed* by the district, the district shall notify those New York State residents whose private information was, or is reasonably believed to have been acquired by a person without valid authorization. The disclosure to affected individuals shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system.~~

~~The district shall consult with the New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) to determine the scope of the breach and restoration measures.~~

~~2. If the breach involved hard copy or computer data *maintained* by the district, the district shall notify the owner or licensee of the information of the breach immediately following discovery, if the private information was or is reasonably believed to have been acquired by a person without valid authorization.~~

~~Note: The notification requirement may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The required notification shall be made after the law enforcement agency determines that such notification does not compromise the investigation.~~

~~The required notice shall include (a) district contact information, (b) a description of the categories of information that were or are reasonably believed to have been acquired without authorization and (c) which specific elements of personal or private information were or are reasonably believed to have been acquired and (d) what the district is doing about it. This notice shall be directly provided to the affected individuals by either:~~

~~1. Written notice~~
~~2. Electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and that the district keeps a log of each such electronic notification. In no case, however, shall the district require a person to consent to accepting such notice in electronic form as a condition of establishing a business relationship or engaging in any transaction.~~
~~3. Telephone notification, provided that the district keeps a log of each such telephone notification.~~

~~However, if the district can demonstrate to the State Attorney General that (a) the cost of providing notice would exceed $250,000; or (b) that the number of persons to be notified exceeds 500,000; or (c) that the district does not have sufficient contact information, substitute notice may be provided. Substitute notice would consist of all of the following steps:~~

~~1. E-mail notice when the district has such address for the affected individual;~~
~~2. Conspicuous posting on the district's website, if they maintain one; and~~
~~3. Notification to major media~~

~~Notification of State and Other Agencies~~

~~Once notice has been made to affected New York State residents, the district shall notify the State Attorney General, the Department of State Division of Consumer Protection and the State Office of Information Technology Services as to the timing, content, and distribution of the notices and approximate number of affected persons.~~

~~If more than 5,000 New York State residents are to be notified at one time, the district shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected individuals. A list of consumer reporting agencies will be furnished, upon request, by the Office of the State Attorney General.~~

This regulation addresses information and data privacy, security, breach and notification requirements for student and teacher/principal personally identifiable information under Education Law §2-d, as well as private information under State Technology Law §208.

The district will inventory its computer programs and electronic files to determine the types of information that is maintained or used by the district, and review the safeguards in effect to secure and protect that information.

I. *Student and Teacher/Principal "Personally Identifiable Information" (PII) under Education Law §2-d*

A. Definitions

"*Biometric record*," as applied to student PII, means one or more measurable biological or behavioral characteristics that can be used for automated recognition of

person, which includes fingerprints, retina and iris patterns, voiceprints, DNA sequence, facial characteristics, and handwriting.

"*Breach*" means the unauthorized acquisition, access, use, or disclosure of student PII and/or teacher or principal PII by or to a person not authorized to acquire, access, use, or receive the student and/or teacher or principal PII.

"Contract or other written agreement" means a binding agreement between the district and a third party, including one created in electronic form and signed with an electronic or digital signature or a click wrap agreement 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.

"*Disclose*" *or Disclosure* mean to permit access to, or the release, transfer, or other communication of PII by any means, including oral, written, or electronic, whether intended or unintended.

"*Personally Identifiable Information*" (PII) as applied to students means the following information for district students:

1. the student's name;
2. the name of the student's parent or other family members;
3. the address of the student or student's family;
4. a personal identifier, such as the student's social security number, student number, or biometric record;
5. other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
6. other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
7. information requested by a person who the district reasonably believes knows the identity of the student to whom the education record relates.

Additionally, the State Chief Privacy Officer has determined that student and parent phone numbers are considered PII.

"*Personally Identifiable Information*" (PII) as applied to teachers and principals means results of Annual Professional Performance Reviews that identify the individual teachers and principals, which are confidential under Education Law §§3012-c and 3012-d, except where required to be disclosed under state law and regulations.

"*Third-Party Contractor*" means any person or entity, other than an educational agency (i.e., a school, school district, BOCES or State Education Department), that receives student or teacher/principal PII from the 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 the educational agency, or audit or evaluation of publicly funded programs. This includes an educational partnership organization that receives student and/or teacher/principal PII from a school district to carry out its responsibilities pursuant to Education Law §211-e (for persistently lowest-achieving schools or schools under registration review) and is not an educational agency. This also includes a not-for-profit corporation or other nonprofit organization, other than an educational agency.

