PELHAM
CITY SCHOOLS

Data Governance Policy

TABLE OF CONTENTS

Contents

Introduction

Pelham 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 we value the trust of our students, parents, and staff.

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

The policy formally outlines how operational and instructional activity shall be carried out to ensure Pelham City Schools' data is accurate, accessible, consistent, and protected. The document establishes who is responsible for information under various circumstances and specifies what procedures shall be used to manage and protect it.

The Pelham City Schools Data Governance Policy shall be a living document. To make the document flexible, with the Board's permission, the Data Governance Committee may quickly modify information in the Appendices in response to changing needs.

2017-2018 Data Governance Committee

The Pelham City Schools 2017-2018 Data Governance committee consists of Mr. Derrick Waddell, Technology Coordinator; Mr. Floyd Collins, Director of Operations; Ms. Holli Hicks, Director of Exceptional Education; Ms. Susan Hyatt, Federal Programs Coordinator; Ms. Kerry Barber, Counselor/District Data Manager; Ms. Amanda Wilbanks, Principal; Mr. Justin Hefner, Principal; Mr. Chase Holden, Assistant Principal; and Ms. Aisha Thorn, Counselor. All members of the Pelham City Schools Administrative Team will serve in an advisory capacity to the committee and will be called upon to attend meetings when the topic of the meeting requires his or her expertise.

Committee Meetings

The Data Governance committee will meet at a minimum once per year. Additional meetings will be called as needed.

Pelham City Schools Data Governance Policy

PURPOSE

A. It is the policy of Pelham City Schools that data or information in all its forms--written, 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 are documented and reviewed annually by the data governance committee.
C. Pelham City Schools conducts annual training on their data governance policy and documents that training.
D. The terms data and information are used separately, together, and interchangeably throughout the policy. The intent is the same.

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 applies to all forms of Pelham 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.

REGULATORY COMPLIANCE

The district will abide by any law, statutory, regulatory, or contractual obligations affecting its data systems. Pelham City Schools complies with all applicable regulatory 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. Payment Card Industry Data Security Standard (PCI DSS)
E. Protection of Pupil Rights Amendment (PPRA)

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

RISK MANAGEMENT

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

See also Appendix B (Definitions and Responsibilities)

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 C (Data Classification Levels)

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

Pelham City Schools shall be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

A. **Software Installation and Use:** All software packages that reside on technological systems within or used by Pelham City Schools shall comply with applicable licensing agreements and restrictions and shall comply with Pelham City Schools' acquisition of software procedures. *See also Appendix D (Acquisition of Software Procedures)*
B. **Virus, Malware, Spyware, Phishing and SPAM Protection:** Virus checking systems approved by the 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 not to turn off or disable Pelham City Schools' protection systems or to install other systems.
C. **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 Pelham 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:
    a. Authorization: Access will 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 Coordinator.
    b. 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 will be held accountable for all actions performed on the system with their User ID. User accounts and passwords shall NOT be shared.
    c. Data Integrity: Pelham City Schools provides safeguards so that PII, Confidential, and Internal Information is not altered or destroyed in an

unauthorized manner. Core data are backed up to multiple locations for disaster recovery.

d. 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:
    i. integrity controls and
    ii. encryption, where deemed appropriate
    iii. *See also Resource 3: Employee Technology Usage Policy Excerpts as related to Data Governance.*

e. Physical and Electronic Access and Security: Access to areas in which information processing is carried out shall be restricted to only appropriately authorized individuals. At a minimum, staff passwords shall be changed annually.
    i. No PII, Confidential and/or Internal Information shall be stored on a device itself such as a hard drive, mobile device of any kind, or external storage device that is not located within a secure area.
    ii. No technological systems that may contain information as defined above shall be disposed of or moved without adhering to the appropriate procedures.
    iii. It is the responsibility of the user to not leave these devices logged in, unattended, and open to unauthorized use.
    iv. *See also Appendix E (Physical and Security Controls Procedures.)*
    v. *See also Appendix F (Data Access Roles and Permissions.)*

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

a. 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 requests 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 Technology Coordinator 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, etc. unless the exception is approved by the data governance committee. *See also Appendix G (Pelham City Schools Memorandum of Agreement.)*

b. 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. PII that is downloaded for educational purposes where possible shall be de-identified before use.

E. **Oral Communications:** Pelham City Schools' staff 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. Pelham 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.

F. **Audit Controls:** Hardware, software, services and/or procedural mechanisms that record and examine activity in information systems that contain or use PII may be reviewed by the Data Governance Committee annually.

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

H. **IT Disaster Recovery:** Controls shall ensure that Pelham City Schools can recover from 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/or Technology Coordinator for response to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages data or systems.

