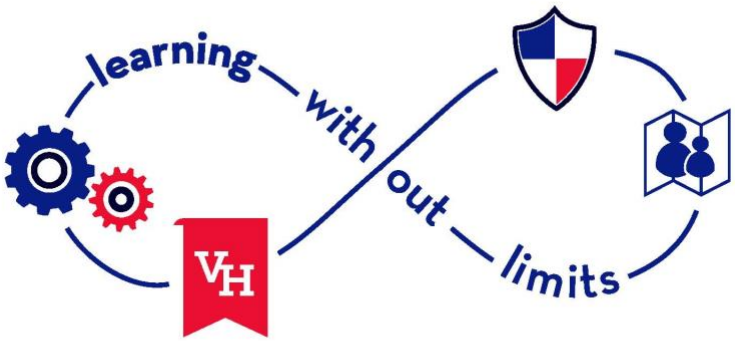


Vestavia Hills City Schools

Data Governance Policy

Presented to Vestavia Hills City Schools Board of Education

Table of Contents

The following documents area affiliated with Vestavia Hills City Schools Data Governance policy, procedures, training, and guidance.

INTRODUCTION

Committee Members

POLICY

APPENDICES

A. Laws, Statutory, Regulatory, and Contractual Security
B. Requirements Information Risk Management Practices
C. Definitions and Responsibilities
D. Data Classification Levels
E. Acquisition of Hardware
F. Acquisition of Software Procedures
G. Virus, Malware, Spyware, Phishing and SPAM Protection
H. Physical and Security Controls
I. Password Control Standards
J. Purchasing and Disposal Procedures
K. Data Access Roles and Permissions
L. Memorandum of Agreement (MOA)

RESOURCES

ALSDE State Monitoring Checklist
Record Disposition Requirements
Email Guidelines

FORMS

Student Data Confidentiality Agreement
Employees Laptop Contract
Student Technology Agreement

INTRODUCTION

Protecting the privacy of students and staff is an important priority, and Vestavia Hills City Schools is committed to maintaining strong and meaningful privacy and security protections. The privacy and security of this information is a significant responsibility, and school officials value the trust of students, parents and staff.

The Vestavia Hills City Schools Data Governance document includes information regarding the Data Governance Committee, the actual Vestavia Hills City Schools Data and Information Governance and Use Policy, applicable Appendices, and Supplemental Resources.

The policy formally outlines the means by which operational and instruction activity shall be carried out to ensure Vestavia Hills City Schools' data are accurate, accessible, consistent, and protected. The document establishes who is responsible for information under various circumstances and specifies the procedures to be used to manage and protect it.

The Vestavia Hills City Schools Data Governance Policy shall be a living document. To make the document flexible, details are outlined in the Appendices. With the Board's approval, the Data Governance Committee may quickly modify information in the Appendices in response to changing needs. All modifications shall be posted on the Vestavia Hills City Schools website.

2017-18 Data Governance Committee

Charles Mason - Superintendent
Kimball Clayton – Systems Administrators
Michael Young – Systems Administrators
Bebe Galloway – Data Management Specialist
Jan Garfinkle – Instructional Technology Specialist
Jane-Marie Marlin – Director of Curriculum and Instruction
Brooke Brown – Director of Curriculum and Instruction

Committee Meetings

The Data Governance committee shall meet, at a minimum, two times per year. Additional meetings shall be called as needed.

Vestavia Hills City Schools Data Governance Policy

I. POLICY

A. It is the policy of Vestavia Hills City Schools that data or inform in all its forms--written, spoken, electronic, or printed – is protected from accidental or intentional unauthorized modification destruction, or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment, software, and practices used to process, store, and transmit data or information

B. The data governance policies and procedures must be documented and reviewed

C. Vestavia Hills City Schools conducts annual training on its data governance policy and documents

D. The terms "data" and "information" are used separately, together, and interchangeably throughout the policy. The intent is the same.

II. SCOPE

The superintendent is authorized to establish, implement, and maintain data and information security measures. The policy, standards, processes, and procedures apply to all students and employees of the district, contractual third parties and agents of the district, and volunteers who have access to district data systems or data. This policy and all its standards apply to all protected health information and other classes of protected information in any form.

This policy applies to all forms of Vestavia Hills City Schools' data and information, including but not limited to:

A. Speech, spoken face-to-face, or communicated by phone or any current and future technologies;
B. Hard copy data printed or written;
C. Communications sent by post/courier, fax, electronic mail, text, chat, and/or any form of social media, etc.;
D. Data stored and/or processed by servers, PC's, laptops, tablets, mobile devices, etc.; and
E. Data stored on any type of internal, external, or removable media or cloud based services.

III. REGULATORY COMPLIANCE

Vestavia Hills City Schools will abide by any law, statutory, regulatory, or contractual obligations affecting its information systems, acts including, but not limited to, the following:

A. Children's Internet Protection Act (CIPA)
B. Children's Online Privacy Protection Act (COPPA)
C. Family Educational Rights and Privacy Act (FERPA)
D. Health Insurance Portability and Accountability Act (HIPAA)
E. Payment Card Industry Data Security Standard (PCI DSS)
F. Protection of Pupil Rights Amendment (PPRA)

See also Appendix A (Laws, Statutory, Regulatory, and Contractual Security)

IV. RISK MANAGEMENT

A. A thorough risk analysis of all Vestavia Hills City Schools' data networks, systems, policies, and procedures shall be conducted on an annual basis or as requested by the Superintendent or designee. The risk assessment shall be used as a basis for a plan to mitigate identified threats – internal or external, natural or man-made, electronic and non-electronic and risk to an acceptable level.

