HOWARD COUNTY
PUBLIC SCHOOL SYSTEM

BOARD OF EDUCATION

POLICY 3060
STUDENT DATA GOVERNANCE AND PRIVACY

Effective: July 1, 2018

I. Policy Statement

The Board of Education of Howard County recognizes its responsibility as stewards of student data to safeguard personally identifiable student data throughout the Howard County Public School System (HCPSS). As a local education agency, the Board also acknowledges that the appropriate processing of student data is necessary for the fulfillment of federal, state, and local legal requirements.

The Board further recognizes the need for a comprehensive policy to address student data governance and privacy that confirms compliance with legal and regulatory mandates, establishes a commitment to public transparency about HCPSS student data practices, and institutes standards for safeguarding the privacy of student data throughout the HCPSS.

II. Purpose

The purpose of this policy is to establish standards and procedures for maintaining a student data governance and privacy program that aligns with federal, state, and local laws and regulations.

III. Definitions

Within the context of this policy, the following definitions apply:

A. Authorization – The approval to process student data in accordance with HCPSS data privacy controls and federal, state, and local laws and regulations.

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

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

D. Data Privacy – The protection of student data from unauthorized data processing.

E. Data Privacy Assessment – A process used to evaluate how a records management process or enterprise information system processes student data.

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

G. Data Privacy Incident Response Plan – The HCPSS protocols that outline the reaction to, mitigation of, and communication regarding an event that potentially compromises the confidentiality, integrity, or availability of student data.

H. Data Processing – The creation, collection, use, maintenance, release, disclosure, and/or destruction of student data.

I. De-identified Data – Data that, based on federal and state standards, the HCPSS has determined cannot reasonably used to identify an individual person.

J. Digital Tool – Any website, application (app), or software that requires an account.

1. Essential Digital Tool – A Superintendent/Designee approved digital tool necessary to deliver educational programs and operational services.

2. Supplementary Digital Tool – A Superintendent/Designee approved digital tool used as non-essential enrichment to students' educational experience.

K. Enterprise Information System – An HCPSS technology platform that processes systemwide student data.

L. Essential – That which is necessary for the delivery of educational programs and operational services (such as, but not limited to, the student information system, the learning management system, and the library media system).

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. Parent – Any one of the following, recognized as the adult(s) legally responsible for the student:

1. Biological Parent – A natural parent whose parental rights have not been terminated.

2. Adoptive Parent – A parent who has legally adopted the student and whose parental rights have not been terminated.

3. Custodian – A person or an agency appointed by the court as the legal custodian of the student and granted parental rights and responsibilities.

4. Guardian – A person who has been placed by the court in charge of the affairs of the student and granted parental rights and responsibilities.

5. Caregiver – An adult resident of Howard County who exercises care, custody, or control over the student but who is neither the biological parent nor legal guardian as long as the person satisfies the requirements of the Education Article §7-101(c) (Informal Kinship Care).

6. Foster Parent – An adult approved to care for a child who has been placed in their home by a state agency or a licensed child placement agency as provided by the Family Law Article, §5-507.

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

Q. Record – Any material created or received by the Board, an HCPSS school or office, or a school system official in connection with the transaction of HCPSS 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 an HCPSS record.

S. School System Official – A person employed by the HCPSS; or a person or organization contracted by the HCPSS to perform a special task (such as an attorney, auditor, school resource officer, medical consultant, or therapist).

T. Student Data – Any PII relating to an identified or identifiable student.

U. Student Education Record – Specific records, as defined and protected by FERPA, mandated by COMAR, and outlined in HCPSS Policy 9050, that are directly related to an individual student and maintained by the HCPSS.

IV. Standards

A. Student data will be:

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

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

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

4. Accurate and, where necessary, kept up to date; and

5. Processed in a manner that provides for the appropriate privacy of the student data, including protection against unauthorized or unlawful processing and using appropriate technical or organizational data privacy controls; and

6. Processed according to the appropriate standards and procedures indicated in HCPSS Policy 3050 Records Management and HCPSS Policy 3040 Technology Security.