COMPLIANCE

The Data Governance Policy applies to all users of Pelham 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 Pelham 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 Pelham 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:

A. Unauthorized disclosure of PII or Confidential Information.
B. Unauthorized disclosure of a log-in code (User ID and password).
C. An attempt to obtain a log-in code or password that belongs to another person.
D. An attempt to use another person's log-in code or password.
E. 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.
F. Installation or use of unlicensed software on Pelham City School technological systems.
G. The intentional unauthorized altering, destruction, or disposal of Pelham City Schools' information, data and/or systems. This includes the unauthorized removal from PCS 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.
H. An attempt 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.

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

CIPA

The Children's Internet Protection Act was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program. 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

PCI DSS

The Payment Card Industry Data Security 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. 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. For more information, see http://www2.ed.gov/policy/gen/guid/fpco/ppra/index.html

Appendix B: Definitions and Responsibilities

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, 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 Pelham 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 Pelham 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

A. Data Governance Committee: The Data Governance Committee for Pelham 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:
    a. Reviewing the Data Governance Policy annually and communicating changes in policy to all involved parties.
    b. Educating data custodians and manage owners and users with comprehensive information about security controls affecting system users and application systems.

B. User Management: Pelham City Schools' administrators are responsible for overseeing their staff use of information and systems, including:
    a. Reviewing and approving all requests for their employees' access authorizations.
    b. Initiating security change requests to keep employees' secure access current with their positions and job functions.
    c. Promptly informing appropriate parties of employee terminations and transfers, in accordance with local entity termination procedures.
    d. Revoking physical access to terminated employees, i.e., confiscating keys, changing combination locks, etc.
    e. Providing employees with the opportunity for training needed to properly use the computer systems.
    f. Reporting promptly to the Data Governance Committee the loss or misuse of Pelham City Schools' information.
    g. Initiating corrective actions when problems are identified.
    h. 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.
    i. Following all privacy and security policies and procedures.

C. User: The user is any person who has been authorized to read, enter, print or update information. A user of information is expected to:
    a. Access information only in support of their authorized job responsibilities.

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

Appendix C: Data Classification Levels

Personally Identifiable Information (PII)

A. PII is information about an individual maintained by an agency, including:
    a. 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.
    b. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
B. 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 Pelham City Schools.

Confidential Information

A. 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, proprietary information of commercial research sponsors, system access passwords and information file encryption keys.
B. Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for Pelham 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

A. Internal Information is intended for unrestricted use within Pelham City Schools, and in some cases within affiliated organizations such as Pelham City Schools' business or community partners. This type of information is already widely-distributed within Pelham 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.

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

Public Information

A. Public Information has been specifically approved for public release by a designated authority within each entity of Pelham City Schools. Examples of Public Information may include marketing brochures and material posted to Pelham City Schools' web pages.
B. This information may be disclosed outside of Pelham City Schools.

Directory Information

Pelham City Schools defines Directory information as follows:

A. Student name
B. Student gender
C. Student address
D. Student telephone listing
E. Student email listing
F. Student photograph
G. Student place and date of birth
H. Student dates of attendance (years)
I. Student grade level
J. Student diplomas, honors, awards received
K. Student participation in school activities or school sports
L. Student weight and height for members of school athletic teams
M. Student most recent institution/school attended
N. Student ID number, not to include student State ID number

Appendix D: Acquisition of Software Procedures

The purpose of the Acquisition of Software Procedures

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

Software Licensing

A. All district software licenses owned by PCS will be:
    a. accurate, up to date, and adequate, and
    b. in compliance with all copyright laws and regulations
B. All other software licenses owned by departments or local schools will be:
    a. accurate, up to date, and adequate, and
    b. in compliance with all copyright laws and regulations
C. Software installed on PCS technological systems and other electronic devices:
    a. will have proper licensing on record,
    b. will be properly licensed or removed from the system or device, and
    c. will be the responsibility of each PCS employee purchasing and installing to ensure proper licensing
D. Unless otherwise approved by the Data Governance Committee, 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:
    a. PCS student and/or staff data will not be shared, sold, or mined with or by a third party,
    b. PCS student and/or staff data will not be stored on servers outside the US unless otherwise approved by Pelham City Schools' Data Governance Committee,
    c. the company will comply with PCS guidelines for data transfer or destruction when contractual agreement is terminated, and

E. 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 purchases shall be approved by the district technology director or designee such as a local school technology coordinator or member of the technology staff.

