Calvert County Public Schools
1305 Dares Beach Road
Prince Frederick, MD 20678

Administrative Procedures for Policy # 1925
Regarding Student Data Governance and Privacy

I. General Provisions

A. In order to process student data properly and maintain the data privacy of individual students, all Calvert County Public School System (CCPS) employees will:

1. Access only the student data for which they have legitimate educational purpose;
2. Process and disclose student data only under authorized conditions and methods outlined in these procedures.

B. In order to minimize the student data CCPS creates, stores, collects, or processes, CCPS will abide by the following provisions:

1. Identify the minimum student data elements and personally identifiable information necessary to accomplish the specific purpose of creating and/or collecting the student data;
2. Limit the creation and/or collection of student data to the minimum information identified; and
3. Take reasonable steps to monitor the continued relevance of the student data being created and/or collected.

CCPS will provide parents the ability to opt-out of any collection and/or sharing of their student's data that does not align with these provisions.

C. In order to implement the student data governance and privacy policies and procedures, the Data Governance Board will:

1. Coordinate with executive leadership and data stewards in departments and schools to manage and maintain the requirements of the student data governance and privacy procedures; and
2. Monitor the compliance of the student data governance and privacy procedures in order to support continuous improvement efforts.

II. Definitions

A. Anonymized data – Data that has had identifying information removed so that the individuals for whom the data describe remain anonymous.

B. Critical Response Team – The group of designated CCPS personnel and system leaders who take action when potential data privacy breach incidents arise.

C. Data Breach – A data breach is any instance in which there is an unauthorized release or access of PII or other information not suitable for public release.

D. Data Governance – A formalized organizational approach to managing the processing of student data across CCPS.

E. Data Governance Board – A group designated by the Superintendent that provides data governance oversite and collaborates with CCPS executive administration and data stewards for ensuring alignment of practices with policies and procedures related to student data governance.

F. Data Management - The shared responsibility and practice of acquiring, entering, validating, updating, storing, and/or reporting of student data.

G. Data Privacy – The protection of student data from unauthorized access and data processing.

H. Data Privacy Breach Plan – The CCPS protocols that outline the identification of, reaction to, mitigation of, and communication regarding an event that potentially compromises the confidentiality, integrity, or availability of student data.

I. Data Privacy Control – An administrative, technical, or physical safeguard employed within CCPS that governs the access to and processing of student data according to the least privilege methodology.

J. Data Stewards - managers and administrators within an organization who are responsible for implementing CCPS data governance policy and maintaining data quality and security.

K. Digital Tool – Any website, application (app), or software that require an account and/or collects student data.

    1. Essential Digital Tool – An approved digital tool necessary to deliver educational programs and operational services.

    2. Supporting Digital Tool – An approved digital tool used as non-essential enrichment to students' educational experience.

L. Digital Tool Data Privacy Review – A process used to evaluate how digital tools manage and protect student data.

M. Family Educational Rights and Privacy Act (FERPA) – A federal privacy law that governs school system's processing of personally identifiable student information and delineates parental rights to their children's education records.

N. Least Privilege – The methodology whereby each user is assigned the appropriate level of access to student data needed for his/her responsibility.

O. Personally Identifiable Information (PII) – Any information that, alone or in combination, would make it possible to identify an individual with reasonable certainty.

P. Provider – 3rd party providers/vendors

Q. Record – Any material created or received by the Board, a CCPS school or office, or a school system official in connection with the transaction of CCPS business. A record includes any form of documentary material, including but not limited to paper documents, electronic documents, microfilm, drawings, maps, pictures and any other documentary material in any format, in which business information is created or maintained.

R. Records Management Practice – Any procedure for collecting or maintaining a CCPS record.

S. Student Data – Any personally identifiable data generated by students, teachers, or CCPS that is by or about an individual student in the educational setting that is saved, stored, or maintained.

T. Student Education Record – Specific records, as defined and protected by FERPA, mandated by COMAR, and outlined in CCPS Policy 1920, that are directly related to an individual student and maintained by CCPS.

III. Standards for Student Data:

A. Processed lawfully and in a transparent manner in relation to the student;

B. Collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes;

C. Stored securely in Information Systems or approved digital tools;

D. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;

E. Accurately entered, validated, and maintained;

F. Processed in a manner that provides for the appropriate privacy and safety of the student data, including protection against unauthorized or unlawful processing of the student data; and

G. Processed according to the appropriate standards and procedures indicated in CCPS Policy 1920 Records Management and CCPS Policy 3040 Technology Security.

IV. Data Governance and Privacy Program: CCPS will maintain a comprehensive student data governance and privacy program that ensures compliance with legal and regulatory mandates, establishes a commitment to public transparency about CCPS student data practices, adheres to CCPS Administrative Procedures for Policy #2305 Regarding Selection and Purchase of Materials of Instruction and Library Materials, and institutes standards for safeguarding the privacy of student data throughout CCPS.