B. The HCPSS will only collect and/or share student data if the collection and/or sharing is:

1. At the consent of the student/parent for one or more specific purposes;

2. Necessary for the performance of an HCPSS approved and FERPA compliant contract, grant, or agreement to provide an essential service or function such as, but not limited to, the student information system, the learning management system, and the library media system;

3. Necessary for compliance with a legal obligation to which the HCPSS is subject;

4. Necessary in order to protect the safety of an individual student;

5. Necessary for the exercise of the official authority vested in the HCPSS, including compliance with the Maryland State Department of Education regulations pertaining to student education records as specified in COMAR and compliance with the United State's Department of Education regulations pertaining to school system reporting and accountability as specified in the Every Student Succeeds Act (ESSA); or

6. Allowed under FERPA.

C. The HCPSS will include student data privacy protections in all contracts, grants, and agreements requiring the sharing of student data. These protections will include, but are not limited to:

1. Limiting the student data shared to the minimum necessary to fulfill the purpose of the contract, grant, or agreement;

2. Mandating that student data are processed only for specified purposes;

3. Prohibiting disclosure of student data to an additional party;

4. Prohibiting processing of student data for commercial gain beyond that of the specified contractual purpose;

5. Mandating the reasonable administrative, technical, and physical safeguards of student data;

6. Mandating the maintenance of a data breach incident response plan and data breach notification process; and

7. Permitting a technical and/or administrative review by HCPSS to monitor compliance with the contractual agreements.

D. The Board of Education will approve all contracts, grants, and agreements that require the processing and/or sharing of HCPSS student data with an entity outside of the HCPSS, notwithstanding those that are required by state and federal regulations as described in Section IV.B.1–5.

E. The HCPSS will maintain a comprehensive student data governance and privacy program that confirms compliance with legal and regulatory mandates, establishes a commitment to public transparency about HCPSS student data practices, and institutes standards for safeguarding the privacy of student data throughout the HCPSS. The student data governance and privacy program requires the HCPSS to:

1. Manage and maintain a method to collect and respond to parent inquires about student data governance and privacy practices;

2. Manage and maintain a method for engaging with offices throughout the HCPSS to encourage the use of digital technologies and data governance strategies that sustain and/or enhance student data privacy;

3. Maintain and publicize an inventory of the student data elements the HCPSS collects with an explanation and/or legal or regulatory authority;

4. Maintain and publicize an inventory of the contracts, grants, agreements, and digital tools that involve student data;

5. Conduct data privacy assessments of enterprise information systems and records management practices that involve student data;

6. Incorporate data privacy controls that apply the least privilege methodology into enterprise information systems and records management practices that process student data;

7. Maintain a Data Privacy Incident Response Plan that includes Maryland breach notification requirements and identifies the critical response team;

8. Respond to potential student data privacy incidents by convening the critical response team and taking action according to the Data Privacy Incident Response Plan;

9. Review public releases of student data in order to ensure data is de-identified;

10. Review internal requests for access to student data in order to incorporate appropriate student data privacy controls and disclosure avoidance techniques;

11. Review the HCPSS responses to external research and data sharing requests in order to incorporate appropriate student data privacy controls for all approved requests;

12. Review contracts, grants, and agreements in order to incorporate appropriate student data privacy requirements;

13. Review digital tools and authorize only those digital tools that adhere to federal, state, and local student data privacy laws and regulations;

14. Conduct annual training and/or notification for all HCPSS personnel, contractors, and volunteers on student data privacy policies, procedures, and practices; and

15. Report biannually to the Board on activities that impact student data privacy, including parental inquiries, data privacy controls, and relevant legislative and regulatory changes.

V. Responsibilities

A. All HCPSS Board members and school system officials 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 supplemental digital tools with students for HCPSS-sanctioned activities.

