PROPOSED POLICY

DATA GOVERNANCE POLICIES AND PROCEDURES	5.91

Data Governance Committee

Name	Department
Chris Padget	Superintendent
Danny Hooper	Testing & Counseling
Geoff Jones	Technology
Lori Beasley	Special Education
Donna McCoy	Child Nutrition
Dennis Brand	Career Tech
Jon Murphy	Transportation
Darryl Brooks	AHS Principal
Carmen Neiswanger	HES Principal
Ginger Feltman	HES Counselor

Committee Responsibilities

In the current Education environment, there is a vast amount of data that is collected, stored, analyzed, and sometimes incorporated into other various programs in order to provide up to the minute analysis of data in the fast-paced world of Technology. To ensure that this data is being monitored and protected with a system of checks and balances, the Henry County School System has implemented a Data Governance Committee with guidance from the Alabama State Department of Education. This committee is charged with the creating policies that will ensure the protection and management of data, reviewing those policies to enhance any areas of needed improvement, and making decisions as to what parties has access to this information. The committee will meet at least once annually in which each meeting will be documented.

Policies and Standards

Each Program Manager is responsible for implementing data governance policies and standards to maintain data accuracy and security. The Technology Coordinator supervises policies and procedures to ensure that state and federal guidelines are being met. Permission levels are determined by the Program Managers to ensure that the levels of access to data is within the scope of the person's assigned

responsibilities. Program Managers have the authority to correct data inaccuracies that ensure that access to personally identifiable information is minimized in order to protect privacy and confidentiality.

Program Managers

Program Managers may include Central Office Personnel and Supervisors, School Nurses, High School Athletic Directors, and Principals. Local School Personnel that may assist Program Managers with the collection of data entry and maintenance may include Principals, Assistant Principals, Counselors, Secretaries, Lunchroom Managers, and Data Entry Clerks.

Program Manager Roles

Activity Area	Program Manager	Role(s)
Information Now™ Student Database (Student Grades, Schedules, Demographics, Attendance, Discipline, Child Nutrition, Transportation, Guardian Contact Info)	Geoff Jones	Database Administrator, State Reporting liaison between ALSDE & Schools, End User Training, End-User Security Manager for Personnel to access Confidential Data
SETSWeb™	Lori Beasley, Janet Cooper, Shari Bonner	Manage Special Education Records
C2C™ Alabama Athletic Eligibility Program	High School Administrators, Athletic Directors	Data Input Determining Athletic Eligibility of High School Athletes
State-Mandated Student Assessment Portals	Danny Hooper	Overseeing Administration of Statewide Assessments, Build Test Rosters, Disseminate Data to Parents, Students, Teachers as deemed appropriate
Accountability Web Portal	Danny Hooper, Chris Padget, Kevin Sanders	Maintains Permissions to Access State Accountability Reports, Cohorts, etc.
Dibels	Lori Beasley	Overseeing K-2 Early Literacy Reading Skills
Renaissance Place™ / AR™ Reading Programs	Geoff Jones (Data Manager)	Overseeing Formative Assessment Program for Grades K-8
Alabama Career Planning – KUDER™	Dennis Brand	Overseeing Student's 4 Year Plan, Resumes, College Plan