A. Student data governance and privacy program requirements:

1. Maintain and publish annually a list of service vendors with whom CCPS has signed a contract and student data is shared;;

2. Conduct data privacy reviews of digital tools and records management practices that involve student data;

3. Incorporate data privacy controls that apply the least privilege methodology within digital tools that process student data;
4. Maintain a Data Privacy Breach Plan that includes Maryland breach notification requirements and identifies the Critical Response Team;
5. Respond to potential student data privacy incidents by convening the Critical Response Team and acting according to the Data Privacy Breach Plan;
6. Review public releases of student data in order to ensure the data is de-identified;
7. Review internal requests for access to student data in order to incorporate appropriate student data privacy controls;
8. Review the CCPS responses to external research and data sharing requests in order to incorporate appropriate student data privacy controls for all approved requests as per CCPS Policy 1315, Requests to Conduct Research in CCPS;
9. Review contracts, grants, and agreements in order to incorporate appropriate student data privacy requirements;
10. Review digital tools and authorize only those that adhere to federal, state, and local student data privacy laws and regulations;
11. Conduct annual training for all CCPS personnel on student data privacy policies, procedures, and practices;
12. Provide notification to all contractors and volunteers on student data privacy policies, procedures, and practices with expectation that these policies, procedures and practices are followed.
13. Share anonymized student data and least identifiable student PII whenever possible;

B. Collection and sharing of student data must meet one or more of the following criteria:

1. Compliant with the Maryland State Department of Education regulations pertaining to student education records as specified in COMAR;
2. Compliant with the United States' Department of Education regulations pertaining to school system reporting and accountability as specified in the Every Student Succeeds Act (ESSA);
3. Allowed under FERPA;
4. Necessary for compliance with a legal obligation to which CCPS is subject;
5. Necessary for the performance of a CCPS approved and FERPA compliant contract, grant, or agreement to provide essential curriculum, service or function;
6. Necessary in order to protect the safety of an individual student;

7. Identified as directory information as outlined in the Students' Rights, Responsibilities and Code of Student Conduct;
8. CCPS approved and COPPA compliant Supporting Digital Tool with student and guardian notification.

C. CCPS will include student data privacy protections in all grants and Provider contracts and agreements that require sharing of student data. These protections will ensure FERPA and COPPA compliance, including, but not limited to:

1. The Superintendent and/or designee will approve all grants and Provider contracts and agreements that require the processing and/or sharing of CCPS student data with an entity outside of the CCPS, notwithstanding those that are required by state and federal regulations.
2. Limiting the student data shared to the minimum necessary to fulfill the purpose of the Provider contract, grant, or agreement;
3. Mandating that student data are processed only for specified purposes;
4. Prohibiting the sharing of student data, including anonymized data, to any third party without written consent of CCPS, except as required by law.
5. Prohibiting processing of student data for commercial gain beyond that of the specified contractual purpose;
6. Prohibiting District Data from being stored outside of the United States without written approval of CCPS;
7. Mandating the reasonable administrative, technical, and physical safeguards of student data;
8. Mandating the maintenance of a data breach incident response plan and data breach notification process; and
9. Permitting a technical and/or administrative review by CCPS to monitor compliance.
10. Mandating alignment with CCPS Addendum to TERMS of SERVICE (Appendix A).

V. Data Privacy Controls, Reviews, and Monitoring

A. To incorporate data privacy controls into its digital tools and records management practices, the Data Governance Board and the department managing the system or practice will coordinate to:

1. Determine the appropriate data privacy controls for an essential digital tool that limits access to student data according to the least privilege methodology;
2. Implement data privacy controls for digital tools that store student data or records management practices;

3. Manage and maintain a process to review the implementation of and efficacy of the data privacy controls; and
4. Make improvements to the data privacy controls as necessary;

B. To review contracts, grants, and agreements in order to incorporate appropriate data privacy requirements, the Data Governance Board will coordinate with relevant departments/offices/schools to:
1. manage and maintain a contract, grant, and agreement review procedure;
2. identify contracts, grants, and agreements involving student data;
3. include contractual requirements that safeguard the privacy of student data in identified contracts and agreements; and
4. ensure that all contracts, grants, and agreements involving student data adhere to the Maryland Student Data Privacy Law.

C. To review digital tools and authorize only those that adhere to federal, state, and local data privacy laws and regulations, the Data Governance Board will coordinate with relevant departments/schools to:
1. Manage and maintain a digital tool review procedure;
2. Identify digital tools that involve student data; and
3. Authorize only those digital tools that adhere to federal, state, and local data privacy laws and regulations.

VI. The CCPS Data Breach plan covers all phases of the incident response, from reporting the breach, initial response activities, investigation of the incident, strategies for notification of affected parties, breach response review, and remediation process. The plan identifies the necessary organizational resources and required administrative support. The CCPS Data Breach plan will be periodically reviewed and tested in conjunction with disaster recovery processes to test their effectiveness and identify areas for improvement.

VII. Responsibilities

A. All CCPS Board members and school system staff will maintain the privacy of all student data by:
1. Following all approved data governance and privacy controls; and
2. Using only contracted essential digital tools or authorized supporting digital tools with students for CCPS-sanctioned activities.

B. The Data Governance Board will collaborate with CCPS executive leadership to manage and maintain the student data governance and privacy program.

C. Departments that manage essential digital tools or records management processes will collaborate with the Data Governance Board to conduct a privacy review of the system or process and incorporate appropriate data privacy controls as necessary.

D. Departments that initiate and/or sign a contract or agreement will collaborate with the Director of Procurement to review the contract or agreement for data privacy implications and include data privacy protections when appropriate.

Citations:

CCPS Policy 1315 Request to Conduct Research