B. The Superintendent/Designee will collaborate with the HCPSS executive leadership to manage and maintain the student data governance and privacy program.

C. Offices that initiate or implement an enterprise information system or records management process will collaborate with the Superintendent/Designee to conduct a data privacy assessment of the system or process and incorporate appropriate data privacy controls as necessary.

D. Offices that initiate and/or sign a contract or agreement will collaborate with the Superintendent/Designee to review the contract or agreement for data privacy implications and include data privacy protections when appropriate.

E. Based upon the recommendation of the Superintendent/Designee, the Board will approve all contracts, grants, and agreements that require the processing and/or sharing of HCPSS student data with an entity outside of the HCPSS, notwithstanding those that are required by state and federal regulations as described in Section IV.B.1–5.

F. The Superintendent/Designee will review the policy every two years to determine whether to recommend revision to this policy and implementation procedures.

VI. Delegation of Authority

The Superintendent is authorized to develop procedures for the implementation of this policy.

VII. References

A. Legal
Every Student Succeeds Act (ESSA), 20 U.S.C. §6301
Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232(g)
Privacy Act of 1974, 5 U.S.C. § 552(a)
Maryland Personal Information Protection Act, Md. Code Com. Law § 4-3501 *et seq*.
The Annotated Code of Maryland, Education Article, §4-131, Student Data Privacy Act of 2015
COMAR 13A.08.02. Student Records

B. Other Board Policies
Policy 2070 Ethics
Policy 3040 Technology Security
Policy 3050 Records Management
Policy 4050 Procurement of Goods and/or Services
Policy 7010 Personnel Records
Policy 8080 Responsible Use of Technology and Social Media
Policy 9050 Student Records

C. Relevant Data Sources

D. Other
Department of Homeland Security: Privacy Impact Assessment Official Guidance
National Institute of Standards and Technology: Publication 800-53
Office of Management and Budget: Circular A-130
HCPSS Ethics Regulations

VIII. History

ADOPTED: June 7, 2018
REVIEWED:
MODIFIED:
REVISED:
EFFECTIVE: July 1, 2018

HOWARD COUNTY
PUBLIC SCHOOL SYSTEM

POLICY 3060-IP
IMPLEMENTATION PROCEDURES

STUDENT DATA GOVERNANCE AND PRIVACY

Effective: July 1, 2018

I. General Provisions

A. In order to process student data properly and maintain the data privacy of individual students, all Howard County Public School System (HCPSS) Board members and school system officials will:

1. Process only the student data to which they have authorized access;

2. Use only authorized methods to process student data; and

3. Disclose student data only under authorized conditions, through authorized methods, and to authorized recipients.

Authorization will be determined through the procedures for conducting data privacy assessment and implementing data privacy controls as outlined in Section III.

B. In order to minimize the student data that the HCPSS creates and/or collects, HCPSS departments will:

1. Document the legal authority and specific purpose for creating and/or collecting student data;

2. Identify the minimum student data elements necessary to accomplish the specific purpose of creating and/or collecting the student data;

3. Limit the creation and/or collection of student data to the minimum information identified;

4. Take reasonable steps to monitor the continued relevance of the student data being created and/or collected; and

5. Provide parents the ability to opt-out of any collection and/or sharing of their student's data that does not align with the provisions specified in Section IV.B. of the policy.

C. In order to implement the student data governance and privacy program, the Superintendent/Designee will:

1. Coordinate with executive leadership and departments/offices to manage and maintain the requirements of the student data governance and privacy program that are delineated in Section IV.D. of the policy;

2. Measure the effectiveness and fidelity of the student data governance and privacy program in order to support continuous improvement efforts; and

3. Develop and implement continuous improvement efforts based on the measured effectiveness and fidelity of the data privacy program.

II. Parent Inquiries and Notifications

A. To manage and maintain communications with parents about the HCPSS student data governance and privacy practices, the Superintendent/Designee will implement methods of annual notification and ongoing communications.

