HOOVER
CITY SCHOOLS

Data Governance Procedures

I. **POLICY**

These procedures are authorized by the following Hoover City Schools policy:

> The Superintendent is authorized to establish procedures governing the storage, use, and sharing of data maintained electronically by the school system. Such procedures shall comply with applicable state and federal law and shall include provisions for data security (including physical security measures), access controls, quality control, and data exchange and reporting (including external data requests, and third party data use). Nothing in this policy or in any procedures authorized hereunder creates or expands any entitlement to confidentiality of records beyond that which is established by law or specific Board policy.
>
> Any unauthorized access, use, transfer, or distribution of Board data by any employee, student, or any other individual may result in disciplinary action (up to and including termination for employees) and other legal action.

II. **SCOPE**

These procedures apply to all data that is stored electronically by the Hoover City school system. These procedures are intended to protect information that is deemed confidential by law from unauthorized modification, destruction, or disclosure throughout its life cycle and to protect the integrity of the school system's equipment and software, including providing an appropriate level of security over the equipment and software used to process, store and transmit such information.

The procedures outlined herein apply to all and employees of the district, contractual third parties and agents of the district who have access to data stored electronically by the school system. This includes all forms of records either stored electronically or derived from electronic records that are deemed confidential by law, including but not limited to:

- Speech, spoken face to face, or communicated by phone or radio,
- Hard copy data printed or written on paper,
- Communications sent by post/courier, fax, electronic mail, text, chat and or any form of social media, etc.,
- Data stored and processed by servers, PCs, laptops, tablets, mobile devices, etc.,
- Data Stored on any type of removable media or cloud based services

The intent of these procedures is to implement the laws governing the confidentiality of the school system's records. Nothing in these procedures is intended to create or expand any entitlement to confidentiality of records beyond that which is established by law. Furthermore, nothing herein should be deemed to create or expand any entitlement to copies of such records beyond what is established by law. In general, Hoover City Schools reserves the right to adopt, revise, interpret, amend, repeal, suspend, or apply its policies and procedures according to its assessment of the needs and interests of the school system; subject only to such limitations on the exercise of such prerogatives as may be imposed by law.

The data governance policies and procedures will be reviewed annually by the data governance committee.

III. REGULATORY COMPLIANCE

Hoover City Schools will abide by any law, statutory, regulatory, or contractual obligations affecting its information systems. The District's data governance policy and procedures are informed by the following laws, rules, and standards, among others:

FERPA
The Family Educational Rights and Privacy Act, applies to all institutions that are recipients of federal aid administered by the Secretary of Education. This regulation protects student information and accords students specific rights with respect to their data.
http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

ALABAMA RECORDS DISPOSITION AUTHORITY
Alabama Law Section 41-13-23 authorized the Alabama Department of Archives and History to publish rules for Local Government Records Destruction. For more information:
http://www.archives.alabama.gov/officials/localrda.html.

COPPA
The Children's Online Privacy Protection Act, regulates organizations that collect or store information about children under age 13. Parental permission is required to gather certain information; see www.coppa.org for details.

Payment Card Industry Data Security Standard (PCI DSS)
This standard was created by a consortium of payment brands including American Express, Discover, MasterCard, and Visa. It covers the management of payment card data and is relevant for any organization that accepts credit card payments. See www.PCI security standards.org for more information.

ISO Standards (http://www.iso.org/iso/home/standards.html)

- ISO 17799:2000 – Information technology – Code of practice for information security management

- ISO 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements
- ISO 27002L2013 - Information technology – Security techniques – Code of practice for information security control

IV. RISK MANAGEMENT

A. A thorough analysis of all Hoover City Schools information networks and systems will be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information. The analysis will examine the types of threats – internal or external, natural or man-made, electronic and non-electronic – that affect the ability to manage the school system's information resources. The analysis will also document the existing vulnerabilities within each component of the information network and systems that could potentially expose school system data to threats.

From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined. The frequency of the risk analysis will be determined at the discretion of the person responsible for the component of the information network and systems in question.

B. The Superintendent or designee will administer periodic risk assessments to identify, quantify, and prioritize risks. Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities.

***Appendix A (Information Security Definitions)**

***Appendix B (Information Security Responsibilities)**

V. DATA CLASSIFICATION

Classification is used to promote proper controls for safeguarding the confidentiality of information. Regardless of classification the integrity and accuracy of all classifications of information must be protected. The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, report) must have the same classification regardless of format.

***Appendix C (Data Classification Levels)**

VI. SYSTEMS AND INFORMATION CONTROL

All computers, laptop, mobile devices, printing and/or scanning devices, network appliances/equipment, AV equipment, servers, internal or external storage, communication devices or any other current or future electronic or technological devices may be referred to as "systems" for purposes of these procedures.

All involved systems and information are assets of Hoover City Schools and are expected to be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

***Appendix D (Acquisition Of Hardware)**

A. **Ownership of Software:** All computer software developed by Hoover City Schools employees or contract personnel on behalf of Hoover City Schools or licensed for Hoover City Schools use is the property of Hoover City Schools and must not be copied for use at home or any other location, unless otherwise specified by the license agreement.

B. **Installed Software:** All software packages that reside on computers and networks within Hoover City Schools must comply with applicable licensing agreements and restrictions and must comply with Hoover City Schools acquisition of software policies.

***Appendix E (Acquisition of Software)**

C. **Virus Protection, Malware, Spyware, and Spam Protection:** Virus checking systems approved by the Information Security Officer and Information Services must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorized to turn off or disable any security checking systems.

D. **Access Controls:** Physical and electronic access to information systems that contain PII, Confidential and Internal information and computing resources is controlled. To ensure appropriate levels of access by internal workers, a variety of security measures will be instituted as recommended by the data governance committee and approved by Hoover City Schools. In particular, the data governance committee shall document roles and rights to the student information system and other like systems. Mechanisms to control access to PII, Confidential and Internal information include (but are not limited to) the following methods:

1. **Authorization:** Access will be granted on a “need to know” basis and must be authorized by the immediate supervisor and application owner with the assistance of the ISO. Any of the following methods are acceptable for providing access under this policy:

a. *Context-based access:* Access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The “external” factors might include time of day, location of the user, strength of user authentication, etc.

b. *Role-based access:* An alternative to traditional access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization's structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.

c. *User-based access:* A security mechanism used to grant users of a system access based upon the identity of the user.