Franklin™, Newton™, WinFSFR™ – MCS CNP Software Programs	Donna McCoy (CNP Supervisor), Geoff Jones (Data Manager)	Determines Child Nutrition Eligibility and Data Accuracy
Student Cumulative Files	Danny Hooper	Overseeing Store Student Educational Records
Attendance and Discipline Records	Dennis Brand	Overseeing Store Student Attendance and Discipline Records
SchoolCast™	Chris Padget, Geoff Jones, School Principals & Assistant Principals	Overseeing Phone Messaging System for Attendance, School Events, Safety Alerts
Global Scholar (Scantrons)	Chris Padget, Kevin Sanders	Overseeing Local Formative and Summative Assessments to Screen & Track Student Progress
AdvancEd (ASSIST™)	Chris Padget, Kevin Sanders	Overseeing Web-based program to broaden & Sharpen thinking about Continuous Improvement, Performance, & Accreditation
LeadAlabama / Val Ed	Chris Padget, Kevin Sanders	Overseeing formative online evaluation system for Educational Leaders, collaborative dialog, Professional Learning Plan, Evidence Collection / 360° Assessment, the Vanderbilt Assessment of Leadership in Education (VAL-ED). LEADAlabama is used to evaluate Certificated Central Office Administrators, Principals, Assistant Principals, & other Specialty Area Administrators.
Educate Alabama	Chris Padget, Kevin Sanders	Overseeing Local Formative Evaluation Online Processes for Teachers, Educators, and Instructional Leaders serving Alabama Public Schools.
STIPD Teacher Administration	Chris Padget, Kevin Sanders	Administration of Teacher Access to Professional Development.

OdysseyWare	Chris Padget	Credit Recovery Software
Atriumm™ Library Management System	School Media Specialists, Geoff Jones (Data Mgmt.)	Overseeing Library Management System
Virtual Alabama	Jon Murphy	School Safety Plans and Online Administration
School Status	Chris Padget	Data Compilation

Policies and Procedures

The Mission for the Henry County Board of Education's Data Use and Governance Policy is to outline the ways that we are protecting the information being stored and accessed today, as well as conforming to new ways that will help us protect tomorrow's data as well in this fast-paced technological world. The ideal Vision is to help establish a clear and concise way to efficiently detail and safeguard the system of data governance while keeping all K-12 Data confidential throughout its lifespan. Data will only be accessed and shared during times of need by personnel with appropriate security levels or when written consent from Students and/or Parents or Guardians is obtained. The procedures outlined in this document are designed to adhere to FERPA (Family Educational Rights and Privacy Act), as well as other Federal guidelines described below.

Goals and Success Measures

Our main priority is to ensure that all data collected, managed, stored, transmitted, used, reported, and destroyed by the district is done so in a way to preserve and protect individual and collective privacy rights and ensure confidentiality and security of collected data.

Goals and Success Measures include the following:

1) Improved data accuracy by continuously reviewing our student data management system.
2) Improved data usability, resulting from monitoring data content for consistency with the organizational Vision and stakeholder's needs.
3) Improved data redundancy, accomplished by avoiding unnecessary duplication of data collection efforts.
4) Increased data security, gained by designing a Data Governance Plan and applying the appropriate levels of security based on the level of data sensitivity.

Funding

Funding for the Data Governance Program will be secured by the school Superintendent at the request of the Technology Coordinator and/or the Data Governance Committee.

Data Rules and Definitions

Data governance can be defined as an organizational approach to data and information management that is formalized by a set of policies and procedures that encompass the full life cycle of data from acquisition to use to disposal. Proactive data governance is necessary to ensure confidentiality, integrity, accessibility, availability, and quality of student data from grades K-12. Our data governance program helps to ensure that information is collected, maintained, used, and disseminated in a way that protects the individuals' rights to privacy, confidentiality, and security, while producing timely and accurate statistical data.

Data Rules and Definitions (cont.)

The Alabama State Department of Education with directives form the Federal Department of Education ultimately makes the final decisions about what student data we can collect, store, and use. Compliance with Federal and State mandates is of utmost importance. The Superintendent and Technology Coordinator are privy to information that is shared with the Data Governance Committee, who then assigns rights to certain employees concerning data management. Local School personnel are assigned the roles of collecting, inputting, and maintaining accurate data by the Technology Coordinator, Superintendent, or Department Supervisors. The Superintendent will ensure that the Henry County School System abides by all laws and contractual obligations affecting its information systems including but not limited to the following:

FERPA (The Family Educational Rights and Privacy Act) protects the privacy of student education records. Generally, Henry County Schools requires written permission from the parent of eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to school officials with legitimate educational interest. Schools may share basic "directory" information, such as student names and addresses, if they give parents the opportunity to opt out. However, written permission is required to release all other student-level information if it is linked to any information that would enable a member of the school community to identify the student. If parents/students find any erroneous data, they may present corrections to local school officials, who will correct such information with appropriate documentation. **A statement will be included in our 2015-2016 student/parent handbook regarding the release of directory information and FERPA.**

The Henry County School System collects individual student data directly from students and/or families through our state-funded student data management system, InformationNow. Local student data is transmitted daily to the State's data management system from which State and Federal Reporting is completed. Each student is assigned a unique student identification number upon enrollment into the Student Management System to ensure compliance with the privacy rights of the student and his or her parent/guardians.

Henry County Schools maintains a complete up-to-date inventory of all records and data systems to target its data security and privacy management efforts allowing protection of sensitive data. The data records inventory specifies what data elements are collected, provides a justification for their collections, and explains the intended purpose(s) for their use.

Hardware and Software Inventory

Hardware Inventory

Computer equipment and other inventories are housed within the local Schools and Central Office Accounting and Technology Department.

Risk Level	Data Info Collected	Justification for Collection	Intended Purpose for Use
LOW	Student Name, State ID #, Address, Phone Number, Parent Info/Contact, Race, Sex, Language	State Reporting Requirements	Student Demographic and Identification
HIGH	Student SSN, Identification Number	State Reporting Requirements	Student Identification
HIGH	Grades	State Reporting Requirements	Track Student Progress throughout School Career
MED	Attendance	State Reporting Requirements	Track Student Attendance throughout School Career
HIGH	Discipline	State Reporting Requirements	Track Student Achievement throughout School Career
MED	Lunch Status	State Reporting Requirements	To Determine if Students qualify for Free Meals
HIGH	Special Ed / 504 / ELL	Collect Data to ensure proper placement of Students in Educational Environment.	To ensure proVision of a Free and appropriate education for students with special needs.
HIGH	Dibels, ACCESS (LEP Students), AAA (Alabama Alternate Assessment), Renaissance – STAR Reading and Math, Work Keys, PSAT, Global Scholar – Performance and Achievement, AP Exams	State Reporting Requirements	Assessments that track Student Achievement throughout School Career to determine areas of strengths and weaknesses as well as College and Career Readiness

Software Inventory

Vendor	Software	Service Description
STI	InformationNow	Management System of Grades, Student Schedules, Demographics, Special Services, Child Nutrition, Transportation, Discipline, Attendance, Parents and/or Guardians.
STI	SetsWeb	Special Education Management System to record IEPs and Eligibility
AHSAA	C2C	Alabama Athletic Eligibility System
ACT	Online Prep	Standards-based Assessment Portal Monitoring Student Progress for College and Career Readiness
ALSDE	Accountability Portal	Graduation Cohort, ELL, Dropout Prevention, AYP, Teacher Preparation, College Report, HQT/OOF, Para Professional
ACP	KUDER	Overseeing Student's 4 Year Plan, Resumes, College Plan
MCS	Franklin, Newton, WinFSFR, CNP Programs	Determines Child Nutrition Eligibility and Data Accuracy
High Ground Solutions	SchoolCast	Overseeing Phone Messaging System for Attendance, School Events, Safety Alerts
Scantron	Global Scholar	Overseeing Local Formative and Summative Assessments to Screen & Track Student Progress
Advance Education, Inc.	AdvancEd (ASSIST)	Web-based program for Continuous Improvement, Performance, and Accreditation
ASC	LeadAlabama	Overseeing formative online evaluation system for Educational Leaders
ASC	Educate Alabama	Overseeing Local Formative Evaluation Online Processes for Teachers, Educators, and Instructional Leaders serving Alabama Public Schools.
STI	STIPD	Administration of Teacher Access to Professional Development
OdysseyWare, Inc.	OdysseyWare	Credit Recovery Software
BookSystems, Inc.	Atriumm	Library Management System
DHS	Virtual Alabama	School Safety Plans and Online Administration
SchoolStatus, Inc.	School Status	Compile Student Information from InformationNow
Renaissance Learning, Inc.	AR and Star Reading and Math Programs	Student Reading and Math Initiative and Assessment
ScholarChip Card, LLC.	ScholarChip (ABE)	Behavioral Assessment and Modifcation

