Houston County Schools

Data Governance Policy

2014-2015

Committee Members

Mr. Johnny Dixon –Chairperson - Middle School Principal
Mr. Tim Pitchford – Superintendent
Mr. Cas Haddock- Student Testing Coordinator
Mr. David Sewell -Data Entry & Accountability Coordinator
Dr. Misty Freeman -Elementary Principal
Mrs. Shirley McGee – Parent, K-12 School
Mr. Bob Blalock –Technology Director
Dr. Rhonda Lassiter– Human Resources / Personnel Director
Mr. Roger Sanders – Counselor, K-12 School
Mrs. Jami Whillock -High School Instructional Coach
Mrs. Angie Linder –Middle School Instructional Coach

Board approved: _____

Decision Making Authority

The Houston County School System provides different levels of data governance working together to ensure a system of checks and balances within the district. This hierarchy begins with the Data Governance Committee which oversees the program with the direction from the Alabama State Department of Education, revising and updating policies as needed. This committee meets at least yearly and is comprised of the superintendent, data manager, counselors, technology coordinator, principals, and our school board attorney. The technology coordinator interprets the policies for the district and helps to ensure state and federal guidelines are being followed. Data stewards (program managers) are responsible for implementing data governance policies and standards and maintaining data quality and security. Permission levels are assigned by the data stewards to ensure that access of information is limited to the scope of each person's job duties. Data stewards have the authority to quickly and efficiently correct data problems while still ensuring that their access to personally identifiable information (PII) is minimized in order to protect privacy and confidentiality. Houston County data stewards include system level coordinators, school nurses, and the high school athletic director (principal). Personnel at the local schools who assist data stewards with data entry and maintenance may include principals, assistant principals, counselors, secretaries, lunchroom managers, and data entry clerks.

General Roles and Responsibilities

The following chart indicates the data stewards (managers) who are assigned to each domain of activity and their general roles and responsibilities as it relates to accountability, management, and security. Data stewards are responsible for actively monitoring data-related activities for compliance with the established standards and policies and procedures.

- **DOMAINS-All are highly sensitive**

Activity domain	Data Steward Assigned	Roles & Responsibilities
INOW-student management system of grades, schedules, demographics, special services, child nutrition, transportation,	David Sewell Accountability Coordinator & Data Manager	Oversee INOW, serve as liaison between SDE & schools regarding reporting requirements, provide training for INOW issues, ensures data security by

discipline, attendance, etc. contact, guardians		providing clearance for personnel to access confidential data.
SETSWEB	Shannon Burgess, Sp Ed Secretary, Denise Whitfield, Sp Ed Coordinator	Manage Sp. Ed records
ILIVE-Distance Learning	High School Counselors'	Distance learning scheduler
C2C Alabama Athletic Eligibility System	High School Athletic Directors/Principals	Determine athletic eligibility of athletes
All State Mandated Student Assessment Portals	Cas Haddock, System Testing Coordinator, Counselors, David Sewell, Data Entry & Accountability Coordinator	Oversees the administration of statewide assessments; ensures test rosters are built for each test through online portals & that test scores are released to building test coordinators or principals who file scores in students' cumulative files & disseminate data to parents, students, and teachers as deemed appropriate
Edirect	David Sewell, Accountability Coordinator & Data Manager	Assigns permissions to users to access state assessment reports
Accountability Web Portal	David Sewell, Accountability Coordinator & Data Manager, Cas Haddock, System Testing Coordinator	Maintains permissions to access state accountability reports, Cohorts, etc.
Dibels	Cas Haddock, System Testing Coordinator, Anthony Stewart, Elementary Coordinator, Principals, & Counselors, Instructional & Reading Coaches'	Oversees K-2 early literacy reading skills
Renaissance Star Reading/ Math Program, ClassWorks, STI Achievement &	David Sewell- Data Manager& Accountability Coordinator, Cas Haddock- System Test Coordinator,	Oversees formative assessment program for grades K-8