A. A list of supported software will be maintained on the PCS District Technology site.
B. It is the responsibility of the PCS Technology Team members to keep the list current and for staff to submit apps or other software to the Technology Team.
C. Unsupported software shall be approved or it will not be allowed on PCS owned devices.
D. When staff recommends submits a Software Request Form, 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.
E. Software that accompanies adopted instructional materials must be vetted by the Curriculum and Instruction Director and the Technology Coordinator before being 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 PCS technology environment and the functionality of the software for the specific discipline or service it will perform.

A. Evaluation may include but is not limited to the following:
    a. Conducting beta testing.

b. Determining how the software will impact the PCS technology environment such as storage, bandwidth, etc.
c. Determining hardware requirements.
d. Determining what additional hardware is required to support a particular software package.
e. Outlining the license requirements/structure, number of licenses needed, and renewals.
f. Determining any Maintenance Agreements including cost.
g. Determining how the software is updated and maintained by the vendor.
h. Determining funding for the initial purchase and continued licenses and maintenance.

Appendix E: Physical and Security Controls

The following physical and security controls shall be adhered to:

A. 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.
B. 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.
C. 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.
D. 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.
E. 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.
F. 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.
G. 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.

Appendix F: Data Access Roles and Permissions

Pelham City Schools maintain the following permission groups in INOW:

A. Administrators
B. Administrator Scheduling
C. Assistant Principal
D. Athletic Directors
E. Attendance Clerk
F. Case Managers
G. Central Office Administrators
H. Central Office Student View
I. Central Office View Only
J. Counselors
K. Data Managers
L. Elementary Teacher
M. Enrollment Clerk
N. Grade Reports
O. INOW Administrator
P. Instructional Coaches
Q. Nurse
R. PHS Attendance Clerk
S. Physical Fitness Testing
T. Principal
U. Secondary Teacher
V. SETS Staff
W. Student Lookup
X. System Nurse
Y. Vocational Teacher

Appendix G: Pelham City Schools 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 PELHAM CITY SCHOOLS (PCS), 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 PCS Student Records</u>

The Company hereby agrees that it shall maintain, in strict confidence and trust, all PCS student records containing personally identifiable information (PII) hereafter

referred to as "Student Information". Student information shall 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 PCS Student Records during the term of the Agreement (collectively, the "Authorized Representatives") to maintain in strict confidence and trust all PCS Student Information. The Company shall take all reasonable steps to insure that no PCS Student information is disclosed to any person or entity except those who (a) are Authorized Representatives of the Company performing functions for PCS under the Agreement and have agreed to be bound by the terms of this Agreement; (b) are authorized representatives of PCS, or (c) are entitled to such PCS student information from the Company pursuant to federal and/or Alabama law. The Company shall use PCS 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 PCS 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 PCS student information.

<u>Other Security Requirements</u>

The Company shall maintain all technologies, policies, procedures and practices necessary to secure and protect the confidentiality and integrity of PCS 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 PCS of planned system changes that may impact the security of PCS data; (g) return or destroy PCS data that exceed specified retention schedules; (h) notify PCS of any data storage outside the US; (i) in the event of

system failure, enable immediate recovery of PCS information to the previous business day. The Company should guarantee that PCS data shall 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 PCS 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 PCS student information compromised by the breach; (c) return compromised PCS data for review; (d) provide communications on the breach to be shared with affected parties and cooperate with PCS efforts to communicate to affected parties by providing PCS 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 PCS 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 PCS 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 PCS 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 PCS data of any kind, failure to follow security requirements and/or failure to safeguard PCS data. The Company's compliance with the standards of this provision is subject to verification by PCS personnel or its agent at any time during the term of the Agreement. Said information should only be used for the purposes intended and shall 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 PCS 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 PCS student data and/or staff data. The Company hereby acknowledges and agrees that, solely for purposes of receiving access to PCS 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 PCS 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 PCS 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.

Resource 1: ALSDE State Monitoring Checklist

1. Has a data governance committee been established and roles and responsibilities at various levels specified?

2. Has the local school board adopted a data governance and use policy?

3. Does the data governance policy address physical security?

4. Does the data governance policy address access controls and possible sanctions?

5. Does the data governance policy address data quality?

6. Does the data governance policy address data exchange and reporting?

7. Has the data governance policy been documented and communicated in an open and accessible way to all stakeholders?

Resource 2: Record Disposition Requirements

The information below is from 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: Employees' Acceptable Use Practices (AUP) for the Use of Technology (also found in Employee Handbook)

Excerpts as related to Data Governance

General Rules

Passwords

Employees will be held responsible for activity on their account. Therefore, employees should:

- Create 'strong' passwords, keep them secure, and change them annually or more frequently.
- Use different passwords for the District's Student Information System, INOW, and general network use.
- Use only their authorized network account. (Unauthorized attempts to login as any other individual are prohibited.)
- Not give students their login credential or allow students to use technology that has been logged into by a staff account.
- Close programs and lock or log out of devices when they will be unattended even for a short time.