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

See also Appendix B (Requirements Information Risk Management Practices)
See also Appendix C (Definitions and Responsibilities)

V. DATA CLASSIFICATION

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

See also Appendix D (Data Classification Levels)

VI. SYSTEMS AND INFORMATION CONTROL

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

* ***See also Appendix E (Acquisition of Hardware)***

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

Software Installation and Use: All software packages that reside on technological systems within or used by Vestavia Hills City Schools shall comply with applicable licensing agreements and restrictions and shall comply with Vestavia Hills City Schools' acquisition of software procedures.

****See also Appendix F (Acquisition of Software Procedures)***

Virus, Malware, Spyware, Phishing and Spam Protection: Virus checking systems approved by the Vestavia Hills City Schools' District Technology Department are deployed using a multi-layered approach (computers, servers, gateways, firewalls, filters, etc.) that ensures all electronic files are appropriately scanned for viruses, malware, spyware, phishing and spam. Users shall neither turn off nor disable Vestavia Hills City Schools' protection systems or install other systems.

****See also Appendix G (Virus, Malware, Spyware, Phishing and Spam Protection, *See Vestavia Hills City Schools Information Security Policy Handbook: Antivirus Policy pg. 3***

Access Controls: Physical and electronic access to information systems that contain Personally Identifiable Information (PII), Confidential Information, Internal Information and computing resources is controlled. To ensure appropriate levels of access by internal workers, a variety of security measures are instituted as recommended by the Data Governance Committee and approved by Vestavia Hills 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 Information, Internal Information and computing resources include, but are not limited to, the following methods:

Authorization: Access shall be granted on a "need to know" basis and shall be authorized by the superintendent, principal, immediate supervisor, or Data Governance Committee with the assistance of the Technology Department. Specifically, on a case-by-case basis, permissions may be added to those already held by an individual user in the student management system, again on a need-to-know basis, and only in order to fulfill specific job responsibilities, with approval of the Data Governance Committee.

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

Identification/Authentication: Unique user identification (User ID) and authentication are required for all systems that maintain or access PII, Confidential Information, and/or Internal Information. Users shall be held accountable for all actions performed on the system with their User ID. User accounts and passwords shall NOT be shared.

- At least one of the following authentication methods must be implemented:
    - Strictly controlled passwords
    - Biometric identification, and/or
    - Token in conjunction with a PIN
- The user must secure his/her authentication control (e.g password, token) such that only that user and possibly a designated security manager know it.
- The user must log off or secure the system when leaving it.

Data Integrity: Vestavia Hills City Schools provides safeguards so that PII, Confidential, and Internal Information are not altered or destroyed in an unauthorized manner. Core data are backed up to a private cloud for disaster recovery. In addition, listed below are methods that are used for data integrity in various circumstances:

- Transaction audit
- Disk redundancy (RAID)

- ECC (Error Correcting Memory)
- Checksums (file integrity)
- Data encryption
- Data Wipes

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

- Integrity controls and
- Encryption, where deemed appropriate
- Access control lists

Note: Only Vestavia Hills City Schools district-supported email accounts shall be used for communications to and from school employees, to and from parents or other community members, to and from other educational agencies, to and from vendors or other associations, and to and from students for school business.

Remote Access: This policy defines standards for connecting to VHCS's network from any host, as well as to define standards for connecting to customer networks in which managed services are provided. These standards are designed to minimize the potential exposure to VHCS from damages, which may result from unauthorized use of resources. Damages include the loss of sensitive or system confidential data, intellectual property, damage to public image, damage to critical VHCS internal systems, etc.
All VHCS staff, contractors, vendors and agents with a VHCS-owned or personally owned computer or workstation used to connect to the VHCS network. This Policy applies to remote access connections used to do work on behalf of VHCS, including reading or sending email and viewing intranet web resources.
Remote access implementations that are covered by this Policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.
Access into Vestavia Hills City Schools' internal network from outside is allowed using the Vestavia Hills City Schools VPN service. All other network access options are strictly prohibited without explicit authorization from the Systems Administrators and/or Data Governance Committee. Further, PII, Confidential Information and/or Internal Information that is stored or accessed remotely shall maintain the same level of protections as information stored and accessed within the Vestavia Hills City Schools' network. PII shall only be stored in cloud storage if the Data Governance Committee or its designees have approved storage.

See Vestavia Hills City Schools Information Security Policy Handbook: Remote Access pg. 11

Physical and Electronic Access and Security: Access to areas in which information processing is carried out shall be restricted only to appropriately authorized individuals. At a minimum, staff passwords shall be changed annually.

- No PII, Confidential and/or Internal Information shall be stored on a device such as a hard drive, mobile device of any kind, or external storage device that is not located within a secure area.
- No technological systems that may contain information as defined above shall be disposed of or moved without adhering to the appropriate Purchasing and Disposal of Electronic Equipment procedures.
- It is the responsibility of the user that devices noted in bullet #1 above not be left logged in, unattended, and open to unauthorized use.

See also Appendix H (Physical and Security Controls)
See also Appendix I (Password Control Standards)
See also Appendix J (Purchasing and Disposal Procedures)
See also Appendix K (Data Access Roles and Permissions)

Data Transfer/Exchange Printing:

- **Electronic Mass Data Transfers:** Downloading, uploading or transferring PII, Confidential Information, and Internal Information between systems shall be strictly controlled. Requests for mass download of, or individual request for, information for research or any other purposes that include PII shall be in accordance with this policy and be approved by the Data Governance Committee. All other mass downloads of information shall be approved by the committee and/or Systems Administrators, and include only the minimum amount of information necessary to fulfill the request. A Memorandum of Agreement (MOA) shall 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, unless the Data Governance Committee approves the exception.