Assessment	Matt Swann, Secondary Coordinator, & Elementary Coordinator, Media Specialists, Teachers	
Alabama Career Planning System-Kuder	Counselors & Principals	Oversee students' 4 year plans, resumes, college plans
ProLunch	Marie Payne, Beth Pittman System CNP Coordinator's	Determines child nutrition eligibility
Student Cumulative Files	David Sewell, Accountability Coordinator & Data Entry Manager, Counselors, Principals'	House student educational records
Discipline Records and Attendance Records	David Sewell, Accountability Coordinator & Data Entry Assistant Principals, Counselors, Cas Haddock	House student discipline/attendance records
Schoolcast	David Sewell, Accountability Coordinator & Data Entry Manager, Marie Payne, CNP Coordinator, Bob Blalock, Technology Director, Assistant Principals' and Counselors	Sends out phone messages of important school events or notices.
Scantron-Global Scholars and Performance Series, STI Achievement, ClasWorks,	David Sewell, Accountability Coordinator & Data Entry Manager, Matt Swann, Secondary Coordinator, Cas Haddock, Testing Coordinator, Denise Whitfield, Sp Ed Coordinator, Rhonda Lassiter, Human Resource Director & Gifted Coordinator, Counselors, & Instructional Coaches, & Principals	Local formative and summative assessments to screen students, track student progress, and identify strengths and deficiencies.
AdvancED Adaptive System of School Improvement Support Tools (ASSIST™).	Mr. Tim Pitchford, Superintendent, Mr, Anthony Stewart, Elem. Supervisor, Mr. Matt Swann, High School Supervisor, Mr. David Sewell, Data Entry & Accountability Coordinator, Mrs. Beth Pittman, Federal Programs	Oversees the Adaptive System of School Improvement Support Tools (ASSIST™) which is a state-of-the-art, web-based platform designed to broaden and sharpen thinking about continuous improvement,

	Coordinator, Mrs. Denise Whitfield, Sp Ed Coordinator, Dr. Rhonda Lassiter, Human Resources/Personnel Director, Mr. Bob Blalock, System Technology Coordinator, Mr. Cas Haddock, System Testing Coordinator, Principals, Parents, Counselors, Instructional Coaches, Media Specialist,	performance and accreditation.
Lead Alabama/Val Ed	Principals, Mrs. Beth Pittman, Lead Al Coordinator, David Sewell, Data Entry & Accountability Coordinator, Mr. Tim Pitchford, Superintendent, Mr. Bob Blalock, System Technology Coordinator, Mr. Cas Haddock, System Testing Coordinator	Oversees the formative, online, evaluation system for educational leaders consisting of a self-assessment, collaborative dialogue, professional learning plan (PLP), evidence collection and a 360° assessment, the Vanderbilt Assessment of Leadership in Education (VAL-ED). LEADAlabama is used to evaluate certificated central office administrators, principals, assistant principals, and all other specialty area administrators.
Educate Alabama	Principals, Mrs. Beth Pittman, Educate Al Coordinator, Mr. David Sewell, Data Entry & Accountability Coordinator, Teachers, Counselors, Media Specialist, Mr. Bob Blalock, System Technology Director, Mr. Cas Haddock, System Testing Coordinator	Oversees the local formative evaluation online processes for teachers/educators and instructional leaders serving Alabama's public schools.
Atriuum-Library Management System	Media Specialist, David Sewell, Accountability Coordinator & Data Entry Manager, Mr. Bob Blalock,	Oversees the library data management system

	System Technology Director, Reading & Instructional Coaches	

Standard Policies and Procedures

With consideration given to and input accepted from all data stakeholders, along with the support from the local superintendent and board of education, the data governance committee has composed policies and standards to include the following components:

Mission and Vision

The Mission of the Houston County Board of Education's Data Use and Governance Policy is to maintain compliance with the *Family Educational Rights and Privacy Act* (FERPA). This policy is based on the knowledge that the appropriate use of data is essential to accelerating student learning, program and financial effectiveness and efficiency, and policy development. Our Vision is to create and maintain a comprehensive, accurate, secure, and efficient system of data governance whereby all K-12 student data remains confidential throughout the life span of the data and is only accessed and shared upon necessity or when written consent from students and/or parents is obtained.

Goals, Governance, Success Measures, Funding Strategies

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 consciously reviewing our student data management system.
2. Improved data usability, resulting from monitoring data content for consistency with the organizational vision and stakeholders' needs;
3. Improved data timeliness, 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 protection to the data based on the level of sensitivity.

Funding for the data governance program will be secured by the school superintendent by 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 as 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.

Decision Rights and Compliance Mechanisms

The Alabama State Department of Education with directives from 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 upmost importance. The Superintendent and technology coordinator are privy to information that is shared with the Data Governance Committee, who assigns rights to certain employees concerning data management. Local school personnel are then assigned by the technology, coordinator, superintendent, or system coordinators to the roles of collecting, inputting, and maintaining accurate data. The superintendent will ensure that the Houston 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, Houston County Schools requires written permission from the parent or 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 is included in our student/parent handbook regarding the release of directory information and FERPA.**

CIPA, the Children's Internet Protection Act, was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program. Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies must include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyber bullying awareness and response.

COPPA, the Children's Online Privacy Protection Act, regulates operators of commercial websites or online services directed to children under age 13 that collect or store information about children. Parental permission is required to gather certain information; see www.coppa.org for details.