2. **Identification/Authentication:** Unique user identification (user id) and authentication is required for all systems that maintain or access PII, Confidential and/or Internal Information. Users will be held accountable for all actions performed on the system with their user id.

a. At least one of the following authentication methods must be implemented:

1. strictly controlled passwords

2. biometric identification, and/or

3. tokens in conjunction with a PIN.

b. The user must secure his/her authentication control (e.g. password, token) such that it is known only to that user and possibly a designated security manager.

c. The user must log off or secure the system when leaving it.

3. **Data Integrity:** Hoover City Schools must be able to provide corroboration that PII, Confidential, and Internal Information has not been altered or destroyed in an unauthorized manner. Listed below are some methods that support data integrity:

- transaction audit
- disk redundancy (RAID)
- ECC (Error Correcting Memory)
- checksums (file integrity)
- encryption of data in storage
- digital signatures
- data wipes

4. **Transmission Security:** Technical security mechanisms must be put in place to guard against unauthorized access to data that is transmitted over a communications network, including wireless networks. The following features must be implemented:

a. integrity controls and

b. encryption, where deemed appropriate

5. **Remote Access:** Access into Hoover City Schools network from outside will be granted using Hoover City Schools approved devices and pathways on an

individual user and application basis. All other network access options are strictly prohibited. Further, PII, Confidential and/or Internal Information that is stored or accessed remotely must maintain the same level of protections as information stored and accessed within the Hoover City Schools network.

6. **Physical Access:** Access to areas in which information processing is carried out should be restricted to only appropriately authorized individuals.

The following physical controls must be in place:

a. Computer systems should be installed in an access-controlled area. The area in and around the computer facility must afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations.

b. File servers containing PII, Confidential and/or Internal Information must be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.

c. Workstations or personal computers (PC) must be secured against use by unauthorized individuals. Local procedures and standards must be developed on secure and appropriate workstation use and physical safeguards.

d. Facility access controls must be implemented to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed. Local policies and procedures must be developed to address the following facility access control requirements:

1. Contingency Operations – Documented procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
2. Facility Security Plan – Documented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
3. Access Control and Validation – Documented procedures to control and validate a person’s access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
4. Maintenance records – Documented policies and procedures to document repairs and modifications to the physical components of the facility which are related to security (for example, hardware, walls, doors, and locks).

***Appendix F (Security Procedures)**

***Appendix G (Password Control Standards)**

***Appendix H (Purchasing and Disposal Procedures)**

***Appendix I (Data Access Roles)**

E. **Data Transfer/Exchange/Printing:**

1. **Electronic Mass Data Transfers:** Downloading, uploading or transferring PII, Confidential, and Internal Information via a mass data transfer between systems must be strictly controlled.

    A. **Internal Requests:** Any internal request from within the school system for a mass download of data that includes PII for research or any other purposes must be in accordance with this policy and be approved by the data governance committee.

    B. **External Requests:** Any external request from outside the school system for a mass download of the school system's electronic records must be approved by the Application Owner and include only the minimum amount of information necessary to fulfill the request. A memorandum of Agreements (MOA) or contract must be in place when transferring PII to external entities such as software or application vendors, textbook companies, testing companies, or any other web based application, etc. unless an exception is approved by the data governance committee. The contents of the MOA or contract will vary depending on the reason for the transfer and how the data will be used.

    The school system may also release de-identified records and information for purposes such as research, provided that all personally identifiable information is removed and a reasonable determination is made that a student's identity is not personally identifiable, whether through single or multiple releases, and taking into account other reasonably available information. Such releases should be approved by approved by the data governance committee.

***Appendix J (Sample MOA)**

2. **Other Electronic Data Transfers and Printing:** PII, Confidential and Internal Information must be stored in a manner inaccessible to unauthorized individuals. PII and Confidential information must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise.

F. **Oral Communications:** Hoover City Schools staff should be aware of their surroundings when discussing PII and Confidential Information that is protected from disclosure by law. This includes the use of cellular telephones in public areas. Hoover City Schools staff should not discuss PII or Confidential

Information in public areas if the information can be overheard. Caution should be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.

G. **Audit Controls:** Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use PII must be implemented. Further, procedures must be implemented to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

H. **Evaluation:** Hoover City Schools requires that periodic technical and non-technical evaluations be performed in response to environmental or operational changes affecting the security of electronic PII to ensure its continued protection.

I. **IT Disaster Recovery**: Controls must ensure that Hoover City Schools can recover from any damage to critical systems, data, or information within a reasonable period of time. Each school, department, or individual is required to report a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages data or systems immediately to the Superintendent, Risk Management Officer, Technology Director and/or ISO for response to. The IT Disaster Plan includes the following:

1. A prioritized list of critical services, data, and contacts.
2. A process enabling Hoover City Schools to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.
3. A process enabling Hoover City Schools to continue to operate in the event of fire, vandalism, natural disaster, or system failure.
4. Procedures for periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary.

VII. Compliance

A. The Data Governance and Use Procedures apply to all users of Hoover City Schools information including: employees, staff, volunteers and outside affiliates. Failure to comply with Information Security Policies and Standards by employees, staff, volunteers and outside affiliates may result in disciplinary action up to and including dismissal in accordance with applicable Hoover City Schools procedures, or, in the case of outside affiliates, termination of the affiliation.

Hoover City Schools will conduct training on its data governance policy for employees, staff, volunteers and outside affiliates that have responsibilities that include creating, using, or maintaining data as necessary and will maintain documentation of such training.

B. Possible disciplinary/corrective action may be instituted for violations of Hoover City Schools data governance policy and procedures, including, but is not limited to, the following:

1. Unauthorized disclosure of PII or Confidential Information as specified in Confidentiality Statement.
2. Unauthorized disclosure of a log in code (user id) or password.
3. Attempting to obtain a log in code or password that belongs to another person.
4. Using or attempting to use another person's sign-on code or password.
5. Unauthorized use of an authorized password to examine records or information for which there for which the user has no legitimate interest.
6. Installing or using unlicensed software on Hoover City Schools computers.
7. The intentional unauthorized destruction of Hoover City Schools information.
8. Attempting to get access to sign-on codes for purposes other than official business, including completing fraudulent documentation to gain access.