See also Appendix L (Memorandum of Agreement)

- **Other Electronic Data Transfers and Printing:** PII, Confidential Information, and Internal Information shall be stored in a manner inaccessible to unauthorized individuals. PII and Confidential Information shall not be downloaded, copied or printed indiscriminately or left unattended and open to compromise. Where possible, PII that is downloaded for educational purposes shall be de-identified before use.

Oral Communications: Vestavia Hills City Schools' employees shall be aware of their surroundings when discussing PII and Confidential Information. This includes but is not limited to the use of cellular telephones in public areas. Vestavia Hills City Schools' staff shall not discuss PII or Confidential Information in public areas if the information can be overheard. Caution shall be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.

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.

Evaluation: Vestavia Hills City Schools requires that periodic technical and non-technical evaluations of access controls, storage, and other systems be performed in response to environmental or operations changes affecting the security of electronic PII to ensure its continued protection.

IT Disaster Recovery: Controls shall ensure that Vestavia Hills 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 any instances immediately to the Superintendent and Technology Department for response to a system emergency or other occurrence (ex. Fire, vandalism, system failure and natural disaster) that damages data or systems. The IT Disaster Recovery shall include the following:

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

Specific goals of the plan are:

- To be operational at a standby facility
- To reinstate VHCS facilities in the VHCS premises
- To minimize the disruption to VHCS's business

See Vestavia Hills City Schools Information Security Policy Handbook: Disaster Recovery pg. 29.

VIII. COMPLIANCE

The Data Governance Policy applies to all users of Vestavia Hills City Schools' information including: employees, staff, students, volunteers, and outside affiliates. Failure to comply with this policy by employees, staff volunteers, and outside affiliates may result in disciplinary action up to and including dismissal in accordance with applicable Vestavia Hills City Schools' procedures, or, in the case of outside affiliates, termination of the affiliation. Failure to comply with this policy by students may constitute grounds for corrective action in accordance with Vestavia Hills City Schools' policies. Further, penalties associated with state and federal laws may apply.

Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:

- Unauthorized disclosure of PII or Confidential Information.
- Unauthorized disclosure of a log-in code (User ID and password).
- Attempting to obtain a log-in code or password that belongs to another person.
- Using or attempting to use another person's log-in code or password.
- Unauthorized use of an authorized password to invade student or employee privacy by examining records or information for which there has been no request for review.
- Installing or using unlicensed software on Vestavia Hills City Schools' technological systems.
- The intentional unauthorized altering, destruction, or disposal of Vestavia Hills City Schools' information data and/or systems. This includes the unauthorized removal from Vestavia Hills City Schools of technological systems such as but not limited to laptops, internal or external storage, computers, servers, backups or other media, copiers, etc. that contain PII or confidential information.
- Attempting to gain access to log-in codes for purposes other than for support by authorized technology staff, including the completion of fraudulent documentation to gain access.

Laws, Statutory, Regulatory, and Contractual Security Requirements
Appendix A

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

CIPA: Congress enacted the **Children's Internet Protection Act** 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 shall include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they shall 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. For more information, see: http://www.fcc.gov/guides/childrens-internet-protection-act

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

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. For more information, see:
http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

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. For more information, see:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/
In general, schools are not bound by HIPAA guidelines.

PCI DSS: A consortium of payment brands including American Express, Discover, MasterCard, and Visa created the **Payment Card Industry Data Security Standard**. It covers the management of payment card data and is relevant for any organization that accepts credit card payments. For more information, see: www.pcisecuritystandards.org

PPRA: The **Protection of Pupil Rights Amendment** affords parents and minor students' rights regarding our conduct of surveys, collection and use of information for marketing purposes, and certain physical exams.

These include the right to the following: Consent before students are required to submit to a survey that concerns one or more of the following protected areas ("protected information survey") if the survey is funded in whole or in part by a program of the U.S. Department of Education (ED)–

- Political affiliations or beliefs of the student or student's parent;
- Mental or psychological problems of the student or student's family;
- Sex behavior or attitudes;
- Illegal, anti-social, self-incriminating, or demeaning behavior;
- Critical appraisals of others with whom respondents have close family relationships;
- Legally recognized privileged relationships, such as with lawyers, doctors, or ministers;
- Religious practices, affiliations, or beliefs of the student or parents; or
- Income, other than as required by law to determine program eligibility.

Receive notice and an opportunity to opt a student out of –

- Any other protected information survey, regardless of funding;
- Any non-emergency, invasive physical exam or screening required as a condition of attendance, administered by the school or its agent, and not necessary to protect the immediate health and safety of a student, except for hearing, vision, or scoliosis screenings, or any physical exam or screening permitted or required under State law; and

- Activities involving collection, disclosure, or use of personal information obtained from students for marketing or to sell or otherwise distribute the information to others.

For more information, see: http://www2.ed.gov/policy/gen/guid/fpco/ppra/index.html

Information Risk Management Practices
Appendix B

The analysis involved in Vestavia Hills City Schools Risk Management Practices examines the types of threats – internal or external, natural or manmade, electronic and non-electronic – that affect the ability to manage and protect the information resource. The analysis also documents any existing vulnerabilities found within each entity, which potentially exposes the information resource to the threats. Finally, the analysis includes an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection.

From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information is determined and addressed based on recommendations by the Data Governance Committee. The frequency of the risk analysis is determined at the district level. It is the option of the superintendent or designee to conduct the analysis internally or externally.

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as VHCS Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the VHCS Confidential information in question.

See Vestavia Hills City Schools Information Security Policy Handbook: Information Sensitivity pg. 15.

