CLASSICAL
CHARTER SCHOOLS

Classical Charter Schools Parent's Bill of Rights (PBOR) for Data Privacy and Security

Classical Charter Schools ("Classical") secures its information technology (IT) systems and protects the privacy of its students. Classical has set forth policies and procedures for data privacy and security in accordance with New York State Education Department (NYSED), Education Law 2-d and Part 121 regulations of the Commissioner of Education.

Classical Charter Schools is committed to protecting the privacy and security of every student and every student's data. Parents should be aware of the following rights they have regarding their child's data per Education Law §2-D Bill of Rights for Data Privacy and Security.

Parents and legal guardians can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose. PII, as identified by Education Law §2-D and FERPA, includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency (this right may not apply to parents).
3. State and Federal laws such as
    - Education Law §2-D; the Commissioner of Education's Regulations at 8 NYCRR Part 121, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99);
    - Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312);
    - Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98);
    - the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including but not limited to encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. NYSED has a complete list of all student data elements that can be accessed by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or at http://www.nysed.gov/data-privacy-security/student-data-inventory
6. The right to have complaints about possible breaches and unauthorized disclosure of PII addressed. Complaints may be submitted to:

Classical Charter Schools
977 Fox Street, 4th Floor
Bronx, NY 10459
(718) 860-4340

Complaints may also be submitted to NYSED at http://www.nysed.gov/data-privacysecurity/report-improper-disclosure, by mail to:

Chief Privacy Officer
New York State Education Department
89 Washington Avenue, Albany, NY 12234
(518) 474-0937

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Any educational agencies that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

Statement on Third-Party Contractors

When third-party service providers receive student data, teacher data or principal data, supplemental information shall be developed and provided to parents that states:

1. Personally identifiable information may not be sold or used for marketing purposes.
2. Each educational agency must publish a parents bill of rights for data privacy and security, which must be included in contracts with third party contractors.

The parents bill of rights must state the following:

a. A student's personally identifiable information cannot be sold or released for any commercial purposes;
b. Parents have the right to inspect and review the full contents of their child's education record;
c. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred;
d. A complete list of all student data elements collected by the State is available for public review at a website or a mailing address, to be included in the bill of rights and
e. Parents have the right to have complaints about possible breaches of student data addressed. A phone number, email and mailing address must be included where parents can send complaints.

The parents’ bill of rights must also include supplemental information for each contract an educational agency enters into with a third party contractor. The supplemental information must include:

a. The exclusive purposes for which the student, teacher or principal data will be used;
b. How the third party contractor will ensure that subcontractors, persons or entities with access to student, teacher or principal data with, if any, will abide by data protection and security requirements;
c. When the agreement expires, and what happens to the student, 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, teacher or principal data will be stored and the applicable security protections, including whether the data will be encrypted.

Additional Contract Requirements: Contracts must also include the following provisions and assurances by third party contractors:

1. That the confidentiality of the student, teacher or principal data will be maintained in accordance with federal and state law, and the educational agency's policy on data security and privacy.
2. A data security and privacy plan outlining how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the educational agency's policy on data security and privacy, including, but not limited to:
    a. Signed copy of the parents bill of rights for data privacy and security
    b. Requirement that any officers or employees of the third party contractor and its assignees who have access to student, teacher or principal data have received or will receive training on the federal and state law governing confidentiality of the data prior to receiving access
3. Access to education records will be limited to individuals with legitimate educational interests;
4. Education records will not be used except for purposes explicitly authorized in the contract;
5. Education records may only be shared with authorized representatives of the third party contractor to the extent they are carrying out the contract, and not to any other party without the prior written consent of the parent or eligible student; or unless required by statute or court order, with notice then provided to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless such notice is prohibited by the statute or court order;
6. The reasonable administrative, technical and physical safeguards maintained to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
7. Data will be encrypted in motion or in custody using a technology or methodology specified by the United States health and human services guidance issued under Section 13402(H)(2) of Public Law 111-5:
8. Requirement to notify the educational agency of any security breach resulting in an unauthorized release of data by the third party contractor or its assignees in violation of applicable state or federal law, the parents bill of rights for student data privacy and security, the data privacy and security policies of the educational agency and/or binding contractual obligations, in the most expedient way possible and without unreasonable delay.

a. In the case of an unauthorized release of student, teacher or principal data, the educational agency shall notify the parent or eligible student, teacher or principal, respectively, of the unauthorized release of student data that includes personally identifiable information in the most expedient way possible and without unreasonable delay, and the third party contractor must promptly reimburse the educational agency for the full cost of such notification.

Classical Users will annually complete information privacy and security training.