Appendix A

INFORMATION SECURITY DEFINITIONS

Availability: Data or information is accessible and usable upon demand by an authorized person.

Confidentiality: Data or information is not made available or disclosed to unauthorized persons or processes.

Integrity: Data or information has not been altered or destroyed in an unauthorized manner.

Involved Persons: Every worker at Hoover City Schools -- no matter what their status. This includes, , students, employees, contractors, consultants, temporaries, volunteers, interns, etc.

Involved Systems: All computer equipment and network systems that are operated within the Hoover City Schools environment. This includes all platforms (operating systems), all computer sizes (personal digital assistants, desktops, mainframes, etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.

Personally Identifiable Information (PII): PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.

Appendix B

INFORMATION SECURITY RESPONSIBILITIES

A. **Information Security Officer: (CTO)**The Information Security Officer (ISO) for each district is responsible for working with user management, owners, custodians, and users to develop and implement prudent security policies, procedures, and controls, subject to the approval of Hoover City Schools. Specific responsibilities include:

- Ensuring security policies, procedures, and standards are in place and adhered to by entity.
- Providing basic security support for all systems and users.
- Advising owners in the identification and classification of computer resources. See Section VI Information Classification.
- Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation.
- Educating custodian and user management with comprehensive information about security controls affecting system users and application systems.
- Providing on-going employee security education.
- Performing security audits.
- Reporting regularly to the Hoover City Schools Data Governance Committee on entity's status with regard to information security.

B. **Information Owner:(Database Administrator)** The owner of a collection of information is usually the manager responsible for the creation of that information or the primary user of that information. This role often corresponds with the management of an organizational unit. In this context, ownership does not signify proprietary interest, and ownership may be shared. The owner may delegate ownership responsibilities to another individual by completing the Hoover City Schools Information Owner Delegation Form. The owner of information has the responsibility for:

- Knowing the information for which she/he is responsible.
- Determining a data retention period for the information, relying on advice from the Legal Department.
- Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created within the unit.
- Authorizing access and assigning custodianship.
- Specifying controls and communicating the control requirements to the custodian and users of the information.
- Reporting promptly to the ISO the loss or misuse of Hoover City Schools information.
- Initiating corrective actions when problems are identified.

- Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
- Following existing approval processes within the respective organizational unit for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

C. **Custodian:(Network Administrator)** The custodian of information is generally responsible for the processing and storage of the information. The custodian is responsible for the administration of controls as specified by the owner. Responsibilities may include:

- Providing and/or recommending physical safeguards.
- Providing and/or recommending procedural safeguards.
- Administering access to information. Releasing information as authorized by the Information Owner and/or the Information Privacy/ Security Officer for use and disclosure using procedures that protect the privacy of the information.
- Evaluating the cost effectiveness of controls.
- Maintaining information security policies, procedures and standards as appropriate and in consultation with the ISO.
- Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
- Reporting promptly to the ISO the loss or misuse of Hoover City Schools information.
- Identifying and responding to security incidents and initiating appropriate actions when problems are identified.

D. User Management:(Network Administrator) Hoover City Schools management who supervise users as defined below. User management is responsible for overseeing their employees' use of information, including:

- Reviewing and approving all requests for their employee's access.
- Initiating security change requests to keep employees' security record current with their positions and job functions.
- Promptly informing appropriate parties of employee terminations and transfers, in accordance with local entity termination procedures.
- Revoking physical access to terminated employees, i.e., confiscating keys, changing combination locks, etc.
- Providing employees with the opportunity for training needed to properly use the computer systems.
- Reporting promptly to the ISO the loss or misuse of Hoover City Schools information.
- Initiating corrective actions when problems are identified.
- Following existing approval processes within their respective organization for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

E. User: The user is any person that has access to electronically stored records. A user of information is expected to:

- Access information only in support of their authorized job responsibilities.
- Comply with Information Security Policies and Standards and with all controls established by the owner and custodian.

- Keep personal authentication devices (e.g. passwords, SecureCards, PINs, etc.) confidential.
- Report promptly to the ISO the loss or misuse of Hoover City Schools information.
- Initiate corrective actions when problems are identified.

Appendix C

Data Classification Levels

Personally Identifiable Information (PII)

PII is any information about an individual maintained by an agency:

a. that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and

b. any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Any disclosure of these records must be in accordance with applicable law.

Confidential Information

Confidential Information is very important and highly sensitive material that is not classified as PII, but that must be protected from disclosure in order to maintain the security of the school system's electronic records. This information must be restricted to those with a legitimate business need for access.

Examples of Confidential Information may include: key financial information, proprietary information of commercial research sponsors, system access passwords and information file encryption keys.

Decisions about the provision of access to this information must always be cleared through the Chief Technology Officer or his designee.

Internal Information

Internal Information is intended for unrestricted use within Hoover City Schools, and in some cases within affiliated organizations such as Hoover City Schools business partners. This type of information is already widely-distributed within Hoover City Schools, or it could be so distributed within the organization without advance permission from the information owner.

Examples of Internal Information may include: personnel directories and internal policies and procedures, and system wide communications such as newsletters and announcements.

Any information not classified as PII, Confidential or Public will, by default, be classified as Internal Information. Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.

Public Information

Public Information has been specifically approved for public release by a designated authority within each entity of Hoover City Schools. Examples of Public Information may include marketing brochures and material posted to any Hoover City Schools-related internet presence.

This information may be disclosed outside of Hoover City Schools.

Appendix D

Acquisition of Hardware

It is the position of Hoover City Schools' IT department to ensure technology equipment being purchased is compatible with existing district equipment and is purchased/ deployed in an acceptable timeframe. The equipment must be purchased from a reputable manufacturer, have a warrantee, and fit within the Hoover City Schools IT department framework.

All purchases of computer hardware or software will be coordinated with the IT department. You should expect at least a two week turnaround on these proposals. That gives the IT department time to evaluate and advise.