Definitions and Responsibilities
Appendix C

Definitions

A. **Availability**: Data or information is accessible and usable upon demand by an authorized person.
B. **Confidentiality**: Data or information is not made available or disclosed to unauthorized persons or processes.
C. **Data**: Facts or information
D. **Entity**: Organization such as school system, school, and department or in some cases business
E. **Information**: Knowledge that you get about something or someone; facts or details.
F. **Data Integrity**: Data or information has not been altered or destroyed in an unauthorized manner.
G. **Involved Persons**: Every user of Involved Systems (see below) at Vestavia Hills City Schools – no matter what their status. This includes nurses, residents, students, employees, contractors, consultants, temporaries, volunteers, substitutes, student teachers, interns, etc.
H. **Systems**: All data-involved computer equipment/devices and network systems that are operated within or by the Vestavia Hills City Schools physically or virtually. This includes all platforms (operating systems), all computer/device sizes (personal digital assistants, desktops, mainframes, telephones, laptops, tablets, game consoles, etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.
I. **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.
J. **Risk**: The probability of a loss of confidentiality, integrity, or availability of information resources.

Responsibilities Data Governance Committee: The Data Governance Committee for Vestavia Hills City Schools is responsible for working to ensure security policies, procedures, and standards are in place and adhered to by the entity.

Other responsibilities include:

- Reviewing the Data Governance Policy annually and communicating changes in policy to all involved parties.

- Educating data custodians and manage owners and users with comprehensive information about security controls affecting system users and application systems.

User Management: Vestavia Hills City Schools' administrators are responsible for overseeing their staff use of information and systems, including:

- Reviewing and approving all requests for their employees' access authorizations.
- Initiating security change requests to keep employees' secure access 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 Technology Department and the Data Governance Committee the loss or misuse of Vestavia Hills 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 technology or data system/software to manage information.
- Following all privacy and security policies and procedures.

Information Owner: The owner of a collection of information is usually the administrator or supervisor responsible for the creation of that information. In some cases, the owner may be the primary user of that information. 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 Vestavia Hills City Schools Information Owner Delegation/Transfer Request Form and submitting the form to the Data Governance Committee for approval. 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 ALSDE guidelines, industry standards, Data Governance Committee guidelines, or advice from the school system attorney.
- Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created.
- Authorizing access and assigning data custodianship if applicable.
- Specifying controls and communicating the control requirements to the data custodian and users of the information.

- Reporting promptly to the Technology Department the loss or misuse of Vestavia Hills City Schools' data.
- Initiating corrective actions when problems are identified.
- Promoting employee education and awareness by utilizing programs approved by the Technology Department, where appropriate.
- Following existing approval processes within the respective organizational unit and district for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

Data Custodian: An administrator or the Technology Department assigns Data Custodian based on his/her role and is generally responsible for the processing and storage of the information. The data 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 Data Governance Committee for use and disclosure using procedures that protect the privacy of the information.
- Maintaining information security policies, procedures and standards as appropriate and in consultation with the Data Governance Committee.
- Promoting employee education and awareness by utilizing programs approved by the Technology Department, where appropriate.
- Reporting promptly to the Data Governance Committee the loss or misuse of Vestavia Hills City Schools' data.
- Identifying and responding to security incidents and initiating appropriate actions when problems are identified.

User: The user is any person who has been authorized to read, enter, print or update information. A user of information is expected to:

- Access information only in support of their authorized job responsibilities.
- Comply with all data security procedures and guidelines in the Vestavia Hills City Schools Data Governance Policy and all controls established by the data owner and/or data custodian.
- Keep personal authentication devices (e.g. passwords, secure cards, PINs, access codes, etc.) confidential.
- Report promptly to the Data Governance Committee the loss or misuse of Vestavia Hills City Schools' information.
- Follow corrective actions when problems are identified.

Data Classification Levels
Appendix D

Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is information about an individual maintained by an agency, including:

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

Unauthorized or improper disclosure, modification, or destruction of this information could violate state and federal laws, result in civil and criminal penalties, and cause serious legal implications for Vestavia Hills City Schools.

Confidential Information

Confidential Information is very important and highly sensitive material that is not classified as PII. This information is private or otherwise sensitive in nature and shall be restricted to those with a legitimate business need for access.

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

Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for Vestavia Hills City Schools, its staff, parents, students including contract employees, or its business partners. Decisions about the provision of access to this information shall always be cleared through the information owner and/or Data Governance Committee.

Internal Information

Internal Information is intended for unrestricted use within Vestavia Hills City Schools, and in some cases within affiliated organizations such as Vestavia Hills City Schools' business or community partners. This type of information is already widely-distributed within Vestavia Hills 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, internal policies and procedures, most internal electronic mail messages.

Any information not explicitly 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 Vestavia Hills City Schools. Examples of Public Information may include marketing brochures and material posted to Vestavia Hills City Schools' web pages.

This information may be disclosed outside of Vestavia Hills City Schools.

Directory Information

Vestavia Hills City Schools defines Directory information as follows:

1. Student first and last name
2. Student gender
3. Student home address
4. Student home telephone number
5. Student school-assigned monitored and filtered email address
6. Student photograph
7. Student place and date of birth
8. Student dates of attendance (years)
9. Student grade level
10. Student diplomas, honors, awards received
11. Student participation in school activities or school sports
12. Student weight and height for members of school athletic teams
13. Student most recent institution/school attended
14. Student ID number

See Vestavia Hills City Schools Information Security Policy Handbook: Information Sensitivity pg. 15

Acquisition of Hardware
Appendix E

It is the position of Vestavia Hills City Schools' Technology 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 Vestavia Hills City Schools Technology Department framework.

All purchases of computer hardware or software will be coordinated with the Technology Department.

Vestavia Hills City Schools' resources will not support hardware or software that is not purchased within these guidelines.

