FREDERICK COUNTY PUBLIC SCHOOLS	Reg. No. 200-32
Subject: DATA SECURITY	**Issued: 7/13/17**
Preparing Office: Office of the Superintendent	**Amended:**

I. Policy 208

II. Procedures

A. The Frederick County Public Schools (FCPS) Written Information Security Program (WISP), in accordance with Board of Education (Board) Policy 208 *Data Security*, shall maintain a documented record of the administrative, technical, and physical controls determined to be appropriate to safeguard personal information under the comprehensive information security program. The FCPS WISP will include:

1. Definitions and framework which determine the methods of providing for the security of the confidentiality, integrity and accessibility of student and employee information.
2. Determining factors for the types and quantity of sensitive information covered by the program.
3. Size, scope and type of organizational unit required to safeguard the personal information under the comprehensive information security program.
4. The amount of resources made available to meet the determined obligations.

B. The FCPS WISP will include guidelines necessary to mitigate within reasonably acceptable levels and communicate the risk profile for FCPS Student and Staff Information Systems (SSIS), by ensuring the systems are configured to meet an acceptable minimum level of IT security controls and data privacy practices.

1. The FCPS WISP will define the required legal and regulatory controls that must be in place to provide the base standard of IT security required for an FCPS information system. The controls detailed within the FCPS WISP will be primarily sourced from the State of Maryland Information Security Policy and Information Technology Security Plan (ITSP) Guidelines and Instructions for Maryland State Agencies, as released and updated by the Maryland State Department of Information Technology (DoIT) and supplemented by the National Institute of Standards and Technology (NIST) Special Publication 800 series.
2. In the event a system has valid justification to deviate from established controls, the DTI will review, document and provide final approval for waiving the requirement based on the requirements established within the FCPS WISP.

C. Board Policy 207 *Data Breach Notification* and FCPS Regulation 200-31 *Data Breach Response Process* provide the guidelines which prescribe the required actions FCPS must take in addressing the unauthorized acquisition of computerized data that compromises the confidentiality, integrity or accessibility of information entrusted to FCPS.

The Department of Technology Infrastructure (DTI) will maintain within the FCPS WISP the clearly documented processes and procedures necessary to take swift and decisive actions in the event a suspected incident is reported.

D. FCPS Regulations 300-45 *Responsible Use of Digital Technology – Staff* and 400-73 *Responsible Use of Digital Technology – Student*s, establish the expected rules of behavior for the use of technology and digital resources provided by FCPS. The Digital Environment Committee will ensure these regulations are maintained in a manner which reflects the ever changing technology environment and are communicated to students and staff.

E. The Digital Environment Committee will maintain an Information Technology Security Awareness Training program as defined in the FCPS WISP, providing a common understanding of data privacy expectations, raise awareness of legal and regulatory responsibilities, and provide best practices to curtail inadvertent violations of sensitive information.

F. The Director of Technology Infrastructure will coordinate and facilitate the IT functions required to meet all county, state and federal technology audit responsibilities. The results of all Independent Verification and Validation (IV and V) audits and the execution of the requirements defined in the WISP will be provided in an annual IT security health report to the FCPS Superintendent.

Approved:

Original signed by

_____

Theresa R. Alban
Superintendent