Hardware or software that is not purchased within these guidelines will not be supported by Hoover City Schools' resources.

Equipment Guidelines

Laptops/Desktops purchased without Information Technology assistance:

- Information Technology will provide assistance for connecting the device to wireless guest networks
- Laptop/Desktop will **not** be part of the Information Technology replacement cycle
- Information Technology will **not** load software licensed by the district
- Information Technology will **not** provide hardware support or warranty services
- Information Technology will **not** provide virus/spyware removal assistance

Printers purchased without Information Technology assistance:

- Information Technology will **not** support this printer
- Information Technology will **not** network this printer

Appendix E

Acquisition of Software Procedures

The purpose of the Acquisition of Software Procedures is to:

- Ensure proper management of the legality of information systems,
- Allow all academic disciplines, administrative functions, and athletic activities the ability to utilize proper software tools,
- Minimize licensing costs,
- Increase data integration capability and efficiency of Hoover City Schools as a whole, and
- Minimize the malicious code that can be inadvertently downloaded.

A. Software Licensing:

1. All district software licenses owned by HCS will be:
    - kept on file at the central office,
    - accurate, up to date, and adequate, and
    - in compliance with all copyright laws and regulations
2. All other software licenses owned by departments or local schools will be:
    - kept on file with the department or local school technology office,
    - accurate, up to date, and adequate, and
    - in compliance with all copyright laws and regulations
3. Software installed on HCS technological systems and other electronic devices:
    - will have proper licensing on record,
    - will be properly licensed or removed from the system or device, and
    - will be the responsibility of each HCS employee purchasing and installing to ensure proper licensing
4. Purchased software accessed from and storing data in a cloud environment will have a Memorandum of Agreement (MOA) or contract on file that states or confirms at a minimum that:
    - HCS student and/or staff data will not be used for any purpose beyond the specific services requested by HCS and will not be shared with a third party unless specifically approved by HCS.
    - HCS student and/or staff data will not be sold or mined with or by a third party,
    - HCS student and/or staff data will not be stored on servers outside the US unless otherwise approved by Hoover City Schools' Data Governance Committee,
    - the company will comply with Hoover City School's guidelines for data transfer or destruction when contractual agreement is terminated, and
    - No API will be implemented without full consent of Hoover City Schools and the ALSDE.

5. Software with or without physical media (e.g. downloaded from the Internet, apps, or online) must still be properly evaluated and licensed if necessary and is applicable to this procedure. It is the responsibility of staff to ensure that all electronic resources are age appropriate, FERPA compliant, and are in compliance with software agreements before requesting use. Staff members are responsible for ensuring that parents have given permission for staff to act as their agent when creating student accounts for online resources when such permission is required by law.

B. Supported Software:

In an attempt to prevent software containing malware, viruses, or other security risk, software is categorized as Supported and Not Supported Software. For software to be classified as Supported Software downloads and/or purchases must be approved by the district technology director or designee such as a local school technology instructional coach or member of the technical staff.

- A list of supported software will be maintained on the Hoover City School's District Technology site.
- It is the responsibility of the HCS Technology Team members to keep the list current and for staff to submit apps or other software to the Technology Team.
- Unsupported software is considered New Software and must be approved or it will not be allowed on HCS owned devices.
- When staff recommends apps for the HCS Mobile Device Management Apps Catalog, Google Apps store or software for installation, it is assumed that the staff has properly vetted the app or software and that it is instructional sound, is in line with curriculum or behavioral standards, and is age appropriate.
- Software that accompanies adopted instructional materials will be vetted by the Curriculum and Instruction Director and the Technology Integration Coordinator and is therefore supported.

C. New Software:

In the Evaluate and Test Software Packages phase, the software will be evaluated against current standards and viability of implementation into the Hoover City Schools technology environment and the functionality of the software for the specific discipline or service it will perform.

1. Evaluation may include but is not limited to the following:
   - Conducting beta testing.
   - Determining how the software will impact the HCS technology environment such as storage, bandwidth, etc.
   - Determining hardware requirements.
   - Determining what additional hardware is required to support a particular software package.
   - Outlining the license requirements/structure, number of licenses needed, and renewals.
2. Determining any Maintenance Agreements including cost.

- Determining how the software is updated and maintained by the vendor.
- Determining funding for the initial purchase and continued licenses and maintenance.

3. When staff recommends apps for the HCS Mobile Device Management Apps Catalog, Google Apps Store or software for purchase and/or testing, it is the responsibility of the appropriate staff to properly vet the app or software to ensure that is instructionally sound, is in line with curriculum or behavioral standards, and is age appropriate.

Appendix F

Security Procedures

Physical Security

Controls are implemented to protect information system resources, the facility housing those resources, and the facilities used to support their operation. To protect against loss of control over system integrity and system availability, organizations need to address physical access controls, environmental controls, fire safety, and protect systems and data storage media from theft.

OBJECTIVE:

This procedure communicates the essential aspects of physical security of computing equipment and data storage media that must be practiced by all information technology organizations to safeguard the integrity and availability of State information system resources and data.

RESPONSIBILITIES:

Agency Management, Information Technology Organization:

Ensure computer systems and network equipment are properly secured to prevent unauthorized physical access and data is properly safeguarded to protect from loss.

Control access to areas containing servers, data stores, and communications equipment. Access to secured areas shall be controlled by the use of access card keys, access code keypads, or key locks with limited key distribution. A record shall be maintained of all personnel who have authorized access.

Closely control keys (where utilized). If a key is reported as missing, change or re-key the corresponding lock(s).

Change access codes, where utilized, at least every 90 days or immediately upon removing someone from the authorized access list.

Maintain a digital log of all visitors granted entry into secured areas or areas containing sensitive or confidential data (e.g., data storage facilities).

Ensure visitors are escorted by a person with authorized access to the secured area.

Ensure each facility containing computer and communications equipment has an appropriate fire suppression system and/or a class C fire extinguisher readily available and in working order.

Store equipment above the floor, in racks whenever feasible, or on a raised floor to prevent damage from dampness or flooding. Use of water/moisture sensors is recommended.