Equipment Guidelines

- Laptops/Desktops purchased without Technology Department assistance
- Technology Department will provide assistance for connecting the device to wireless guest networks
- Laptop/Desktop will not be part of the Technology Department replacement cycle
- Technology Department will not load software licensed by the district
- Technology Department will not provide hardware support or warranty services
- Technology Department will not provide virus/spyware removal assistance
- Technology Department will not support nor network printers purchased that are not on VHCS Spec List

Acquisition of Software Procedures
Appendix F

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 Vestavia Hills City Schools (VHCS) as a whole, and
- Minimize the malicious code that can be inadvertently downloaded.

Software Licensing:

All district software licenses owned by Vestavia Hills City Schools will be:

- kept on file at the data center,
- accurate, up to date, and adequate, and
- in compliance with all copyright laws and regulations

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

Software installed on Vestavia Hills City Schools 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 Vestavia Hills City Schools employee purchasing and installing to ensure proper licensing

Purchased software accessed from and storing data in a cloud environment will have a Memorandum of Agreement (MOA) on file that states or confirms at a minimum that:

- Vestavia Hills City Schools student and/or staff data will not be shared, sold, or mined with or by a third party,
- VHCS student and/or staff data will not be stored on servers outside the US unless otherwise approved by Vestavia Hills City Schools' Data Governance Committee,
- the company will comply with VHCS guidelines for data transfer or destruction when contractual agreement is terminated, and
- No API will be implemented without full consent of VHCS and the ALSDE

Software with or without physical media (e.g. downloaded from the Internet, apps, or online) shall 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.

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 the district technology department or designee such as a local school technology specialist or member of the technical staff shall approve purchases.

- Unsupported software is considered New Software and shall be approved or it will not be allowed on VHCS owned devices.
- When staff recommends apps for the VHCS Mobile Device Management Apps 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 Department and is therefore supported.

New Software:

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

Evaluation may include but is not limited to the following:

- Conducting beta testing.
- Determining how the software will impact the VHCS 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.
- 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.

When staff recommends apps for the VHCS Mobile Device Management Apps 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 instructional sound, is in line with curriculum or behavioral standards, and is age appropriate.

Virus, Malware, Spyware, Phishing and SPAM Protection
Appendix G

Virus, Malware, and Spyware Protection

Vestavia Hills City Schools is entrusted with the responsibility to provide appropriate protection against malware threats, such as viruses and spyware applications. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems they cover. This policy applies to all computers that Vestavia Hills City Schools is responsible to manage. This explicitly includes any system for which Vestavia Hills City Schools has a contractual obligation to administer. This also includes all computer systems setup for internal use by Vestavia Hills City Schools, regardless of whether Vestavia Hills City Schools retains administrative obligation or not.

Anti-Virus

All computers MUST have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system.

Mail Server Anti-Virus

If the target system is a mail server it MUST have either an external or internal anti-virus scanning application that scans all mail destined to and from the mail server. Local anti-virus scanning applications MAY be disabled during backups if an external anti-virus application still scans inbound emails while the backup is being performed.

Anti-Spyware

All computers MAY have an anti-spyware application installed that offers real-time protection to the target system

Internet Filtering

Student learning using online content and social collaboration continues to increase. Vestavia Hills City Schools views Internet filtering as a way to balance safety with learning—letting good content, resources, and connections in while blocking the bad. To balance educational Internet resource and app use with student safety and network security, the Internet traffic from all devices that authenticate to the network is routed through the filter using the user's network credentials. For guest devices, users see a "pop-up screen" that requires them to login to the Internet filter with his/her network credentials or a guest login and password to gain access to the Internet. This process sets the filtering level appropriately based on the role of the user, such as, student, staff or guest, and more specifically for students, the grade level of the child. All sites that are known for malicious software, phishing, spyware, etc. are blocked.

Phishing and SPAM Protection

Virus checking systems approved by the Vestavia Hills City Schools Technology Department are deployed using a multi-layered approach (computers, servers, gateways, firewalls, filters, etc.) that ensures all electronic files are appropriately scanned. Users shall neither turn off nor disable Vestavia Hills City Schools' protection systems or install other systems.

Security Patches

To provide a stable and secure network environment for Vestavia Hills City Schools' network applications, staff, business partners, and contractors. As part of this goal, it is Vestavia Hills City Schools network policy to ensure all computer devices connected to Vestavia Hills City Schools' network have proper virus protection software, current virus definition libraries, and the most recent operating system and security patches installed.

****See Vestavia Hills City Schools Information Security Policy Handbook: Antivirus Policy pg. 3; Patch Management pg. 23***

Physical and Security Controls
Appendix H

The following physical and security controls shall be adhered to:

1. Network systems shall be installed in an access-controlled area. The area in and around the computer facility shall afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations.
2. Monitor and maintain data centers' 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%.
3. File servers and/or storage containing PII, Confidential and/or Internal Information shall be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.
4. Computers and other systems shall be secured against use by unauthorized individuals. It is the responsibility of the user to not leave these devices logged in, unattended, and open to unauthorized use.
5. Ensure network systems and network equipment are properly secured to prevent unauthorized physical access and data is properly safeguarded to protect from loss. A record shall be maintained of all personnel who have authorized access.
6. Maintain a log of all visitors granted entry into secured areas or areas containing sensitive or confidential data (e.g., data storage facilities). Record the visitor's name, organization, and the name of the person granting access. Retain visitor logs for no less than 6 months. Ensure visitors are escorted by a person with authorized access to the secured area.
7. Monitor and control the delivery and removal of all asset-tagged and/or data-storing technological equipment or systems. Maintain a record of all such items entering or exiting their assigned location using the district approved technology inventory program. No technology equipment regardless of how purchased or funded shall be moved without the explicit approval of the technology department.
8. Ensure that technological equipment or systems being removed for transfer to another organization or being designated as surplus property is appropriately sanitized in accordance with applicable policies and procedures.