B. The annual notifications and ongoing communications will include, but are not limited to:

1. Publicizing the process for parents to opt-out of the collection and/or sharing of their student's data when the collection and/or sharing does not align with the provisions specified in Section IV.B. of the policy.

2. Publicize a list of all current enterprise information systems, records management practices, contracts, grants, agreements, and digital tools that involve student data and the student data involved.

III. Data Privacy Assessments and Controls

A. To conduct data privacy assessments on enterprise information systems and records management practices, the Superintendent/Designee will coordinate with the department initiating or implementing the system or practice to:

1. Document the student data that the enterprise information system or records management practice creates, collects, uses, maintains, and/or discloses;

   a. If the information system or records management practice generates new information, the privacy assessment will document the types and purpose of the student data generated.

   b. If the information system or records management practice receives information from another system or practice, the privacy assessment will document the types and sources of the student data received.

2. Document the legal authority and specific purposes of the student data being created, collected, used, maintained, and/or disclosed by the enterprise information system or records management practice;

3. Document the nature and scope of legally authorized usages and disclosures of student data;

4. Document any relevant records retention schedules for the student data being maintained according to the Records and Information Disposition Schedules; and

5. Document the procedure for individuals to opt in/out, when applicable, of the creation, collection, use, maintenance, and/or disclosure of student data.

B. To incorporate data privacy controls into its enterprise information systems and records management practices, the Superintendent/Designee and the department initiating or implementing the system or practice will coordinate to:

1. Determine the appropriate data privacy controls for an enterprise information system or records management practice that limit access to student data according to the least privilege methodology;

2. Implement data privacy controls for specific enterprise information systems 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.

IV. HCPSS Data Privacy Incident Response Plan

A. To maintain a Data Privacy Incident Response Plan that includes Maryland breach notification requirements and aligns with the HCPSS Technology Security Incident Response Procedures, the Superintendent/Designee will:

1. Review its Data Privacy Incident Response Plan at least annually to revise and update the plan according to current nationally benchmarked best practices in risk management, data security, and data privacy;

2. Conduct an annual drill of the Data Privacy Incident Response Plan with all relevant HCPSS offices and departments, and modify the plan according to procedural gaps exposed through the drill process; and

3. Collaborate with executive leadership and departments/offices to align the Data Privacy Incident Response Plan with the HCPSS Continuity of Operations Plan and Disaster Recovery Plan.

B. If a potential data privacy incident arises, the critical response team will:

1. Convene to assess the potential data privacy incident;

2. Take coordinated action according to the Data Privacy Incident Response Plan;

3. Notify individuals affected according to the regulatory mandates of the Maryland data breach notification requirements; and

4. Use the lessons learned from the incident response to improve the processes of identifying, defending, detecting, responding to, and recovering from future potential incidents.

V. Data Privacy Reviews

A. To review contracts, grants, and agreements in order to incorporate appropriate data privacy requirements, the Superintendent/Designee will:

1. Coordinate with relevant departments/offices to manage and maintain a contract, grant, and agreement review procedure;

2. Coordinate with relevant departments/offices to identify contracts, grants, and agreements involving student data;

3. Coordinate with relevant departments/offices to include contractual requirements that safeguard the privacy of student data in identified contracts and agreements; and

4. Coordinate with relevant departments/offices to ensure that all contracts, grants, and agreements involving student data adhere to the Maryland Student Data Privacy Law.

B. To review supplemental digital tools and authorize only those supplemental digital tools that adhere to federal, state, and local data privacy laws and regulations, the Superintendent/Designee will:

1. Coordinate with relevant departments/offices to manage and maintain a digital tool review procedure;

2. Coordinate with relevant departments/offices to identify digital tools that involve student data; and

3. Coordinate with relevant departments/offices to authorize only those digital tools that adhere to federal, state, and local data privacy laws and regulations.

VI. History

ADOPTED: June 7, 2018
REVIEWED:

MODIFIED:
REVISED:
EFFECTIVE: July 1, 2018