Equipment

Employees shall not:

- Intentionally harm, destroy, disable, or remove parts from any District technology. Employees may be held financially responsible for the repair, replacement, or reconfiguration of affected equipment.
- Employees shall not modify computer hardware in any way without the permission of school administrators.
- Invite or allow outside individuals to repair or modify District technology without first obtaining permission from the Technology Department.
- Move or dispose of District equipment without following proper equipment transfer procedures.
- Remove equipment from their building without first completing the appropriate permission form.

- Bring in, buy, or use Wireless Access Points or network switches which have not been specifically approved of by the Technology Department for use on the District's network.
- Use personal equipment or accounts to provide students with unfiltered Internet access.

Use

Employees shall not:

- Attempt to disable or circumvent security measures, including Internet filtering software.
- Use technology for non-educational, commercial, political, or "for-profit" purposes.
- Use technology for antisocial behaviors such as harassment and discriminatory remarks, etc.
- Intentionally view, seek, obtain, or modify information, other data, or passwords belonging to other users.
- Install unlicensed software onto any District device.

Internet Filtering and Access

Expectations of Privacy

All technology resources, including but not limited to, network and Internet resources, accounts, electronic systems, computers or other devices owned, leased, or maintained by the Board are the sole property of the Board. Authorized Board personnel may, at any time and without prior notice, access, search, examine, inspect, collect, or retrieve information of any kind from the Board's technology resources, including computer or related equipment, files, and data to determine if a user is in violation of any of the Board's policies, rules, and regulations regarding access to and use of technology resources, for or in connection with any other matter or reason related to the safe and efficient operation, maintenance, or administration of the school system, or for any other reason not prohibited by law. Users of school system technology resources have no personal right of privacy or confidentiality with respect to the use or content of such resources. In addition, school officials may read, examine, or inspect the contents of any personally-owned technology devices upon

reasonable suspicion that the contents or recent utilization of the device contains evidence of a violation of Board Policy, the Code of Conduct, Acceptable Use Practices, or other school or system rules or regulations. The Board of Education will cooperate with any properly executed request from any local, State, or Federal law enforcement agency or civil court.

Access to the Internet

It is the policy of the Board to provide its employees and students with Internet access for the purpose of supporting activities that serve, and are consistent with, the identified educational and administrative objectives of the District.

Filtering

The District filters Internet access in order to comply with Federal rules and to ensure that staff and students are protected from harmful and inappropriate material. However, no technology protection measure will be 100% effective. Therefore, all users should report any sites which contain inappropriate materials or materials harmful to minors to the Technology Coordinator or his/her designee. The District will not be responsible for any damage suffered by the user due to a technical failure to block or filter inappropriate Internet sites or electronic communications.

- Teachers should pre-screen websites before showing to their class to ensure suitability.
- Teachers should supervise and monitor their student's use of Internet and/or electronic communications in order to assist in ensuring that their use is consistent with all rules, regulations, and protection measures.
- Teachers should not permit students to set up 'hotspots' using their personal devices in order to provide other students with unfiltered Internet access.
- Teachers should know which of their students have a letter on file from the parent disallowing them from using the Internet independently and enforce these restrictions.

Data Plans and Filtering

- Employees may not purchase data plans which would provide students with unfiltered Internet access with 'school' funds (i.e., local school funds, District, Federal, or donated funds passing through system accounts).

- Employees may not 'tether' a device to District technology on a District campus in order to bypass the District's Internet filter.

Requests for Opening up Filtered Sites

Employees may request a review of filtered sites. They may also request a temporary release of specific sites at specific workstations to complete their work. Such requests should take place following established technology procedures. [1Pub. L. No. 106-554 and 47 USC 254(h)]

FERPA and Technology

The use of technology can greatly increase the exposure of protected information whether via email, websites, or use of various software programs. Employees are expected to understand and comply with the provisions of Federal Family Education Rights Protection Act, which requires that schools provide and protect information regarding its students. Employees should take extra precautions when using technology to transmit any protected information in order to be sure it will only reach the appropriate recipients. Employees may be asked to sign Security Agreements that further define rules regarding protecting data.

Online Media Publications

Teachers should familiarize themselves with the Media Release provisions of the Student Code of Conduct. This portion of the Code of Conduct refers to a wide range of media, both in print and online formats on the District's own website.