See also Appendix J (Purchasing and Disposal Procedures)

Password Control Standards
Appendix I

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. Vestavia Hills City Schools' purpose is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. All personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Vestavia Hills City Schools facility, has access to the Vestavia Hills City Schools' network, or stores any non-public Vestavia Hills City Schools' information. A poorly chosen password may result in the compromise of Vestavia Hills City Schools' entire school system network. As such, all Vestavia Hills City Schools staff (including contractors and vendors with access to Vestavia Hills City Schools' systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Password Standards:

Users are responsible for complying with the following password standards for network access or access to secure information:

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the Vestavia Hills City Schools Technology Department administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every twelve months. The recommended change interval is every three months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

- Passwords shall never be shared with another person, unless the person is a designated security manager.

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least fifteen alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Do not use the same password for Vestavia Hills City Schools' accounts as for other non-VHCS access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various VHCS access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share Vestavia Hills City Schools' passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential VHCS information.

See Vestavia Hills City Schools Information Security Policy Handbook: Password Policy pg. 6

Purchasing and Disposal Procedures
Appendix J

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 Vestavia Hills City Schools' (VHCS) district Technology Department.

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

Purchasing Guidelines

All systems that will be used in conjunction with Vestavia Hills City Schools' technology resources or purchased, regardless of funding, shall be purchased from an approved list or be approved by a local school Instructional Technology Specialist and/or the district Technology Department. Failure to have the purchase approved may result in lack of technical support, request for removal from premises, or denied access to other technology resources.

Alabama Competitive Bid Laws

All 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. All technological systems, services, etc. over $15,000 purchased with public funds are subject to Alabama's competitive bid laws.

Inventory

The Technology Department and/or Instructional Technology Specialist at each school inventory all technological devices or systems. It is the responsibility of the local Instructional Technology Specialist to conduct this inventory. The district technology staff is responsible for ensuring that any network equipment, fileservers, or district systems, etc. are inventoried.

Disposal Guidelines

Equipment shall 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, Technology Department, and BOE shall approve school disposals by discard or recycle. Written documentation in the form of a spreadsheet including but not limited to the following shall be provided to the BOE two weeks prior to the next Board of Education meeting:

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

Methods of Disposal

Once equipment has been designated and approved for disposal, it shall be handled according to one of the following methods. It is the responsibility of the local school ITS and Technology Department to modify the inventory entry to reflect any in-school transfers, in-district transfers, recycles, 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, or central office discards.

Transfer/Redistribution

If the equipment has not reached the end of its estimated life, an effort shall 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.

Discard

All electronic equipment in the Vestavia Hills City Schools district shall 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 shall be wiped clean of this information prior to leaving the school district.

A district-approved vendor shall be contracted for the disposal of all technological systems/equipment. The vendor shall 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. Doing so may make Vestavia Hills City Schools and/or the employee who disposed of the equipment liable for violating environmental regulations or laws.

Required Documentation and Procedures

For purchases, transfers and redistributions, recycle, 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.

Any equipment recycled shall 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 shall 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.

Any re-usable hardware that is not essential to the function of the equipment that can be used as spare parts shall be removed: special adapter cards, memory, hard drives, zip drives, CD drives, etc.
A district-approved vendor SHALL handle all disposals that are not redistributions, transfers, or donations. Equipment shall be stored in a central location prior to pick-up. Summary forms shall be turned into district technology office and approved by the Finance Director prior to the scheduled "pick up" day. Mice, keyboards, and other small peripherals may be boxed together and shall not be listed on summary forms.

Data Access Roles and Permissions
Appendix K

Student Information Applications

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

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.

Information Now Access

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, internal discipline, and other legal liabilities.

Vestavia Hills City Schools maintain the following permission groups in Chalkable (iNow):

- Administrators (Chalkable Group)
- Alternative School
- Attendance Clerk
- Bookkeepers
- Case Manager (Exceptional Education)
- Census Clerk
- CNP Central Office
- CNP Manager
- College Counselor
- Counselor
- Data Entry Clerk
- Discipline Clerk
- District Level Access
- District Reporting Access
- District Personnel Administrators
- District Technician
- Elementary Teacher
- Enrollment Clerk
- Grad Exam Guidance Clerk
- Guidance Clerk

- Head Nurse
- Instructional Technology Specialist
- Nurse
- PE Teacher
- PST Recorder
- Registrar
- Scheduling Clerk
- School Administrator
- Secondary Teacher
- SETS Staff
- Transcript Clerk

**Complete list of Permissions available upon requests*

Vestavia Hills City Schools Technological Services and Systems Memorandum of Agreement (MOA)
Appendix L

Vestavia Hills 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 **Vestavia Hills 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:

Confidentiality Obligations Applicable to Certain VHCS Student Records. The Company hereby agrees that it shall maintain, in strict confidence and trust, all VHCS 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 VHCS Student Records during the term of the Agreement (collectively, the "Authorized Representatives") to maintain in strict confidence and trust

all VHCS Student Information. The Company shall take all reasonable steps to insure that no VHCS Student information is disclosed to any person or entity except those who (a) are Authorized Representatives of the Company performing functions for VHCS 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 VHCS student information from the Company pursuant to federal and/or Alabama law. The Company shall use VHCS 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 VHCS 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 VHCS 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 VHCS 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 VHCS of planned system changes that may impact the security of VHCS data; (g) return or destroy VHCS data that exceed specified retention schedules; (h) notify VHCS of any data storage outside the US; (i) in the event of system failure, enable immediate recovery of VHCS information to the previous business day. The Company should guarantee that VHCS data would 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 VHCS 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 VHCS student information compromised by the breach; (c) return compromised VHCS data for review; (d) provide communications on the breach to be shared with affected parties and cooperate with VHCS efforts to communicate to affected parties by providing VHCS 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 VHCS 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 VHCS 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 VHCS 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 VHCS data of any kind, failure to follow security requirements and/or failure to safeguard VHCS data. The Company's compliance with the standards of this provision is subject to verification by VHCS 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 VHCS 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 VHCS student data and/or staff data. The Company hereby acknowledges and agrees that, solely for purposes of receiving access to VHCS 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 VHCS 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 VHCS 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]