B. Complaints of Breaches or Unauthorized Releases of PII

If a parent/guardian or eligible student wishes to claim that student PII has been breached (discloses, accessed or released) without authorization, they must submit this complaint in writing to the district. Complaints may be received by the Data Protection Officer or insert other title, but may also be received by any district employee, who must immediately notify the Data Protection Officer. This complaint process will be communicated to parents, and eligible students. All employees are required to report breaches of student or teacher/principal PII that they are aware of to the Data Protection Officer.

The district will acknowledge receipt of complaints promptly, commence an investigation, and take the necessary precautions to protect personally identifiable information.

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

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

The district will 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 LGS-1.

After going through the district's complaint procedure, parents and eligible students may also submit complaints to the State Education Department's Chief Privacy Officer at privacy@nysed.gov.

C. Notification of Student and Teacher/Principal PII Breaches

If a third-party contractor has a breach or unauthorized release of PII, it will promptly notify the Data Protection Officer *or insert other title* in the most expedient way possible, without unreasonable delay, but no more than seven calendar days after the breach's discovery.

The Data Protection Officer *or insert other title* will then notify the State 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 State Education Department.

The Data Protection Officer *or insert other title* will 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.

The district will notify affected parents, eligible students, teachers and/or principals in the most expedient way possible and without unreasonable delay, but no more than 60 calendar days after the discovery of a breach or unauthorized release or third-party contractor notification.

However, if notification would interfere with an ongoing law enforcement investigation or cause further disclosure of PII by disclosing an unfixed security vulnerability, the district will notify parents, eligible students, teachers and/or principals within seven calendar days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends.

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

- a 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 PII affected;
- an estimate of the number of records affected;
- a brief description of the district's investigation or plan to investigate; and
- contact information for representatives who can assist parents or eligible students with additional questions.

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.

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

The unauthorized acquisition of student social security numbers, student ID numbers, or biometric records, when in combination with personal information such as names or other identifiers, may also constitute a breach under State Technology Law §208 if the information is not encrypted, and the acquisition compromises the security, confidentiality, or integrity of personal information maintained by the district. In that event, the district is not required to notify affected people twice, but must follow the procedures to notify state agencies under State Technology Law §208 outlined in section II of this regulation.

II. *"Private Information" under State Technology Law §208*

A. Definitions

"*Private information*" means either:

1. personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the personal information plus the data element is not encrypted or encrypted encryption key that has also been accessed or acquired:

- Social security number;
- Driver's license number or non-driver identification card number;
- Account number, credit or debit card number, in combination with any required security code, access code, password or other information which would permit access to an individual's financial account;
- account number or credit or debit card number, if that number could be used to access a person's financial account without other information such as a password or code; or
- biometric information (data generated by electronic measurements of a person's physical characteristics, such as fingerprint, voice print, or retina or iris image) used to authenticate or ascertain a person's identity; or

2. a user name or email address, along with a password, or security question and answer, that would permit access to an online account.

"Private information" does not include information that can lawfully be made available to the general public pursuant to federal or state law or regulation;

"*Breach of the security of the system*" means unauthorized acquisition or acquisition without valid authorization of physical or computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the district. Good faith acquisition of personal information by an officer or employee or agent of the district for the purposes of the district is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

B. Procedure for Identifying Security Breaches

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, the district will consider:

1. indications that the information is in the physical possession and control of an unauthorized person, such as removal of lost or stolen computer, or other device containing information;
2. indications that the information has been downloaded or copied;
3. indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; and/or
4. any other factors which the district shall deem appropriate and relevant to such determination.

C. Notification of Breaches to Affected Persons

Once it has been determined that a security breach has occurred, the district will take the following steps:

1. If the breach involved computerized data *owned or licensed* by the district, the district will notify those New York State residents whose private information was, or is reasonably believed to have been accessed or acquired by a person without valid authorization. The disclosure to affected individuals will be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and to restore the integrity of the

system. The district will consult with the New York State Office of Information Technology Services to determine the scope of the breach and restoration measures.

2. If the breach involved computer data *maintained* by the district, the district will notify the owner or licensee of the information of the breach immediately following discovery, if the private information was or is reasonably believed to have been accessed or acquired by a person without valid authorization.

The required notice will include (a) district contact information, (b) a description of the categories information that were or are reasonably believed to have been accessed or acquired without authorization, (c) which specific elements of personal or private information were or are reasonably believed to have been acquired and (d) the telephone number and website of relevant state and federal agencies that provide information on security breach response and identity theft protection and prevention. This notice will be directly provided to the affected individuals by either:

1. Written notice
2. Electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and that the district keeps a log of each such electronic notification. In no case, however, will the district require a person to consent to accepting such notice in electronic form as a condition of establishing a business relationship or engaging in any transaction.
3. Telephone notification, provided that the district keeps a log of each such telephone notification.