HIPAA, the Health Insurance Portability and Accountability Act, applies to organizations that transmit or store Protected Health Information (PII). It is a broad standard that was originally intended to combat waste, fraud, and abuse in health care delivery and health insurance, but is now used to measure and improve the security of health information as well.

Routine Monitoring

The ALSDE monitors our Data Governance Policy during routine system wide comprehensive monitoring visits.

Dissemination of Data Governance Policy

A General overview of the Houston County Board of Education Data Governance Policy is available to the public and all internal stakeholders via the District Website. As exposing these specific security measures to outside, unknown parties could result in greater risk to the District's data, this document will not be made publicly available. Requests for detailed information about the District's data security procedures shall be brought to the committee or the Superintendent who will determine the legitimacy of the request and respond accordingly.

Data Inventories

The Houston County School System collects individual student data directly from students and/or families through our state funded student data management system, INOW. 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 identifier upon enrollment into the student management system to ensure compliance with the privacy rights of the student and his or her parents/guardians.

Maintaining a complete up-to-date inventory of all records and data systems, including those used to store and process data, enables Houston County Schools to target its data security and privacy management efforts to appropriately protect sensitive data. The data records inventory specifies what data elements are collected, provides a justification for their collection, and explains the intended purpose(s) for their use. Houston County Schools reviews its inventory yearly.

STUDENT DATA FILES: High Risk (HR) Medium Risk (MR) Low Risk (LR)

Data elements collected	Justification for collection	Intended purpose(s) for use
LR: Basic Demographic Information: Student name, State ID #,address, phone, parent info/contact, race, sex, home language, etc.	State reporting requirements	Student Identification
Student info: HR: Social security number and/or Identifying Number	State reporting requirements	Student Identification
HR: Grades	State reporting requirements	Track students achievement levels throughout their school career
MR: Attendance	State reporting requirements	Track students attendance throughout their school career
HR: Discipline	State reporting requirements	Track students discipline throughout their school career
MR: Free/Reduced Lunch information	State reporting requirements	To determine if students qualify for free/reduced meals
HR: Special Ed/504/ELL data	Data is collected to ensure proper placement of students	To ensure provision of a free and appropriate education for

	in the educational environment	students with special needs
HR: Assessment data from the following assessments: • Dibels • Aspire • ASA • ACCESS (LEP students) • AAA (Alabama Alternate Assessment) • Quality Core End of Course Assessments • Explore (grade 8) • Renaissance- Star Reading and Math (grades K-8) • Plan (grade 10) • ACT (grade 11) • Work Keys (grade 12) • PSAT (grade 11) • Global Scholars- Performance and Achievement Series • Sti Achievement & Assessment • Clasworks • AP exams	State reporting requirements	Track students achievement levels throughout their school career to determine areas of strengths and weaknesses and college and career readiness

COMPUTER EQUIPMENT INVENTORY:

Computer equipment inventories are housed within the local schools and central office staff.

SOFTWARE INVENTORY

INOW-student management system of grades, schedules, demographics, special services, child nutrition, transportation, discipline, attendance, contacts, guardians
SETSWEB-special education portal to record IEP processes and eligibility
C2C Alabama Athletic Eligibility System
ACT Assessment Portals—Aspire & Quality Core

ACT online Prep
Edirect
Accountability Web Portal
Dibels-Early learning literacy program - The DIBELS assessment is used to assess students' mastery of early reading skills
Rennaissance- Star Reading/ Math Program- Local standardized, computer-adaptive progress monitoring tools, identifying students' strengths and weaknesses.
Pro Lunch program
Kuder Navigator-Alabama's College and Career Planning System-
ILIVE-Access Distance Learning Portal for student registration
STI Achievement & Assessment – Local formative and summative assessments to screen students, track student progress, and identify students' strengths and deficiencies.
Artiuum-Library Management System - Web-based Library Automation
Global Scholars -Local formative and summative assessments to screen students, track student progress, and identify strengths and deficiencies.

*********Data inventories shall be updated yearly by the data governance committee.

Data Content Management

Houston County Schools ensures that only those 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 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.

Data Records Management

Records management is determined at the system level. System level coordinators oversee data in the areas of assessment, special education, federal programs, and child nutrition. System level coordinators 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 guidance offices. Counselors also maintain assessment data for their respective schools since they also serve as the building test coordinators for their school. Counselors and secretaries at the local schools work diligently to protect individual privacy by removing all direct and indirect identifiers from PII data, such as from student schedules, report cards, student profiles, etc.

Data Quality

A proactive approach to data governance requires establishing data quality standards and regularly monitoring and updating the data management strategies to ensure that the data are accurate, relevant, timely, and complete for the purposes they are intended to be used. To ensure high quality data, the following strategies are used to prevent, detect, and correct errors and misuses of data.