Monitor and maintain data center temperature and humidity levels. The American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) recommends an inlet temperature range of 68 to 77 degrees and relative humidity of 40% to 55%.

Store electronic media in secured and environmentally controlled areas, in fire safe containers whenever feasible. Backup/archive media shall, whenever feasible, be stored in a secure off-site storage facility.

Monitor and control the delivery and removal of all asset-tagged and/or data-storing IT equipment. Maintain a record of all such items entering or exiting their assigned location.

Ensure that equipment being removed for transfer to another organization or being designated as surplus property is appropriately sanitized in accordance with applicable policies and procedures.

Emergency Access:

Each entity is required to establish a mechanism to provide emergency access to systems and applications in the event that the assigned custodian or owner is unavailable during an emergency.

Procedures must be documented to address:

1. Authorization,
2. Implementation, and
3. Revocation

Appendix G Passwords

Password Control Standards

The Hoover City Schools Data Governance and Use Policy requires the use of **strictly** controlled passwords for accessing Personally Identifiable Information (PII), Confidential Information (CI) and Internal Information (II).

Listed below are the minimum standards that must be implemented in order to ensure the effectiveness of password controls.

Standards for accessing PII, CI, II:

Users are responsible for complying with the following password standards:

1. Passwords must never be shared with another person, unless the person is a designated security manager.
2. Every password must, where possible, be changed regularly – (between 90 and 180 days depending on the sensitivity of the information being accessed)
3. Passwords must, where possible, have a minimum length of six characters.
4. Passwords must never be saved when prompted by any application with the exception of central single sign-on (SSO) systems as approved by the ISO. This feature should be disabled in all applicable systems.
5. Passwords must not be programmed into a PC or recorded anywhere that someone may easily find and use them.
6. When creating a password, it is important not to use words that can be found in dictionaries or words that are easily guessed due to their association with the user (i.e. children's names, pets' names, birthdays, etc…). A combination of alpha and numeric characters are more difficult to guess.

Where possible, system software must enforce the following password standards:

1. Passwords routed over a network must be encrypted.
2. Passwords must be entered in a non-display field.
3. System software must enforce the changing of passwords and the minimum length.

Appendix H

Purchasing

This procedure is intended to provide for the proper purchasing and disposal of technological devices only. Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, AV equipment, server, internal or external storage, communication device or any other current or future electronic or technological device may be referred to as systems in this document. For further clarification of the term technological systems contact the Hoover City School's Chief Technology Officer.

All involved systems and information are assets of Hoover City Schools and are expected to be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

A. Purchasing Guidelines

All systems that will be used in conjunction with Hoover City Schools' technology resources or purchased, regardless of funding, should be purchased from an approved list or be approved by a local school Technology Coach and/or the district Chief Technology Officer. Failure to have the purchase approved may result in lack of technical support, request for removal from premises, or denial of access to other technology resources.

B. Alabama Competitive Bid Laws

Most electronic equipment is subject to Alabama competitive bid laws. There are several purchasing coops that have been approved for use by the Alabama State Examiners office: http://www.examiners.state.al.us/purchcoop.aspx. Generally for technological devices and services, Hoover City Schools purchase from the Alabama Joint Purchasing Agreement (ALJP): https://connect.alsde.edu/sites/eia/aljp/SitePages/ALJP%20(Alabama%20K-12%20(IT)%20Joint%20Purchasing)Home.aspx. In the event that a desired product is not included in one of these agreements, Hoover City Schools bids the item or items using the district's competitive bid process. Most technological systems, services, etc. over $15,000 purchased with public funds are subject to Alabama's competitive bid laws.

C. Inventory

All technological devices or systems over $500 are inventoried by the Technology Department in accordance with the Hoover City Schools Finance Department using the Destiney inventory system. There are some exceptions under $500, including, but not limited to, companion devices or peripherals that are inventoried. The district technology staff is responsible for ensuring that any network equipment, fileservers, or district systems, etc. are inventoried.

D. Disposal Guidelines

Equipment should be considered for disposal for the following reasons:

1. End of useful life,
2. Lack of continued need,
3. Obsolescence,
4. Wear, damage, or deterioration,
5. Excessive cost of maintenance or repair.

The local school principal, Chief Technology Officer, and the Chief Financial Officer must approve school disposals by discard or donation. Written documentation in the form of a spreadsheet including but not limited to the following must be provided.

1. Fixed asset tag (FAT) number,
2. Location,
3. Description,
4. Serial number, and
5. Original cost and account code if available.

E. Methods of Disposal

Once equipment has been designated and approved for disposal, it should be handled according to one of the following methods. It is the responsibility of the local school to modify the inventory entry to reflect any in-school transfers, in-district transfers, donations, or discards for technological systems. The district technology staff is responsible for modifying the inventory records to reflect any transfers within the central offices, transfers of central office electronic equipment to local schools, central office donations, or central office discards.

1. Transfer/Redistribution

If the equipment has not reached the end of its estimated life, an effort should be made to redistribute the equipment to locations where it can be of use, first within an individual school or office, and then within the district. Service requests may be entered to have the equipment moved, reinstalled and, in the case of computers, laptops, or companion devices, have it wiped and reimaged or configured.

1. Discard

All electronic equipment in the Hoover City Schools district must be discarded in a manner consistent with applicable environmental regulations. Electronic equipment may contain hazardous materials such as mercury, lead, and hexavalent chromium. In addition, systems may contain Personally Identifiable Information (PII), Confidential, or Internal Information. Systems must be wiped clean of this information prior to leaving the school district.

A district-approved vendor must be contracted for the disposal of all technological systems/equipment. The vendor must provide written documentation verifying the method used for disposal and a certificate stating that no data of any kind can be retrieved from the hard drive or any other component capable of storing data.

Under no circumstances should any technological systems/equipment be placed in the trash.

2. **Donation**

If the equipment is in good working order, but no longer meets the requirements of the site where it is located, and cannot be put into use in another part of a school or system, it may be donated upon the written request of the receiving public school system's superintendent or non-profit organization's director.

It should be made clear to any school or organization receiving donated equipment that Hoover City Schools is not agreeing to and is not required to support or repair any donated equipment. It is donated AS IS.

