RULE 4008

PERSONNEL: General

Board Data Governance

I. Purpose

Data maintained on Baltimore County Public Schools' (BCPS) information systems is the property of the school system, and BCPS exercises control over the access to data. This rule establishes guidelines for the management of school system data, assigns stewardship responsibilities for BCPS data, establishes the standards for custodianship of such data and sets forth procedures for storage, retrieval, destruction, backup and access, as needed, to ensure proper management and protection of data.

II. Definitions

A. *Authorized Users* – The Board, Board employees and approved consultants, independent contractors, volunteers, government agencies and others who have been permitted access to Board data.

B. *Data* – A general term used to refer to the school system's information resources and administrative records, including, but not limited to data in any form, including print, electronic, audio-visual, backup and archived data.

C. *Data Governance* – Systemwide controls to ensure the confidentiality, integrity, accessibility, availability and quality of data.

D. *Data Integrity* – Overall completeness, accuracy and consistency of data.

E. *Data Steward* – An individual identified as having the responsibility of maintaining standards for the security, integrity and availability of data in a specific content area.

F. *Data Stewardship* – The formalization of accountability for the management of data resources.

III. Responsibilities

A. Data Governance Committee (DGC)

1. The Data Governance Committee (DGC) is a committee established by the Superintendent and charged with the task of the development

of procedures and enforcement of the school system's data governance policy.

2. The DGC will have the authority to:
   a. Establish, maintain and enforce standards and procedures for the management of BCPS information assets;
   b. Identify individuals to serve as data stewards;
   c. Coordinate data steward activities; and
   d. Support data stewards to resolve data issues and conflicts.

B. Data Stewards

Data stewards have the primary administrative and management responsibilities for segments of the data within their specific content area and will be responsible for:

1. Maintaining the data] in their content domain in compliance with the Board's Data Governance Policy;
2. Approving requests for access to data within their content area, specifying the appropriate access procedure and ensuring appropriate access rights and permissions;
3. Ensuring that the authorized user of the data for which the steward is responsible is aware of information-handling procedures; and
4. Ensuring proper use and integrity of data.

C. The Department of Information Technology

The executive director of information technology is responsible for developing and implementing security procedures and controls that:

1. Provide security support for all systems and authorized users including virus, malware, spyware, phishing and spam protection;
2. Incorporate security mechanisms to guard against unauthorized access to data that are transmitted over a communications network;
3. Ensure data integrity by implementing monitoring, maintenance and backup systems; and
4. Develop a written plan for responding to a data breach.

D. The Department of Organizational Effectiveness

The Department of Organizational Effectiveness, in cooperation with the Department of Information Technology, will be responsible for ensuring all employees are informed annually of the data governance policy and are aware of their responsibilities under this policy, rule and implementing procedures.

E. Principals and Office Heads

BCPS principals and office heads are responsible for:

1. Reviewing and approving all requests for their employees' access authorizations;
2. Providing employees with the training needed to properly use computer systems and to ensure compliance with the data governance policy, this rule and school system procedures;
3. Reporting promptly to the data governance committee the lose or misuse of BCPS data;
4. Following existing approval processes for the selection, purchase and implementation of any data system/software to manage information; and
5. Following all BCPS privacy and security policies and procedures as well as federal and state laws and regulations.

F. Authorized Users

An usher who has been authorized to access data shall adhere to the following:

1. Confidentiality: respecting the confidentiality and privacy rights of individuals whose data they may access;
2. Ethics: observing the ethical restrictions that apply to data in which they have access;
3. Policy adherence: abiding by applicable laws and Board policies, rules and procedures with respect to access, use, protection, proper disposal and disclosure of data; and
4. Responsible access: accessing and using institutional data only as required in the conduct of school system business.

IV. Data Sharing

A. The BCPS data sharing/student privacy requirements shall apply to all vendors or software, applications and/or services that require access to the personally identifiable information of BCPS students.

B. The data sharing/student privacy requirements shall be posted on the school system's Web site.

V. Data and Records Retention

Data and records shall be retained and disposed of in accordance with the school system's records retention schedule and electronically stored information (ESI) procedures.

VI. Discipline

A. Any employee deemed to have violated the Board's data governance policy, this rule or school system procedures may be subject to suspension of his/her system access privileges and disciplinary action, up to and including termination.

B. In the case of a consultant, independent contractor, volunteer and/or outside affiliate, the contracting office head will make a decision on whether services should be terminated.

Legal References:
15 U.S.C. §§ 6501–6505, *Children's Online Privacy Protection Act of 1998*
18 U.S.C. §2701-2711, *Electronic Communications Privacy Act*
20 U.S.C. §1232g, *Family Educational Rights and Privacy Act (FERPA)*
Annotated Code of Maryland, General Provisions Article §§4-101 to 4-601 (Public Information Act)
Annotated Code of Maryland, State Government Article §10-610, *Records Management Programs*
COMAR 13A.08.02, *Student Records*

Related Policies:
Board of Education Policy 3170, *Performance Management System for Continuous Improvement*
Board of Education Policy 4002, *Obligations of the Employees of the Board of Education of Baltimore County*
Board of Education Policy 4100, *Employee Conduct and Responsibilities*
Board of Education Policy 4104, *Technology Acceptable Use Policy (TAUP) for Employees and Approved Non-Employees*
Board of Education Policy 5230, *Student Records*
Board of Education Policy 6202, *Technology Acceptable Use Policy (TAUP) for Students*
Board of Education Policy 8361, *Statement of Purpose and Policy*
Board of Education Policy 8410, *Reporting Fraud, Waste, Abuse or Unlawful Acts*

Related Rules: Superintendent's Rule 2373, *Public Information Act Requests*
Superintendent's Rule 4104, *Technology Acceptable Use Policy (TAUP) for Employees and Approved Non-Employees*
Superintendent's Rule 5230, *Student Records*

Rule Superintendent of Schools
Approved: 12/06/11
Edited: 09/23/14 (*Effective: 10/01/14*)
Revised: 08/07/18