Building the Future CCPS Carroll County Public Schools	**Data Governance**	**Administrative Regulation #**	EH
		Implemented	August 14, 2019
		Reviewed/Updated	
Page 1 of 6			
Procedure Owner	Superintendent		

Administrative Regulation

1. Purpose

To establish a Data Governance Program oversight structure and provide guidance for the system Data Governance Plan.

2. Scope

This regulation is applicable to all employees, temporary employees, and contractors of the school system. The regulation must be used to assess the risk to system data associated with conducting business.

This regulation shall provide oversight on the following:

- Data Collection
- Access Control
- Data Disclosure
- Data Breach
- Records Retention
- Data Quality and Integrity
- Transparency
- Non-Disclosure Assurances for Employees
- Acceptable Use Agreements
- Data Security and Privacy Training for Employees

3. Prerequisites

This regulation works in conjunction with numerous other system Policies and Regulations. In the event that related regulations are not clearly aligned with the systems Data Governance Plan, the procedures, standards, and guidelines associated with this regulation shall have predominance.

Associated Policies:

- AF - Student Data Privacy Policy
- EHB - Data Records Retention
- IIAA Selection, Evaluation, and Adoption of Instructional Materials.
- IJND - Telecommunications Policy
- ILB - Test Security and Data Reporting
- JR - Disclosure of Directory Information
- JRB - Protection of Pupil Rights-Surveys, Physical Exams, Marketing Personal Information, and Inspection of Certain Material
- JRC - Family Educational Rights

- JRD - Use of Student's Photograph, Video Image, or Voice for Educational, Informational or Public Relations Purposes

4. Responsibilities

The Data Policy Committee shall be responsible for establishing and sustaining the system Data Governance Program.

The Data Governance Committee is focused on establishing and maintaining system-wide processes and guidelines regarding data collection, quality, availability and use. It does this by:

The Data Governance Coordinator, appointed by the Superintendent, is responsible for leading the overall direction and implementation of the Data Governance Program.

Data Stewards are responsible for implementing data governance policies and standards and maintaining data quality and security.

5. Definitions

Acceptable Use Agreement – The Acceptable Use Agreement is a document that stipulates practices and constraints to which a user must agree before being permitted to access computer systems or data.

Access Controls – Access controls limits entry to information system resources to authorized users, programs, processes, or other systems. Components of an access control system include, for example, physical access, authentication systems, and file encryption.

Breach – A data breach is the intentional or unintentional release of secure information to an untrusted environment.

Breach Notification Plan – A Breach Notification Plan is a systematic, consistent, and documented method for providing stakeholder notification in the event security incident has resulted in a breach. The Breach Notification Plan work in conjunction with the Security Incident Response Plan.

Confidentiality – Confidentiality relates to the management of another individual's personally identifiable information. Confidentiality refers to the obligations of those who receive personal information about an individual to respect the individual's privacy by safeguarding the information

Data Collection – Data collection is the process of gathering and recording information. The process of gathering and recording data results in the creation of a record.

Data Quality and Integrity – Data quality and integrity is the process for ensuring, to the greatest extent possible, that information is accurate, relevant, timely, and complete for the purposes for which it is to be used.

Data Stewards – Data stewards are professional staff who are responsible for implementing data governance policies and standards and maintaining data quality and security. It is the data steward's responsibility to ensure that information is collected, maintained, used, and disseminated in a way that respects privacy, ensures confidentiality and security.

Disclosure – Data disclosure means to permit access to or the release, transfer, or other communication of data by any means. Disclosure can be authorized, such as when a parent or an eligible student gives written consent to share education records with an authorized party. Disclosure can also be unauthorized or inadvertent (accidental). An unauthorized disclosure can happen due to a data breach or a loss. An accidental disclosure can occur when data released in public aggregate reports are unintentionally presented in a manner that allows individual students to be identified.

Non-Disclosure Assurances – Non-Disclosure Assurances for Employees are practices and constraints regarding the disclosure of confidential records. The assurances are intended to minimize the risk of unauthorized or inadvertent disclosure due to human error and misuse of information.