However, if the district can demonstrate to the State Attorney General that (a) the cost of providing notice would exceed $250,000; or (b) that the number of persons to be notified exceeds 500,000; or (c) that the district does not have sufficient contact information, substitute notice may be provided. Substitute notice would consist of all of the following steps:

1. E-mail notice when the district has such address for the affected individual;
2. Conspicuous posting on the district's website, if they maintain one; and
3. Notification to major media.

However, the district is not required to notify individuals if the breach was inadvertently made by individuals authorized to access the information, and the

district reasonably determines the breach will not result in misuse of the information, or financial or emotional harm to the affected persons. The district will document its determination in writing and maintain it for at least five years, and will send it to the State Attorney General within ten days of making the determination.

Additionally, if the district has already notified affected persons under any other federal or state laws or regulations regarding data breaches, including the federal Health Insurance Portability and Accountability Act, the federal Health Information Technology for Economic and Clinical Health (HI TECH) Act, or New York State Education Law §2-d, it is not required to notify them again. Notification to state and other agencies is still required.

D. Notification to State Agencies and Other Entities

Once notice has been made to affected New York State residents, the district shall notify the State Attorney General, the State Department of State, and the State Office of Information Technology Services as to the timing, content, and distribution of the notices and approximate number of affected persons.

If more than 5,000 New York State residents are to be notified at one time, the district will also notify consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected individuals. A list of consumer reporting agencies will be furnished, upon request, by the Office of the State Attorney General.

If the district is required to notify the U.S. Secretary of Health and Human Services of a breach of unsecured protected health information under the federal Health Insurance Portability and Accountability Act (HIPAA) or the federal Health Information Technology for Economic and Clinical Health (HI TECH) Act, it will also notify the State Attorney General within five business days of notifying the Secretary.

First Reading: June 10, 2008
Second Reading: June 24, 2008
Adoption Date: June 24, 2008
First Reading: August 5, 2014
Second Reading: August 26, 2014
Adoption Date: August 26, 2014
First Reading: September 30, 2025

# PARENTS' BILL OF RIGHTS FOR STUDENT DATA PRIVACY AND SECURITY - EXHIBIT

(Pursuant to Education Law §2-d and Commissioner's Regulations Part 121)

The Deer Park School District ("District") affirms its commitment to safeguarding student, teacher, and principal personally identifiable information (PII) in educational records from unauthorized access, disclosure, or misuse, in accordance with federal and state law.

## Parents' Rights

1. A student's personally identifiable information cannot be sold or released for any marketing or commercial purpose.
2. Parents have the right to inspect and review the complete contents of their child's education record and to request corrections or amendments if the information is inaccurate, misleading, or violates the child's privacy rights.
3. Parents will be notified in the event of a breach or unauthorized release of their child's personally identifiable information.
4. State and federal laws protect the confidentiality of personally identifiable information. Safeguards consistent with industry standards and best practices—including administrative, technical, and physical measures aligned with the NIST Cybersecurity Framework—must be in place when data is collected, stored, or transferred.
5. A complete list of all student data elements collected by the State is available for public review at:
   http://www.nysed.gov/data-privacy-security
   or by writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

## Complaint Procedures

- Parents have the right to submit complaints about possible breaches or unauthorized disclosures of student data.
- Complaints should be directed to:
  **Superintendent of Schools**
  Deer Park School District
  1881 Deer Park Avenue, Deer Park, NY 11729
  Phone: 631-274-4010
  Email: dataprotection@deerparkschools.org

- Complaints may also be directed to the **Chief Privacy Officer**, New York State Education Department, 89 Washington Avenue, Albany, NY 12234, Email: **privacy@nysed.gov**

The District will acknowledge complaints within **five business days** and provide a resolution timeline.

## Third-Party Contractors

Each contract the District enters into with a third-party contractor that receives student data or teacher/principal data shall include:

- The exclusive purpose for which the data will be used.
- Assurance that subcontractors will abide by the same data protection and security requirements.
- Expiration date of the agreement and procedures for secure return or destruction of the data.
- A process for parents, eligible students, teachers, or principals to challenge the accuracy of data held by the contractor.
- Location of data storage (described in a manner that protects data security), security protections in place, and whether the data is encrypted.
- Vendor obligation to notify the District of any breach within **seven calendar days**.
- Proof of **annual privacy and security training** for vendor staff with access to PII.
- A requirement that vendors bear the costs of breach notification and remediation.

## Posting and Transparency

- This Parents' Bill of Rights will be posted on the District website, provided in multiple languages as needed, and attached to all contracts where PII is shared.

- Annual FERPA/Ed Law §2-d notifications will be issued to parents, including the right to opt out of the disclosure of directory information.

## Annual Review

The Parents' Bill of Rights will be reviewed annually to ensure compliance with updates from the NYSED Chief Privacy Officer and applicable law.