Data Collection

Henry County Schools ensures that only the data necessary for meeting the justified and documented set of policy, operational, and research needs are collected and maintained. All data elements are classified by their sensitivity levels. The committee evaluates the risk for disclosure of Personally Identifiable Information (PII); potential for adverse effects for the individual should the data become compromised; and legal requirements to protect the data. The Technology Coordinator helps ensure that appropriate security efforts are applied to protect the data.

Records Management

Data Records management is determined at the system level by Department Supervisors who oversee data in the areas of assessment, Special Education, Federal Programs, and Child Nutrition. Department Supervisors assign personnel to oversee the day-to-day operation of data management at each school. They also work with local school Data Managers to ensure that handling of records throughout all stages of the data lifecycle, including acquiring, maintaining, using, and archiving or destroying both regular and secure data records is done in a manner consistent with the data governance policy. All cumulative files are housed in the respective School Campus in a secure environment. Counselors also maintain assessment data for their respective schools since they also serve as the Building Test Coordinators for their schools. Counselors and secretaries at the local schools protect individual privacy by removing all direct and indirect identifiers from PII data, such as student schedules, report cards, student profiles, etc.

Data Quality

A proactive approach to data governance requires establishing data quality standards, regularly monitoring and updating data management strategies to ensure that the data is accurate, relevant, timely, and complete for the purpose in which it was designed for use. To ensure high-quality data, the following strategies are used to prevent, detect, and correct errors and misuse of data:

1. Data Entry Personnel or their designees must review student information for accuracy as it is submitted by parents, students, and teachers. This includes grades submitted into the InformationNow Student Management System.
2. Data Entry Personnel or their designees must correct data immediately when errors are brought to their attention.
3. Data Entry Personnel or their designees allow access to only those individuals with a “need to know” basis.

Data Access

Data users are expected to respect the confidentiality and privacy of individuals whose records they access; to observe any restrictions that apply to high risk data; and to abide by applicable laws, policies, procedures and guidelines with respect to access, use, or disclosure of information. The unauthorized use, storage, disclosure, or distribution of System Data in any medium is expressly forbidden. As is the access

or use of any System Data for any type of personal gain or profit, for the personal gain or profit of others, or to satisfy one's personal curiosity or that of others.

Each employee at the system will be responsible for being familiar with the System's Data Governance Policy and the security measures as they relate to his/her position and job duties. It is the express responsibility of authorized users and their respective supervisors to safeguard the data they are entrusted with, ensuring compliance with all aspects of this policy and related procedures.

Employees, whether or not they are authorized users, are expressly forbidden from installing any program or granting any access within any program to high risk data without notifying and receiving written permission from the Technology Coordinator.

Violations of these data security measures may result in the following sanctions:

- Loss of Data access privileges
- Administrative Action
- Civil and / or Criminal Liability

InformationNow Student Management System

Certain individuals have a right to access Student Data, including personally identifiable information and aggregate level data. The categories of people are outlined as follows:

Administrative Rights View all PII at System or School Level	**Grades and Low Risk Demographics**	**Census Information / Low Risk Demographics:**	**Health Information and Demographics**	**Demographics and Child Nutrition Information**
Superintendent, System Coordinators, Principals & Assistant Counselors.	*Teachers.*	*Media Specialists, Office Secretaries, Data Clerks.*	*Nurses.*	*Lunchroom Managers.*

InformationNow Parent Access

Parents are given annual access to some of their Student's educational record information (grades, schedule, attendance, and discipline) through the InformationNow Home Portal. Login information is given to the parent during Parent/Teacher Orientation at the beginning of each School Year. Parent login passwords and usernames are changed annually for protection of data and system access. Any parent not attending the Orientation, must physically come to the front office of each school and sign for the Username and Password after being verified as a Primary Contact for the Student they wish to access.