Privacy – Privacy relates to individual autonomy and each person's control over their own information. This includes each person's right to decide when and whether to share personal information, how much information to share, and the circumstances under which that information can be shared

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

Risk Assessment – Risk assessment is the process of identifying: (1) all assets an organization possesses, (2) all potential threats to those assets, (3) all points of vulnerability to those threats, (4) the probability of potential threats being realized, and (5) the cost estimates of potential losses. Risk assessment enables an organization to at least consider the range of potential threats and vulnerabilities it

faces, and is the first step in effectively securing an information and technology system.

Security – Security means protecting information (in all media) through appropriate administrative, technical, and physical security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Security Incident Response Plan – A Security Incident Response Plan is a systematic, consistent, and documented method of approaching and managing situations that may have a negative impact on the confidentiality, integrity, or availability of system applications or data.

Transparency – Transparency is the obligation to provide notice to the individuals regarding the collection, use, dissemination, and maintenance personal and public information.

6. Procedure

A. The Superintendent shall establish a Data Policy Committee. The committee shall be comprised of seven key members of the Superintendent's Executive Leadership Team (ELT) including the Data Governance Coordinator.

   The Data Policy Committee will:
   - Develop and review Data Governance Policy;
   - Resolve issues identified by the Data Governance Committee;
   - Review data procedures and major data-related decisions proposed by the Data Governance Committee; and
   - Hold program offices accountable for participating in the Data Governance Program and adhering to the Data Governance Policy.

   The Data Policy Committee shall inform and consult with the Data Governance Committee on issues in governance, professional development needs, and concerns of data stewards. As needed, the Data Policy Committee may call upon other CCPS employees to serve in an advisory capacity.

   The Data Policy Committee shall meet, at minimum, biannually.

B. The school system will maintain a Data Governance Committee. The Data Governance Committee with be comprised of the Superintendent's Executive Leadership Team. The Data Governance Committee will:

- Establish, maintain, and enforce standards and procedures for the management of CCPS data.
- Identify individuals to serve as data stewards.
- Support data stewards to resolve data issues and conflicts.
- Hold their program area staff accountable for participating in the Data Governance Program and adhering to the Data Governance Policy.

Individual Data Governance Committee members are designated as the owners of the data in systems and applications that fall under their program areas.

The Data Governance Committee will meet quarterly as an item on regularly scheduled ELT meetings.

C. The Data Governance Coordinator manages the establishment, monitoring, improvement, documentation, and training for the Data Governance Program, as well as for data policies and processes. The coordinator serves as the liaison among data governance groups and members to ensure effective communication. The coordinator also is responsible for identifying program, process, and technological enhancements that will improve data quality and data use and eliminate redundant effort.

D. Data stewards are professional staff who have been identified by the Data Governance Committee. They have responsibility and authority for a given area of data, from collection through use, regardless of where those data reside across the agency. Data Stewards are responsible for:
   - Determining how data are defined, collected, audited, and reported to meet program area requirements and the agency's and external stakeholders' data use needs;
   - Informing how metrics are calculated and how the source system of record is determined for external reporting;
   - Reviewing and approving data releases;
   - Collaborating with other Data Stewards to ensure that the data meet all agency data use needs;
   - Communicating program area needs for data privacy, security, and archiving;
   - Documenting core processes regarding data collection, calculation, and reporting;
   - Ensuring that metadata are documented and maintained;
   - Identifying critical data issues that impede data quality and use;
   - Participating in work groups to identify, propose, and implement resolutions to critical data issues;
   - Tracking federal, state, and other pending legislation or regulations involving data elements in their domains and communicating the potential effects;

- Evaluating and proposing process changes to improve data quality and/or agency efficiency;
- Communicating data governance policies, processes, and decisions to others within the program area.

7. Reports

The CCPS Data Governance Plan shall include procedures, standards, and guidelines that oversee the following lifecycle components:

A. The collection or generation of data
B. Data maintenance: including a data dictionary, inventory, quality and security
C. Data access, breech, use, disclosure, and transparency
D. Data retention and disposal

8. Expiration/Review

Every three years or as needed

9. Effective Date

August 14, 2019