CARDINAL McCLOSKEY
COMMUNITY CHARTER SCHOOL

Data Security and Privacy Policy

Protecting Student Privacy

Cardinal McCloskey Community Charter School ("CMCCS" or the "School") takes seriously its obligations to secure data systems and protect the privacy of students and is committed to promoting sound information practices and policies that will strengthen data privacy and security.

CMCCS will follow all applicable laws and regulations for the handling and storage of protected data in our school and when disclosing or releasing it to others including, but not limited to, third party contractors. CMCCS adheres to this policy in order to implement the requirements of New York State Education Law Section 2-d and its regulations.

General Provisions

This policy shall be published on the School's website and notice of the policy will be provided to all employees.

The Board of Trustees of Cardinal McCloskey Community Charter School (the "Board") adopts the National Institute for Standards and Technology Cybersecurity Framework Version ("NIST CSF") for data security and protection. The Data Protection Officer is responsible for ensuring that the School's systems follow NIST CSF and adopt technologies, safeguards and practices which align with it. This will include an assessment of the School's current cybersecurity state, their target future cybersecurity state, opportunities for improvement, progress toward the target state, and communication about cybersecurity risk.

Nothing contained in this policy shall be construed as creating a private right of action against CMCCS.

The Board has designated the Human Resources Manager as the School's Data Protection Officer. The Data Protection Officer is responsible for the implementation of the policies and procedures required in Section 2-d of the New York State Education Law and its accompanying regulations, and to serve as the point of contact for data security and privacy for the School.

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

i. the protections of "personally identifiable information" of student and teachers/principals under Section 2-d of the New York State Education Law and Part 121 of the Commissioner of Education;
ii. the protections of "private information" under Section 208 of the New York State Technology Law;
iii. the New York State SHIELD Act; and
iv. procedures to notify persons affected by breaches or unauthorized access of protected information.

Student and Teacher/Principal "Personally Identifiable Information" New York State Education Law § 2-d

1. General Provisions

PII, as applied to student data as defined in the Family Educational Rights and Privacy Act ("FERPA), includes certain types of information that could identify a student. 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 New York State Education Law §§ 3012-c and 3012-d, except where required to be disclosed under state law and regulations.

The School 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 School will monitor its data systems, develop incident response plans, limit access to PII to School 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.

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

Under no circumstances will the School 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 School 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 School will not report the following student data to the New York State Education Department:

i. juvenile delinquency records;
ii. criminal records;
iii. medical and health records; and
iv. student biometric information.

The School has created and adopted a Parent's/Guardian's Bill of Rights for Data Privacy and Security. It has been published on the School's website cmccs.org. The Parent's/Guardian's Bill of Rights includes, but is not limited to, provisions stating that:

i. student PII cannot be sold or released for any commercial or marketing purpose;
ii. parents/guardians and eligible students (i.e., 18 years or older) have the right to inspect and review the complete contents of the student's education record;
iii. 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 and transferred;
iv. 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
v. parents/guardians have the right to have complaints about possible breaches of student data addressed, and the contact information to direct those complaints.

2. Third-party Contractors

The School 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 School's data security and privacy policy.

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

i. adopt technologies, safeguards, and practices that align with NIST CSF;
ii. comply with the School's data security and privacy policy and applicable laws impacting the School;
iii. limit internal access to PII to only those employees or sub-contractors that need access to provide the contracted services;
iv. not use the PII for any purpose not explicitly authorized in its contract;
v. not disclose any PII to any other party without the prior written consent of the parent/guardian or eligible student (i.e., students who are 18 years or older) (except

for authorized representatives of third-party contractors to the extent they are carrying out the contract or unless required by statute or court order and the third party contractor provides notice of disclosure to the School, unless expressly prohibited);

vi. maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody;

vii. use encryption to protect PII in its custody; and

viii. 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 School.

If the third-party contractor has a breach or unauthorized release of student PII, it will promptly notify the School in the most expedient way possible without unreasonable delay but no more than seven (7) calendar days after the breach's discovery.

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

The School 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 School. At a minimum each plan will:

i. 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;

ii. specify the administrative, operational, and technical safeguards and practices it has in place to protect PII;

iii. demonstrate that it complies with the requirements of 8 N.Y.C.R.R. § 121.3(c) (the Parent's Bill of Rights for Data Privacy and Security);

iv. 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;

v. specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure PII is protected;

vi. specify how the third-party contractor will manage data security and privacy incidents that implicate PII including any plans to identify breaches and unauthorized disclosures, and to promptly notify the School; and

vii. describe if, how, and when data will be returned to the School, transitioned to a successor contractor, at the School's direction, deleted, or destroyed by the third-party contractor when the contract is terminated or expires.

4. Training

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

5. Reporting

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

Privacy Officer without unreasonable delay, but no more than ten (10) calendar days after such discovery.

The School will notify affected parents/guardians, eligible students, teachers and/or principals in the most expedient way possible and without delay, but no more than sixty (60) calendar days after the discovery of a breach or unauthorized release or third-party contractor notification. If, however, notification would interfere with an ongoing law enforcement investigation, or cause further disclosure of PII by disclosing an unfixed security vulnerability, the School will notify parents/guardians, eligible students, teachers and/or principals within seven (7) calendar days after the security vulnerability has been remedied, or the risk of interference with the law enforcement investigation ends.

The Principal, 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/guardians, eligible students, and district staff a process for filing complaints about breaches or unauthorized releases of student and teacher/principal PII.

6. Notifications

The Data Protection Officer will report every discovery or report of a breach or unauthorized release of student, teacher, or principal PII to the State's Chief

"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 School's information storage or computerized data which compromises the security, confidentiality, or integrity of "private information" maintained by the School must be promptly reported to the Principal and the Board of Trustees.

The Board directs the Principal, 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 School 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 School 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.

REVISED: 5/6/26