Assessment Data

The System Test Coordinator is responsible for all student assessment data. Building Test Coordinators at each school (counselors) are given rights to enter students into online portals for testing and to retrieve, disseminate, and house student assessment data in the guidance office in filing cabinets and cumulative student folders. All personnel who are given rights to online assessment results, sign test security agreements and confidentiality over the web statements when given access.

Special Education

Special Education data is housed in SETSWeb and in Special Education files at the Central Office and in each case manager's room under lock and key. After several years, pertinent data from Special Education files are stored at the Central Office in the Special Education Department. The Special Education Coordinator is in charge of how information is collected, stored, disseminated, and destroyed. A Special Education Secretary assists the Coordinator and is privy to all Special Education information. Case managers and Psychometrists have access to IEP's and all other Special Education records through SETSWeb. Administrators, Regular Teachers and Counselors are not given access to SETSWeb files to ensure confidential data is not dispersed to unauthorized users.

Cumulative Student Records

Student Cumulative files are housed at each School in a secure environment and files are sent up to the next school from feeder schools (i.e. 5th, 6th, or 8th grade files are sent to the 6th, 7th, or 8th grade schools at the end of the year). Certified staff and office personnel such as secretaries and data clerks have access to student files if they need to retrieve personal information for parents or postsecondary institutions upon written request by the student/parent (if the student is under 18).

Child Nutrition

Child Nutrition information is housed within an on-site program called Newton, as well as the Free and Reduced program called Franklin. Lunch statuses are also stored in InformationNow and in hard copies which are housed in the lunchroom manager's office. The Child Nutrition Supervisor oversees the management of Student Data for the System to process.

Exchanging Data with External Entities

Ensuring that data dissemination activities comply with federal, state, and local laws is a key organizational responsibility. The release or sharing of any data without written consent must adhere to the policies and regulations established by the Henry County Board of Education including procedures for protecting PII when sharing with other agencies and disclosure in public reports. Furthermore, the Henry County Schools

Student handbook notifies stakeholders about their rights under federal, state, and local laws, governing data privacy. Student data is shared with certain external entities contracted through the ALSDE, to manage, disaggregate, store, and assess student achievement levels. These entities include, by may not be limited to:

- ACT Assessments: ACT, Work Keys
- ACT Online Prep
- Dibels – Dynamic Indicators of Basic Early Literacy
- Metritech – ACCESS for ELL's testing program
- Global Scholar – Performance and Achievement Series
- C2C – Athletic Eligibility Program for AHSAA
- Kuder Navigator – Career Planning System
- ILIVE – ACCESS Distance Learning
- SchoolStatus – Data Compilation

Other entities which are contracted with at the District Level:

- SchoolCast – Student and Parent Notification System
- Franklin and Newton Child Nutrition Program Management
- Heartland Solutions MySchoolBucks Online Payment System

No school or department shall enter into a contract for the use of any program that requires the import or export of any District or School Data without first consulting and receiving approval from the Data Governance Committee. The Data Governance Committee will determine which of the following should be required of the service provider and assist in ensuring these requirements are met prior to any data transfer:

1) Contract
2) Designating the service provider as an "Official" as defined in FERPA
3) Memorandum of Understanding
4) Memorandum of Agreement
5) Non-Disclosure Agreement

Henry Co Schools Non-Disclosure Agreement

THIS NON-DISCLOSURE AGREEMENT by and between the Henry County Schools and _____ (the "Service Provider"), relates to the disclosure of valuable confidential information. The "District" refers to all schools, departments, and other entities, within Henry County Schools. The Service Provider renders to any free or fee-based company, organization, agency, or individual which is providing services to the District or is conducting District-approved academic research. The Disclosing Party and the Receiving Party are sometimes referred to herein, individually as a "Party" and collectively, as the "Parties".