Vestavia Hills City Schools

By:_____

Resource 1: ALSDE State Monitoring Checklist

A. Data Governance and Use Policy				
ON-SITE	YES	NO N/A	Indicators	Notes
1. Has a data governance committee been established and roles and responsibilities at various levels specified?			• Dated minutes of meetings and agendas • Current list of roles and responsibilities	
2. Has the local school board adopted a data governance and use policy?			○ Copy of the adopted data governance and use policy ○ Dated minutes of meetings and agenda	
3. Does the data governance policy address physical security?			• Documented physical security measures	
4. Does the data governance policy address access controls and possible sanctions?			• Current list of controls • Employee policy with possible sanctions	
5. Does the data governance policy address data quality?			• Procedures to ensure that data are accurate, complete, timely, and relevant	
6. Does the data governance policy address data exchange and reporting?			• Policies and procedures to guide decisions about data exchange and reporting • Contracts or MOAs involving data exchange	
7. Has the data governance policy been documented and communicated in an open and accessible way to all stakeholders?			• Documented methods of distribution to include who was contacted and how • Professional development for all who have access to PII	

Resource 2: Record Disposition Requirements

The information below is form the Local Boards of Education Records Disposition Authority approved by the Local Government Records Commission, October 2, 2009. The complete document can be found at: http://www.archives.alabama.gov/officials/localrda.html.

The following sections are of special interests:

- 1.04 Administrative Correspondence
- 4.02 20-Day Average Daily Membership Reports
- 4.04 Principals Attendance Reports
- 6.01 Student Handbooks
- 6.03 Daily/Weekly Teacher Lesson Plans
- 9.14 Websites
- 10.04 Purchasing Records
- 10.05 Records of Formal Bids
- 10.06 Contracts
- 10.08 Grant Project Files

Resource 3: Email Guidelines

The purpose of these guidelines is to prevent tarnishing the public image of Vestavia Hills City Schools. When email goes out from Vestavia Hills City Schools the general public will tend to view that message as an official Policy from Vestavia Hills City Schools. These guidelines cover appropriate use of any email sent from a Vestavia Hills City Schools' email address and apply to all staff, vendors, and agents operating on behalf of Vestavia Hills City Schools.

Prohibited Use

The VHCS email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Staffs who receive any emails with this content from any VHCS staff should report the matter to their supervisor immediately.

Personal Use

Using a reasonable amount of VHCS resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a VHCS email account is prohibited. VHCS System Administrators/ITS shall approve virus or other malware warnings and mass mailings from VHCS before sending. These restrictions also apply to the forwarding of mail received by a VHCS staff.

Monitoring

VHCS staff shall have no expectation of privacy in anything they store, send or receive on the system's email system. VHCS may monitor messages without prior notice. VHCS is not obliged to monitor email messages.

Enforcement

Any staff found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.

Staff E-Mail

- Email is stored on Vestavia Hills City School System equipment and is considered property of Vestavia Schools and should not be considered a private means of communication.
- E-mail accounts are provided to staff for professional and educational purposes and should not be used for political gain, personal business, commercial activity or non-educational subscription services.

- Users should send email only to those to whom the email applies. Mass school email should be used sparingly.
- Only e-mail accounts provided by the school system for communication between teachers and students will be maintained and supported.
- E-mail is archived for two months.

Student E-Mail

- VHCS provides our students with a Gmail account through Google Apps for Education. Email is provided to our students so they can easily collaborate on documents, presentations, and spreadsheets.
- Email is restricted to teacher and student communication to protect student privacy and prevent them from being contacted by unapproved sources outside the school system. As a result, you will not be able to email your student at his or her vhcsk12.com address, nor will they be able to email you.

See Vestavia Hills City Schools Information Security Policy Handbook: Email Policy pg. 26

VESTAVIA HILLS CITY SCHOOLS
STUDENT DATA CONFIDENTIALITY AGREEMENT

I acknowledge my responsibility to respect the confidentiality of student records and to act in a professional manner in the handling of student performance data. I will ensure that confidential data, 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 student data collected by myself or 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 Vestavia Hills City Schools Student Data Confidentiality Agreement.
- Student data will only be accessed for students for whom I have a legitimate educational interest and will be used for the sole purpose of improving student achievement.
- I understand that student specific data is 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 data. I will not share any student's information from any source with another student.
- I will securely log in and out of the programs that store student specific data. I will not share my password. Any documents I create containing student specific data 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)
- Regardless of its format, I will treat all information with respect for student privacy. I will not leave student data in any form accessible or unattended, including information on a computer display.

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

Signature of Employee_____ Date_____

Job Title _____ School_____

***Name:* _____**

***Laptop Serial #:*_____**

***VHCS Asset Tag #:* _____**

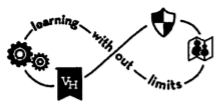
Please read the following contract and indicate your acceptance of the terms listed below by signing both copies.