1. Data stewards or their designees review student information for accuracy as it is submitted by parents, students, and teachers. This includes grades submitted into the INOW portal.
2. Data stewards or their designees correct data immediately when errors are brought to their attention.
3. Data stewards or their designees allow access to only those individuals with a “need to know” status as determined by data stewards.

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 one's own 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 these security measures as they relate to his or 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 prohibited from installing any program or granting any access within any program to high risk without notifying the Technology Coordinator.

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

- loss of data access privileges,
- administrative actions,
- and/or personal civil and/or criminal liability.

INOW -Student Management System

Certain individuals have a right to access student data, including both personally identifiable information and aggregate level data. These 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 & Demographics**	**Demographics and Lunch Information**
System Level Superintendent System Coordinators Principals Counselors **School Level** Assistant Principals RTI coordinator Secretaries	Teachers	Librarians Data Clerks	Nurses	Lunchroom Manager

Parent Access

Parents are given access to some of their child's current educational records (grades, schedule, attendance, discipline) through the INOW home portal. Log in information is given to the parent when they present in person to sign for a user name and password. Passwords are changed upon initial log in to the portal.

Assessment Data

The system test coordinator is the data steward of 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 board office and in each case manager's room under lock and key. After a certain number of years, pertinent data from special education files are sent to the school building level to be filed in respective cumulative files. The System 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 at the school level have access to IEP's and all other special education records through SETSWEB. Counselors are given access to SETSWEB on a view-only basis. Teachers have access to IEPs and must sign to verify that they have received them and will keep them confidential.

Cumulative Student Records

Student cumulative files are housed in the guidance office. Files are sent up to the next school from feeder schools (i.e., 5th grade files are sent to middle school at the end of the year and 8th grade files are sent to high school). 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 child is under 18).

Child Nutrition Information

Child nutrition information is housed within an onsite program called Pro Lunch Free/reduced lunch status is also stored in INOW and in hard copies which are housed in the lunchroom manager's office. A child nutrition coordinator oversees the management of student data for the system.

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 Houston County including procedures for protecting PII when sharing with other agencies and disclosure avoidance procedures for protecting PII from disclosure in public reports. Furthermore, The Houston 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, but may not be limited to:

- ACT Assessments: Aspire, Explore, Plan, ACT, Quality Core, WorkKeys;
- ACT online Prep
- Dibels-Dynamic Indicators of Basic Early Literacy
- Metritech-ACCESS for ELL's testing program
- Global Scholars –Performance and Achievement Series
- C2C-Athletic Eligibility Program
- Kuder Navigator-Career Planning System
- ILIVE-Access Distance Learning
- STI Achievement & Assessment Services
- Clasworks

Other entities which are contracted with at the district level:

- Renaissance Learning is a web-based testing agency that we contract with locally for progress monitoring for RTI for grades K-8. We have an agreement with them to follow all state and federal laws regarding the maintenance of student privacy.
- One Call-Student Messenger Program
- Pro Lunch-Child Nutrition Information System

No school or department should enter into a contract for the use of any program that requires the import of District 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

Sample Non-Disclosure Agreement

THIS NONDISCLOSURE AGREEMENT by and between Houston 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 Houston County Schools. The Service Provider refers 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 Houston 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 Houston 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 or aspect of such confidential Information for any other purpose, without the District’s prior written 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, accessed 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 other party, or any 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 regulation applying to educational agencies
- any other information not covered by FERPA, HIPAA, or other local, state, or federal regulation which the District requires the Service Provider to treat as confidential

Physical Data Security and Risk Management

Data collected by the Houston 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 technical 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 exception to this would be any software program purchased or utilized by the ALSDE. In this case, the ALSDE shall take all security responsibility for data it accesses or receives from Geneva City 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 rights, when necessary.

4) Technical controls and monitoring cannot ensure with 100% certainty that no unauthorized access occurs. For instance, a properly authorized user leaves their 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 file cabinet, etc. In addition, all printed 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 notify the Technology Coordinator. A technician will remove the hard drive from the device and destroy it prior to the device being disposed of or auctioned off.

(D) **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.

(E) **Sensitive Data as it pertains to Desktops/Laptops/Workstations/Mobile Devices**

1) Firewalls and anti-virus 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 is 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 principals' 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.

Houston 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 Houston 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 polices, as well as state and federal laws and statutes. This includes, but is not limited to the Federal Educational Rights and Privacy Act (FERPA) and HIPAA.

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 will keep my computer workstation secure by locking or logging off when the machine is unattended. 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 actions
- and/or personal civil and/or criminal liability

Please sign below to indicate you understand and agree to the above statements.

Printed Name	Signature	Date