To further the goals of this Agreement, the Parties may disclose to each other, information that the Disclosing Party considers proprietary or confidential.

The disclosure of Henry County's confidential information by a Receiving Party may result in loss or damage to the District, its Students, Parents, Employees, or other persons or operations. Accordingly, the Parties agree as follows:

- Confidential information disclosed under this Agreement by Henry County Schools shall only be transmitted in compliance with the District's approved security protocols. The Receiving Party must accept the data transmitted in these formats.
- The Service Provider will request or receive confidential information from the District solely for the purpose of entering into or fulfilling its contractual obligations or pre-approved academic research.
- The Service Provider agrees not to use, or assist anyone else to use, any portion of aspect of such confidential for any other purpose, without the District's prior consent.
- The Service Provider will carefully safeguard the District's confidential information and may be required to describe such safety measures to the District upon request.
- The Service Provider will not disclose any aspect or portion of such confidential information to any third party, without the District's prior written consent.
- Confidential Information disclosed under this agreement shall not be installed, access, or used on any computer, network, server or other electronic medium that is not the property of the District or the Service Provider, or to which third-parties have access, unless otherwise provided in a separate contract or agreement between the parties hereto.
- The Service Provider shall inform the District promptly if the Service Provider discovers that an employee, consultant, representative, or any other outside party has made, or is making or threatening to make unauthorized use of confidential information.

The Service Provider shall immediately cease all use of any confidential information and return all media and documents containing or incorporating any such confidential information within five (5) days to the District after receiving written notice to do so, or whenever the contract for services between the District and the Service Provider expires or is terminated. In addition, the Service Provider may be required by the District to destroy any confidential information contained on primary or backup media upon written request of the District.

Date:	Date:
District:	Service Provider:
Printed Name:	Printed Name:
Signature:	Signature:
Title:	Title:
Phone/Email:	Phone/Email:

Confidential Information includes:

- Any written, electronic, or tangible information provided by a disclosing Party
- Any information disclosed orally by a Disclosing Party that is treated as confidential when disclosed
- All information covered by FERPA or other local, state, or federal regulations applying to educational agencies
- Any other information not covered by FERPA, HIPPA, or other local, state, or federal regulations which the District requires the Service Provider to treat as confidential.

Physical Data Security and Risk Management

Data collected by Henry County Schools is maintained within a secure infrastructure environment located within the District and within a remote location for backup. Access to data is limited to pre-identified staff members, which are granted clearance by the Superintendent and/or Technology Coordinator related to their job responsibilities of student management, federal reporting, program assessment, and policy development.

(A) **Responsibilities**

1) The Technology Coordinator shall implement, maintain, and monitor technician access controls and protections for the data stored on the System's Network.
2) System employees shall not select or purchase software programs that will utilize or expose high risk data without first consulting the Technology Coordinator to determine whether or not adequate controls are available within the application to protect that data (the only exception to this would be any software or program purchased or utilized by the ALSDE. In this case, the ALSDE shall take all security responsibility for data it accesses or receives from Henry County Schools).
3) The Technology Coordinator and/or System Data Administrators will provide training for authorized users on how to properly access data to which they have access rights, when necessary.
4) Technical controls and monitoring cannot ensure with 100% certainty that unauthorized access will never occur. For instance, a properly authorized user leaves a workstation while logged in, and an unauthorized person views the data in their absence. Therefore, it is the shared responsibility of all employees to cooperatively support the effectiveness of the established technical controls through their actions.
5) The Data Governance Committee will determine the best physical and/or logical controls available to protect data. This shall include:
    a. Which data should be classified as High Risk
    b. Where that data resides (which software program(s) and servers)
    c. Who should have access to that data (Authorized Users)
    d. What level of control the Authorized User should have to that data (i.e. read only, read/write, print, etc.)