1. I acknowledge receipt of the laptop computer and associated hardware. (laptop, charger, and dongle)
2. I acknowledge receipt of all the software that is installed on the laptop computer. I understand that all software obtained by Vestavia Hills City Schools through its academic licensing program is the property of the system.
3. I understand that I may not make copies of or loan the software on this laptop, nor may I install any software for which I do not have appropriate licensing. I further understand that I am responsible for any penalties incurred for the installation or use of any illegal or pirated software or files on this laptop.
4. I understand that I must immediately report loss or suspected theft of the laptop to the Vestavia Hills City Schools Technology Department and must make sure the local police are informed.
5. I understand that I am financially responsible for a lost or stolen laptop and am responsible for
all damages to this laptop that are not covered by warranty, or deemed acceptable as normal wear and tear. Our warranties do not cover spilled liquids, damage from dropping of machine, unprotected power surges, or damaged or cracked computer screens.
_____ (initial here)
6. I understand that if this laptop needs repair, I am to deliver it to the local school technology person by the next school day for authorized repair and/or service.
7. I understand that I will be identified on the Vestavia Hills City Schools Network by the address of the Network Interface Card and/or machine name and that I will be held responsible for all communications originating from that address.
8. I understand that when leaving employment with Vestavia Hills City Schools, I must return the laptop and all peripheral equipment by the last day of employment. I further understand that the laptop must be in good working order, along with all peripheral equipment, or I will be held liable for the replacement cost of each item. (laptop, charger, dongle)
9. I understand the laptop should travel in the protective case in moderate temperature environments, and it is not to be "check-in" luggage during travel.
10. I understand that the laptop must be returned on any and all school-designated check-in dates.

I have read, understand, and agree to abide by the above laptop contract.

Name (Print) _____ School _____

Signature _____Date _____



VESTAVIA HILLS CITY SCHOOLS
PUBLICATION CONSENT FORM

_____

NAME OF STUDENT (PLEASE PRINT)

_____

NAME OF PARENT/GUARDIAN (PLEASE PRINT)

The undersigned, as parent/guardian of the student named above, do hereby consent to the use of photographs, videos, or intellectual property to be used by Vestavia Hills City Schools (VHCS) in official publications and other media, for any and all publicity and art purposes.

I also hereby grant to VHCS the rights to copyright or otherwise protect any matter in which said photographs, videos, reproductions, intellectual property hereof and/or testimonial appear.

I release VHCS from any liability in connection with the use, reproduction and publication of any of the photographs, videos, or intellectual property.

Description of intellectual property:
To include but not limited to: directory information as defined in the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99); honors, awards, and special recognitions; and any classroom or extracurricular work associated with said recognitions.

_____

PARENT/GUARDIAN SIGNATURE

_____

DATE

For more details on FERPA Directory Information, visit
http://www2.ed.gov/policy/gen/guid/fpco/faq.html

Agreements of Vestavia Hills City Schools Students

Vestavia Hills City Schools' Code of Conduct

Attached is a copy of the VHCS Code of Conduct.

I confirm that my child has read, and agrees to, the VHCS Code of Conduct.

I agree ☐ Yes ☐ No

Bring Your Own Device Procedure (BYOD)

Attached is a copy of the VHCS BYOD Procedure.

I confirm that I have read, and agree to, Vestavia's BYOD Procedure.

I agree ☐ Yes ☐ No

Acceptable Use Procedure

Students will not be allowed to access school technologies until this form is completed, signed, and submitted. If you have any specific questions about this procedure, please contact a member of the school or district technology staff. The complete text of the Vestavia Hills City Schools' Acceptable Use Procedure is attached.

My child may use the internet while at school according to the VHCS Acceptable Use Procedure. ☐ Yes ☐ No

Student: I have read, understand, and agree to abide by the terms of the Vestavia Hills board of Education Acceptable Use Procedure. Should I commit any violation or in any way misuse my access to Vestavia Hills City Schools' technology, I understand and agree that my access privileges may be revoked and/or disciplinary action, according to the District Code of Conduct, may be taken.

Student agrees ☐ Yes ☐ No

Student ☐ I am 18 or older ☐ I am under 18

If I am signing this procedure, when I am under 18, I understand that when I turn 18, this procedure will continue to be in full force and effect, and I agree to abide by this procedure.

Parent/Guardian: As the parent or legal guardian of the above student, I have read, understand, and agree that my child or ward shall comply with the terms of the Vestavia Hills Board of Education Acceptable Use Procedure. I understand that access is being provided to the students for education purposes only. However, I understand that it is

impossible for the district to restrict access to all offensive and controversial materials, and further understand my child or ward's responsibility for abiding by the procedure. I am therefore signing this procedure and agree to indemnify and hold harmless the school and school district that provide the opportunity for technology access against all claims, damages, losses, and costs that may result from my child or ward's use of his or her access to technology or his or her violation of the district's acceptable use procedure.

Parent/Guardian agrees ☐ Yes ☐ No

Google Apps for Education

See the attached information on Google Apps for Education.

I confirm that I have read, and agree to, Vestavia's Procedures on Google Apps for Education. ☐ I agree

Web Publishing

Your child's school may wish to publish examples of student projects, photographs/video, or student recognition on the school/district web site, school/district television channels, and miscellaneous media coverage for television and newspaper. A student's personal information and name will not be published on the school/district web site.

My child's projects and/or videos may be used for school publications and websites.
☐ Yes ☐ No

My child's projects and/or videos may be used for non-school publications and media coverage. Non-school publications/media include but are not limited to: national and local newscasts, magazines, newspapers, etc.
☐ Yes ☐ No

Permission to Photograph

We frequently get requests from TV and newspaper reporters to videotape and/or photograph our students and their activities. Our teachers videotape and/or photograph various aspects of our student activities for instructional purposes. Also, occasionally teachers like to include photographs of classroom activities on their websites. Names, however, are not posted with the pictures. Therefore, we would like your permission to videotape and/or photograph your child if the occasion arises and possibly use the picture on the school website.

Select one:
☐ Yes, I give permission for my child to be videotaped/photographed/ included in class website postings.

☐ No, I do not give permission for my child to be videotaped/photographed/ included in class website postings.

Select one:

☐ Yes, I give permission for my child to be included in the school yearbook.

☐ No, I do not give permission for my child to be included in the school yearbook.