DEER PARK UNION FREE SCHOOL DISTRICT

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Pursuant to Education Law Section 2-d, the Deer Park School District ("District") hereby sets forth the following Parents' Bill of Rights for Data Privacy and Security,

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

2. Parents have the right to inspect and review the complete contents of their child's education record;

3. State and federal laws protect the confidentiality of personally identifiable information (as defined under Education Law Section 2-d(d), and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred;

4. A complete list of all student data elements collected by the State is available for public review at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234; and

5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to Superintendent of Schools, Deer Park School District, 1881 Deer Park Avenue, Deer Park, NY 11729, 631-274-4010 or Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234, email to CP0@mail.nysed.gov.

6. Each contract the District enters into with a third party contractor where the third party contractor receives student data, or teacher or principal data, shall include the following supplemental information:

    a. The exclusive purpose for which the student data, or teacher or principal data, will be used;

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

c. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

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

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

7. The Parents' Bill of Rights shall be subject to change pursuant to the direction from the New York State Education Department Chief Privacy Officer and the Regulations of the Commissioner of Education.

ATTACHMENT

OBLIGATIONS OF THIRD PARTY CONTRACTORS

1. Officers and/or employees of the third party contractor and its assignees who have access to student data or teacher or principal data must receive training on the federal and state law governing confidentiality of such data.

2. Limit internal access to education records to those individuals that are determined to have legitimate educational interests.

3. Not use the education records for any other purposes than those explicitly authorized in its contract.

4. Except for authorized parties of the third party contractor, to the extent they are carrying out the contract, not disclose any personally identifiable information to any other party (a) without the prior written consent of the parent or eligible student; or (b) unless required by statute or court order and the party provides a notice of the disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order.

5. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody.

6. Uses encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the Secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.