(B) **Location of Data and Physical Security**

1) High risk data shall be stored on servers/computers which are subject to network/workstation controls and permissions.
2) Servers storing sensitive information shall be operated by the Technology Coordinator, in compliance with all security and administration standards and policies.
3) All servers containing system data will be located in secured areas with limited access. At the school or other local building level, the principal or other location supervisor will ensure limited, appropriate access to these physically secured areas.
4) District staff who must print reports that contain high or medium risk data shall take responsibility for keeping this material in a secure location – vault, locked filing cabinet, etc. In addition, all printer material containing high risk documentation shall be shredded when no longer in use.

C) **Disposal of Hardware containing System Data**

1) Prior to disposal of any computer, the user will always notify the Technology Coordinator. A technician will remove the hard drive from the device and destroy it prior to the device being disposed or recycled.

C) **Application of Network and Computer Access Permissions**

1) The Technology Coordinator shall be responsible for implementing network protection measures that prevent unauthorized intrusions, damage, and access to all storage and transport mediums; including, but not limited to:

a. Maintaining firewall protection access to the network and/or workstations.

b. Protecting the network from unauthorized access through wireless devices or tapping of wired media, including establishing “guest” wireless networks with limited network permissions.

c. Implementing virus and malware security measures throughout the network and on all portable computers.

d. Applying all appropriate security patches.

e. Establishing and maintaining password policies and controls on access to the network, workstations, and other data depositories.

C) **Sensitive Data (Desktops, Laptops, Workstations, Mobile Devices)**

1) Firewalls and Antivirus software must be installed on all desktops, laptops, and workstations that access or store sensitive information, and a procedure must be implemented to ensure that critical operating system security patches are applied in a timely manner.

2) Storage of sensitive information on laptops, mobile devices, and devices that are not used or configured to operate as servers are prohibited, unless such information is encrypted in a Technology Department-approved encryption format.

Data Governance Training

Training in data security and student privacy laws is provided to these specific individuals by the Technology Coordinator on a regular basis in order to maintain their data use clearance along with a signed Data Security Agreement assurance of confidentiality and privacy which is kept on file in the District Office.

(A) School and Central office Administrators will receive refresher training on FERPA and other data security procedures annually at Principal Meetings.

(B) Principals and Central Office Administrators shall contact the Technology Coordinator when in doubt about how to handle Medium to High Risk information.

(C) Principals and Central office Administrators will be kept aware of emerging issues pertaining to data security.

(D) All new teachers will be trained on data security procedures as related to their professional responsibilities.

(E) All users will receive reminders throughout the year via email regarding malware threats and phishing scams and how to report suspected threats.

Henry County Schools Data Security Agreement

Electronic data is very portable and can be vulnerable to theft and unintended disclosure. Therefore, having access to personal and private information as part of one's job duties also carries with it important responsibilities to protect the security and privacy of that data.

As an employee who has access to Henry County Schools student/employee data, I understand that I have the responsibility to handle, maintain, and disseminate information contained in these records in a secure manner. I understand that my access to and dissemination of student/employee data is subject to local policies, as well as state and federal laws and statutes. This includes, but is not limited to, the Federal Educational Rights.

I understand that transferring personal information to a third party outside of the school system in any electronic format may only be done after approval by an appropriate System Coordinator and/or the Technology Coordinator. Except when explicitly instructed to do so by school or District Administrators, I understand that copies of student/employee data should never be kept on a temporary storage device such as a USB drive or CD, and that student/employee data should not be removed from the school premises on a laptop.

I affirm that I will keep my computer workstation secure by locking or logging off when the machine is unattended. I will not allow any Student to use any Teacher computer, iPad, or other device that I use to access Student Data. I will not share network or program passwords with others. I will not allow personal data that has been printed into the view or hands of unintended parties. I will not use my software rights to grant others permission to data to which they are not entitled. Violations of data security measures may result in the following sanctions:

- Loss of data access privileges
- Administrative action
- And/or possible Civil and/or Criminal Liability.

By signing below, I am affirming that I understand and agree to the above requirements.

_____

Printed Name

_____ _____

Signature Date