HCS staff should make every effort before offering donated equipment, to make sure that it is in good condition and can be re-used. Microsoft licenses or any other software licenses are not transferred outside the Hoover City School system.

Donations are prohibited to individuals outside of the school system or to current faculty, staff, or students of Hoover City Schools.

F. Required Documentation and Procedures

1. For purchases, transfers and redistribution, donations, and disposal of technology-related equipment, it is the responsibility of the appropriate technology team member to create/update the inventory to include previous location, new school and/or room location, and to note the transfer or disposal information. When discarding equipment, the fixed asset tag is removed from the equipment and turned in with other documentation to the local school bookkeeper. The CTO in turns submits to the CFO for approval and to the Superintendent's Office for Board approval.

2. When equipment is donated, a copy of the letter requesting the equipment must be on-file with the district technology office prior to the donation. Equipment is donated in order of request.

3. Any equipment donated should be completely wiped of all data. This step will not only ensure that no confidential information is released, but also will ensure that no software licensing

violations will inadvertently occur. For non-sensitive machines, all hard drives should be fully wiped using a wiping program approved by the district technology office, followed by a manual scan of the drive to verify that zeros were written.

4. Any re-usable hardware that is not essential to the function of the equipment that can be used as spare parts should be removed: special adapter cards, memory, hard drives, zip drives, CD drives, etc.

5. A district-approved vendor MUST handle all disposals that are not redistributions, transfers, or donations. Equipment should be stored in a central location prior to pick-up. Summary forms must be turned into district technology office and approved by the CFO prior to the scheduled "pick up" day. Mice, keyboards, and other small peripherals may be boxed together and should not be listed on summary forms.

Appendix I

Access Roles and Permissions

I. Student Information Applications

a. Any software system owned and/or managed by the District which is used to store, process, or analyze student educational records as defined by FERPA shall be subject to strict security measures.

InformationNow

SetsWeb

Infocus

Home Portal

b. Only Supervisory District Administrators will have responsibilities over the District Student Information Systems, which will determine appropriate roles and access to the data and will enforce compliance with these roles and permissions.

II. InformationNow Access

1. InformationNow enables authorized users to access the application from any device with internet access.

2. Only authorized users of INOW will be allowed access, no one is allowed to give out user name/password or allow someone to utilize the program while logged in. All personnel will log out of INOW when not in use or when leaving the room. No one will misuse any information or share any personal student information. Violation of our policy, misuse of data, or FERPA violation can have serious consequences, including loss of Federal funding and internal discipline,.

3. The technology department will monitor all use of INOW.

4. Confidentiality: Employees are provided the rights to utilize only the portions of INOW that the employee needs to perform their job duties and to prevent unauthorized personnel from seeing data that they are not approved to see or utilize. Strict measures are in place to oversee no one is given rights without district approval. Once a person is approved through the school board and documentation is submitted to human resources, they are input into INOW. Then one person in the district authorizes rights that reflect the requisition that is submitted.

5. Once the person is no longer employed, they are removed from Active directory, unable to log in. The rights are quickly removed from the database, allowing no further access.

6. Types of Users:

a. Personnel: In order to allow access to the correct personnel, InformationNow is integrated with Active Directory, which has a strong password requirement. All personnel must agree to the personnel acceptable use policy. Only long term subs that have been approved per the board and have signed the acceptable use policy will have access to INOW.

b. Students: Students are allowed to see their secure data through the Home Portal that includes attendance and grades under individual log in rights that are reset every year and that haves strong requirements for user names and passwords. They must agree to the acceptable use policy to access their data.

c. Parents/Guardians: The parents/guardians of secondary students have access to their student's grades and attendance through the Home Portal. They must provide proper documentation to prove to the local schools that they are the student's parent or guardian before access is granted. They must agree to the acceptable use policy to access data.

d. Volunteers: Due to FERPA and other confidentiality expectation, volunteers are granted VERY limited view only access to INOW. They must sign a confidentiality agreement at the local school before accessing any data.

(Form Attached)

7. Types of rights

Administrators: this is only for the default Administrator that has full rights.

Staff Affected: District Database Administrator

Rights: All rights

Admin1

Staff Affected: Superintendent, Assistant Superintendent, Chief Technology Officer, Network Administrator

Rights: limited full access to district except deleting, clearing, closing Academic sessions

Admin Grades

Staff Affected: one person at each school per the administrator

Rights: able to fix grades issues when teacher is not available but has approved.

Athletic Group

Staff Affected: one person at each secondary school athletic department

Rights: allows staff member to check Is Athlete for the C2C software

Attendance Group

Staff Affected: school staff members that are responsible for attendance and district student services department

Rights: Able to take attendance in the student maintenance area of INOW, can only put in check in, check outs, daily attendance, and other attendance – not related to attendance in classroom module. Able to search and find students as needed.

Bookkeepers

Staff affected: district and school bookkeepers

Rights: Allows for them to see students to pay fees appropriately.

Certification

Staff Affected: District person that checks certification of teachers

Rights: access to staff and what classes they teach for verification

College and Career

Staff Affected: one person assigned at each high school

Rights: able to check and select appropriate college and career readiness items from custom

Counselor

Staff Affected: all secondary counselors

Rights: able to assign appropriate schedules and look at transcripts and grades to make sure they are on the right track. They have access to the counseling area. Able to search and find students as needed.

Direct Lunch

Staff Affected: District CNP director

Rights: Can run district Lunch information, reports, and import

Discipline

Staff Affected: Only district assistant superintendent and school administrators

Rights: able to view, edit, and create discipline records

Discipline Read Only

Staff Affected: Chief Technology officer, one registrar from each high school and the district special ed coordinator

Rights: view only of discipline

District Enroll

Staff Affected: District Student services personnel

Rights: enroll at district level

District Personnel Administrator

Staff Affected: Central Office staff

Rights: View rights only of specific data needed for their department.