Anti-Virus, Phishing, and other Forms of Cyber Attacks

Everyone must do his/her part to prevent the district's devices and network from being infiltrated and damaged by various forms of malicious behavior. Employees should:

- Not disable the antivirus software on District technology.
- Never respond to emails claiming that they need you to update your email account or password. The Technology Department will NEVER ask you to do this. Delete these emails or forward them to spam@pelhamcityschools.org. NEVER click on links within these emails whether from home computers or work computers.
- Make sure that laptops which are taken off site or used infrequently are connected to the network periodically so that the antivirus software can be updated.

Rules for Email and Electronic Communications

Electronic communications, in its many forms, can be a very efficient and effective method of communicating with others; however, it has many inherent risks. Once sent or posted, the author no longer has control over the information contained in the message or posting. The purpose of this Acknowledgement is to make Board employees and others granted network accounts aware of certain risks and responsibilities that accompany using electronic communications provided by Pelham City Schools.

This Acknowledgement provides guidance on the professional, ethical, legal, and responsible use of System electronic communications (Email, website, etc.). This document does not constitute all rules or procedures concerning electronic communications. This Acknowledgement applies to all full-time employees, part-time employees, contracted employees, temporary employees, and others acting on behalf of Pelham City Schools. It applies to any person or group of persons who have email accounts, and also to those who request that an account holder send a message on their behalf. It is applicable to all electronic communications regardless of the physical location (school, office, home, or any other offsite location) of the user.

Prohibited Use

The Pelham City Schools' electronic communications programs shall not be used for the creation or distribution of any content that:

- Discloses unauthorized or restricted information to inside or outside parties via electronic communications, including restricted or confidential information that would violate the privacy of individuals or violate any other local, state, or federal laws including, but not limited to FERPA and HIPAA.
- Contains private information such as student grades, discipline incidents, suspensions, social security numbers, special education status, or Individualized Education Plans in cases where it would violate FERPA.
- Discloses personal information regarding students, faculty, staff, or parents to third parties.
- Contains information that pertains to someone other than the addressee (For instance, do not address Emails to numerous individuals that contains private information that does not apply to all of the recipients).
- Defames, slanders, or libels another person or organization.

- Contains or links to pornography or other content inappropriate for K-12.
- Contains content that may be considered offensive or discriminatory, because of a person's race, sex, hair color, disabilities, age, sexual orientation, religious beliefs and practice, political beliefs, or national origin.
- Contains content or files that violate any copyright or trademark law. Users should be aware that passing on emails that contain copyrighted or trademarked material may have legal consequences even though they were not the original sender.
- Intentionally contains malicious or harmful software such as computer viruses and spyware.
- Contains fraudulent, harassing, or intimidating content.
- Violates any license governing use of software.
- Is intended for personal or private financial gain.
- In addition, should employees receive electronic communications that contain such information, they should not forward such messages to others, whether inside or outside the System.

Teacher Web Publishing Requirements

Identification of Students

The following restrictions have been established in order to protect students and comply with their parent's wishes. School administrators should put procedures in place to notify teachers when a parent has provided the school with a letter prohibiting the school/teacher from publishing their child's name, picture, information or work on the school or teacher website. Per the Student Code of Conduct, the parent has ten (10) days from the student's first day of attendance to provide the school with notice. Therefore, teachers should be cautious in posting student information during the first few weeks of school.

- Only use the student's first name and initial of last name (JaneD) when referring to or identifying students on the web. Note that provisions for official online school newspapers may be different.
- Never post a student's last name, home address, email address, phone number, student number, or social security number online.
- Do not use or upload files which use the student's name in the file name (e.g. maryjones.gif, jdoe_as_hamlet.html).

- Teach students not to post their own full name or contact information to the website when contributing content. Remove such information if it is included prior to approving the comment to become public.

Student Data and Grades

- Never post student attendance, grades, or discipline to teacher websites. INOW Home Portal is the appropriate place for students and their parents to view this information because access is password restricted to those individuals.
- Do not post examples of student work which includes grades or corrections unless the example is completely fictitious. This includes student work from prior years.
- Public comments by teachers on student work should provide general feedback and guidance, not grades or scores.

Resource 4: Agreements for Contract Employees

Including Long Term Substitutes

Procedure:

A. All contract employees should complete the following prior to gaining access to the Pelham City Network, INOW, and SETS (if applicable):
    a. Complete the Third Party Account Request Form, read and sign to acknowledge the Technology Usage Practices.
    b. Read and sign the Pelham City Schools Student Data Confidentiality Agreement
B. Once the above has been completed and forms reviewed, if all requirements are met, the new email account will be enabled.
C. Account will be when Technology Department receives the Third Party Account Request Form for the contracted employee.