District Registrar

Staff Affected: district registrar

Rights: full editing rights and view of all schools to enroll and clean up data

Elementary Counselor

Staff Affected: Elementary counselors

Rights: view student basic information and contacts

ELL

Staff Affected: ELL teachers

Rights: able to edit ELL information

Enrichment

Staff Affected: Enrichment teachers

Rights: able to check the enrichment box under custom

Enrollment Clerk

Staff Affected: enrollment personnel at each school (registrars)

Rights: able to enroll student and input any data need for the student to enroll

General School

Staff Affected: staff members that needed to view all students (special ed, enrichment, front office staff)

Rights: able to view basic information of students – very limited, only to find student, view health conditions, view special instructions, contacts, lockers, and basic schedule

Grade Setup

Staff Affected: Registrars

Rights: set up basic grade information like posting grading periods and added announcements to report cards. Cannot change major parts of grading or grades themselves

Groups

Staff Affected: athletic secretaries

Rights: to put students in athletic programs that will upload to schoolmessenger

Human Resource

Staff Affected: human resources dept

Rights: add staff member – cannot give rights can only add the staff member's name and information

Infocus

Staff Affected: district or school administration

Rights: access to reports in Infocus

iPads and Email

Staff Affected: project specialist and secretary

Rights: able to check the iPad ELI agreement box and send emails, able to see general student info and contact info

Lunch codes

Staff Affected: Lunchroom managers and District CNP Director

Rights: lunch codes for students

Nurse

Staff Affected: nurses and approved subs

Rights: Medical information for students

Paid Sub

Staff Affected: subs and approved volunteers

Rights: LIMITED view only rights to find student

Past Academic Session

Staff Affected: Registrars and administrator

Rights: view previous years data for reporting purposes

PE Teachers

Staff Affected: PE staff

Rights: able to do fitness screening

Phone numbers

Staff Affected: transportation department

Rights: able to view phone numbers for students in case of emergency

Query

Staff Affected: authorized office staff

Rights: able to run queries for reports

Schedule Group

Staff Affected: one administrator for each secondary and one registrar for each elementary

Rights: set up master schedule and assign students, cannot add anything to valid courses, only district database administrator adds courses to the valid course area

School tab

Staff Affected: front desk personnel

Rights: needs access to bus and locker information

SchoolEdit Group

Staff Affected: approved office staff

Rights: able to edit general information on student like

School Personnel Administrator

Staff Affected: school administrators and registrars

Rights: general view rights of all students in local school and editing rights of general information

SETS Staff

Staff Affected: special ed teacher units

Rights: able to access their students from SetsWeb and create and edit special ed folders for students under their care

SRO Officers

Staff Affected: SRO officers

Rights: general view only rights to directory information.

SS number access

Staff Affected: selected (approved) office personnel

Rights: rights to see social security numbers for students due to paperwork or reports they are responsible for.

Staff Change

Staff Affected: Secretary to superintendent and certification specialist

Rights: able to change any information on a staff member that is incorrect

Staff Social

Staff Affected: Administrators and approved per admin secretaries

Rights: able to see staff social security numbers for legal purposes, paperwork, or reports that are needed

Student filter

Staff Affected: office staff and administrators

Rights: able to change and add student filters for reports

Transcript Area Maintain

Staff Affected: person at each high school that is approved

Rights: for adding transcript information for transfer students and any manual entry due to credit recovery or summer school

Transcript Clerk

Staff Affected: transcript clerk and athletic secretary

Rights: print only rights for transcripts

BGIS Teachers

Staff Affected: brocks gap teachers

Rights: rights for classroom grades, attendance, and email

Teacher

Staff Affected: Teachers

Rights: rights for classroom grades, attendance, and email, cannot change options (set to category points)

Teacher Middle

Staff Affected: middle school teachers

Rights: rights for classroom grades, attendance, and email – cannot change categories or options (set to category points)

Tech

Staff Affected: technology dept

Rights: general view rights for log ins

Appendix J

Sample Hoover City Schools
Services and Systems Memorandum
of Agreement (MOA)

THIS MEMORANDUM OF AGREEMENT, executed and effective as of the ___ day of _____________, 20__, by and between _________________, a corporation organized and existing under the laws of _____________ (the “Company”), and **Hoover City Schools (HCS)**, a public school system organized and existing under the laws of the state of Alabama (the “School Board”), recites and provides as follows.

Recitals

The Company and the School Board are parties to a certain agreement entitled “_________________________” hereafter referred to as (the “Agreement”). In connection with the execution and delivery of the Agreement, the parties wish to make this Memorandum of Agreement (also referred to as MOA or Addendum) a part of the original Agreement in order to clarify and/or make certain modifications to the terms and conditions set forth in the original Agreement.

The Company and the School Board agree that the purpose of such terms and conditions is to ensure compliance with the Family Educational Rights and Privacy Act (FERPA) and the overall privacy and security of student Personally Identifiable Information (PII) hereafter referred to as student information and/or data, including but not limited to (a) the identification of the Company as an entity acting for the School Board in its performance of functions that a School Board employee otherwise would perform; and (b) the establishment of procedures for the protection of PII, including procedures regarding security and security breaches.

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is acknowledged hereby, the parties agree as follows.

Agreement

The following provisions shall be deemed to be included in the Agreement:

<u>Confidentiality Obligations Applicable to Certain HCS Student Records</u>. The Company hereby agrees that it shall maintain, in strict confidence and trust, all HCS student records containing personally identifiable information (PII) hereafter referred to as “Student Information”. Student information will not be shared with any other resource or entity that is outside the intended purpose of the Agreement.

The Company shall cause each officer, director, employee and other representative who shall have access to HCS Student Records during the term of the Agreement (collectively, the “Authorized Representatives”) to maintain in strict confidence and trust all HCS Student Information. The Company shall take all reasonable steps to insure that no HCS Student information is disclosed to any person or entity except those who (a) are Authorized Representatives of the Company performing functions for HCS under the Agreement and have agreed to be bound by the terms of this Agreement; (b) are authorized representatives of HCS, or (c) are entitled to such HCS student information from the Company pursuant to federal and/or Alabama law. The Company shall use HCS student information, and shall take all reasonable steps necessary to ensure that its Authorized Representatives shall use such information, solely for purposes related to and in fulfillment of the performance by the Company of its obligations pursuant to the Agreement.
The Company shall: (a) designate one of its Authorized Representatives to be responsible for ensuring that the Company and its Authorized Representatives maintain the HCS student information as confidential; (b) train the other Authorized Representatives with regard to their confidentiality responsibilities hereunder and pursuant to federal and Alabama law; (c) maintain at all times a list of Authorized Representatives with access to HCS student information.

Other Security Requirements. The Company shall maintain all technologies, policies, procedures and practices necessary to secure and protect the confidentiality and integrity of HCS student information, including procedures to (a) establish user IDs and passwords as necessary to protect such information; (b) protect all such user passwords from detection and unauthorized use; (c) prevent hostile or unauthorized intrusion that could result in data corruption, or deny service; (d) prevent and detect computer viruses from spreading to disks, attachments to e-mail, downloaded files, and documents generated by word processing and spreadsheet programs; (e) minimize system downtime; (f) notify HCS of planned system changes that may impact the security of HCS data; (g) return or destroy HCS data that exceed specified retention schedules; (h) notify HCS of any data storage outside the US; (i) in the event of system failure, enable immediate recovery of HCS information to the previous business day. The Company should guarantee that HCS data will not be sold to, accessed by, or moved by third parties.

In the event of a security breach, the Company shall (a) immediately take action to close the breach; (b) notify HCS within 24 hours of Company's first knowledge of the breach, the reasons for or cause of the breach, actions taken to close the breach, and identify the HCS student information compromised by the breach; (c) return compromised HCS data for review; (d) provide communications on the breach to be shared with affected parties and cooperate with HCS efforts to communicate to affected parties by providing HCS with prior review of press releases and any communications to be sent to affected parties; (e) take all legally required, reasonable, and customary measures in working with HCS to remediate the breach which may include toll free telephone support with informed customer services staff to address questions by affected parties and/or provide monitoring services if necessary given the nature and scope of the disclosure; (f) cooperate with HCS by providing information, records and witnesses needed to respond to any government investigation into the disclosure of such records or litigation concerning the breach; and (g) provide HCS with notice within 24 hours of notice or service on Company, whichever occurs first, of any lawsuits resulting from, or government investigations of, the Company's handling of HCS data of any kind, failure to follow security requirements and/or failure to safeguard HCS data. The Company's compliance with the standards of this provision is subject to verification by HCS personnel or its agent at any time during the term of the Agreement. Said information should only be used for the purposes intended and should not be shared, sold, or moved to other companies or organizations nor should other companies or organization be allowed access to said information.

Disposition of HCS Data Upon Termination of Agreement

Upon expiration of the term of the Agreement, or upon the earlier termination of the Agreement for any reason, the Company agrees that it promptly shall deliver to the School Board, and shall take all reasonable steps necessary to cause each of its Authorized Representatives promptly to deliver to the School Board, all required HCS student data and/or staff data. The Company hereby acknowledges and agrees that, solely for purposes of receiving access to HCS data and of fulfilling its obligations pursuant to this provision and for no other purpose (including without limitation, entitlement to compensation and other employee benefits), the Company and its Authorized Representatives shall be deemed to be school officials of the School Board, and shall maintain HCS data in accordance with all federal state and local laws, rules and regulations regarding the confidentiality of such records. The non-disclosure obligations of the Company and its Authorized Representatives regarding the information contained in HCS data shall survive termination of the Agreement. The Company shall indemnify and hold harmless the School Board from and against any loss, claim, cost (including attorneys' fees) or damage of any nature arising from or in connection with the breach by the Company or any of its officers, directors, employees, agents or representatives of the obligations of the Company or its Authorized Representatives under this provision.

Certain Representations and Warranties. The Company hereby represents and warrants as follows: (a) the Company has full power and authority to execute the Agreement and this MOA and to perform its obligations hereunder and thereunder; (b) the Agreement and this MOA constitute the valid and binding obligations of the Company, enforceable in accordance with their respective terms, except as such enforceability may be limited by bankruptcy or similar laws affecting the rights of creditors and general principles of equity; and (c) the Company's execution and delivery of the Agreement and this Addendum and compliance with their respective terms will not violate or constitute a default under, or require the consent of any third party to, any agreement or court order to which the Company is a party or by which it may be bound.

Governing Law; Venue. Notwithstanding any provision contained in the Agreement to the contrary, (a) the Agreement shall be governed by and construed in accordance with the laws of the State of Alabama, without reference to conflict of laws principles; and (b) any dispute hereunder which is not otherwise resolved by the parties hereto shall be decided by a court of competent jurisdiction located in the State of Alabama.

IN WITNESS WHEREOF, the parties hereto have caused this Addendum to be executed by their duly authorized officers effective as of the date first written above.

[COMPANY NAME]

By:______________________________

[Name]
[Title]

Hoover City Schools

By:______________________________

HOOVER CITY SCHOOLS

STUDENT DATA CONFIDENTIALITY AGREEMENT

I acknowledge my responsibility to respect the confidentiality of student educational records. I will ensure that educational records, including data on individual students, is not created, collected, stored, maintained, or disseminated in violation of state and federal laws.

Furthermore, I agree to the following guidelines regarding the appropriate use of educational records made available to me from other school/system employees, iNow, SETS or any other file or application I have access to:

- I will comply with school district, state and federal confidentiality laws, including the state Data and Information Governance and Use Policy, the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g and 34 CFR Part 99; and, and the Hoover City Schools Student Data Confidentiality Agreement.
- Educational records will only be accessed for students for whom I have a legitimate educational interest.
- I understand that educational records are never to be transmitted via e-mail or as an e-mail attachment unless the file is encrypted and/or password protected.
- I understand that it is illegal for a student to have access to another student's educational records. I will not share any student's educational records with another student.
- I will securely log in and out of the programs that store educational records. I will not share my password. Any electronic data containing educational records will be stored securely within the District network or within a password protected environment. I will not store student specific data on any personal computer and/or external devices that are not password protected. (external devices include but are not limited to USB/Thumb drives and external hard drives)
- I will protect educational records from unauthorized disclosure, including information on a computer display.

By signing below, I acknowledge, understand and agree to accept all terms and conditions of the Hoover City Schools Student Data Confidentiality Agreement.

Signature of Employee___________________________ Date_____________

Job Title ______________________________________ School___________