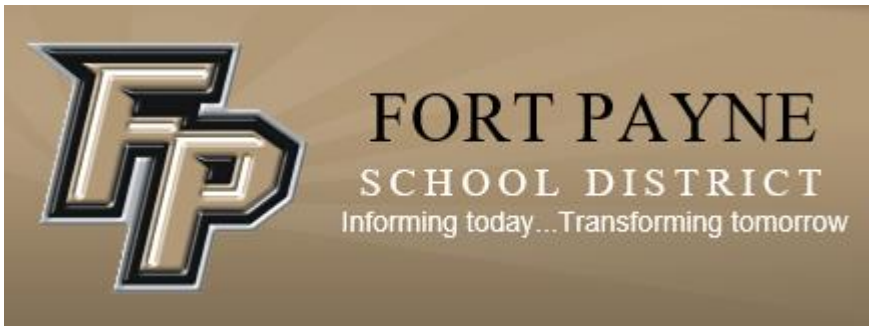


Fort Payne City Schools

Data Governance/Employee Acceptable Use Policy

TABLE OF CONTENTS

Introduction

Protecting the privacy of students and staff is an important priority, and Fort Payne 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 Fort Payne City Schools Data Governance/Employee AUP document includes information regarding the Data Governance Committee, the actual Fort Payne City Schools Data and Information Governance and the Employee Acceptable Use Policy, applicable Appendices, and Supplemental Resources.

The policy formally outlines the means by which operational and instructional activity shall be carried out to ensure Fort Payne 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.

Committee Meetings

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

Fort Payne City Schools Data Governance/Employee AUP Policy

I. PURPOSE/OVERVIEW

A. It is the policy of Fort Payne City Schools that data or information 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. All policies and procedures must be documented and made available to individuals responsible for their implementation and compliance. All activities identified by the policies and procedures must also be documented. Documentation must be retained for at least six (6) years after initial creation, or after changes are made. The data governance policies and procedures are documented and reviewed annually by the Data Governance Committee.

C. Fort Payne City Schools conducts annual training on its Data Governance/Employee AUP 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 Fort Payne 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.;

E. Data stored on any type of internal, external, or removable media or cloud based services.

III. REGULATORY COMPLIANCE

The district shall abide by any law, statutory, regulatory, or contractual obligations affecting its data systems, acts including, but not limited to, the following:

A. Children's Internet Protection Act (CIPA) http://www.fcc.gov/guides/childrens-internet-protection-act

B. Children's Online Privacy Protection Act (COPPA) www.coppa.org

C. Family Educational Rights and Privacy Act (FERPA)
http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

D. Health Insurance Portability and Accountability Act (HIPAA)
http://www.hhs.gov/ocr/privacy/hipaa/understanding/

E. Payment Card Industry Data Security Standard (PCI DSS) www.pcisecuritystandards.org

F. Protection of Pupil Rights Amendment (PPRA)
http://www2.ed.gov/policy/gen/guid/fpco/ppra/index.html

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

IV. RISK MANAGEMENT

The analysis involved in Fort Payne 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.

**** See also Appendix B (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 C (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 Fort Payne City Schools and therefore shall be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

A. **Ownership of Software:** All computer software developed by Fort Payne City Schools employees or contract personnel on behalf of Fort Payne City Schools, licensed or purchased for Fort Payne City Schools use is the property of Fort Payne City Schools and shall not be copied for use at home or at any other location, unless otherwise specified by the license agreement.
B. **Software Installation and Use:** All software packages that reside on technological systems within or used by Fort Payne City Schools shall comply with applicable licensing agreements and restrictions and shall comply with Fort Payne City Schools' acquisition of software procedures.

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

C. **Copyright Laws:** Fort Payne City Schools' employees will not download and/or install software or digital media without obtaining proper licensing. Fort Payne City Schools' employees will strictly adhere to copyright laws, including Fair Use Guidelines (http://www.copyright.gov/fls/fl102.html.) This is regardless if we are dealing with digital copyright or physical material copyright. It is the employee's responsibility to obtain any necessary written permission granting the authority to publish any copyrighted materials, including but not limited to photographs, images, cartoons, logos, digital sound, and music files. Fort Payne City Schools' employees will not plagiarize information received in any form.
D. **Employee Files:** Fort Payne City Schools' employees should be aware that all files on Fort Payne City Schools' equipment, which includes but is not limited to: servers, computers, mobile devices and even personal files, are the property of the Fort Payne City School System. Fort Payne City Schools' employees should have no expectation of privacy in anything created, stored, sent, or received on Fort Payne City Schools' equipment. Fort Payne City Schools' employees' files can be monitored without prior notification if the administration of The Fort Payne City School System deems this necessary.
E. **Email Usage:** Fort Payne City Schools' employees will not send or forward emails containing libelous, defamatory, offensive, racist, or obscene remarks, cartoons, pictures, etc. Fort Payne City Schools' employees will not send unsolicited or chain mail. Fort Payne City Schools' employees will not send messages under a false identity. Fort Payne City Schools' employees will not access email of other users. Fort Payne City Schools' employees must take the same care in drafting email as they would for any other communication. Fort Payne City Schools' employees should be aware that although the email system is meant for business use, rare and infrequent personal usage is allowable if it is reasonable and does not interfere with work. Fort Payne City Schools' employees are advised to keep personal emails

on personal email accounts. Regardless personal usage email should be restricted to planning and non-instructional time unless there is an emergency. Employees should be aware that all messages distributed via the Fort Payne City School System's email system, even personal emails, are the property of the Fort Payne City School System. Employees should have no expectation of privacy in anything created, stored, sent, or received on the Fort Payne City School System's email system. Fort Payne City Schools' employees' email can be monitored without prior notification if the administration of the Fort Payne City School System deems this necessary.

F. Social Networking/Communication: Social networking is an online technology tool that allows for prompt communication of information and resources**.** Fort Payne City Schools' employees shall only use approved social networking sites, websites, and other communication tools that are on the "FPCS Approved Websites/Apps List." All sites used shall be linked from Fort Payne City Schools' website to safeguard student privacy under CIPA, COPPA, and FERPA laws, as well as Fort Payne City Schools' property, reputation, and integrity. These tools can include, but are not limited to, text, audio, video, images, blogs, podcasts, Twitter, Facebook, Instagram, etc. Linking personal sites or advertising personal sites from school approved sites is not allowed. Using the school name on personal sites is not allowed. Personal sites should not be created using school email. Communication between teachers to students and parents should occur using school approved communication tools only. Fort Payne 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.

G. Mobile Devices Issued to Employees: Fort Payne City Schools' employees that are issued a mobile device (laptop, iPad, Chromebook, and etc.) will receive the mobile device and needed accessories. It is the Fort Payne City Schools' employee's responsibility to care for the equipment and ensure that it is retained in a safe environment. Fort Payne City Schools' employees should treat the mobile device with care by not dropping it, getting it wet, leaving it outdoors, leaving it unattended, or using it with food or drink. Fort Payne City Schools' employees should keep the mobile device locked with a passcode or password to keep sensitive information safe and to protect the mobile device from unauthorized use. Fort Payne City Schools' employees should not lend the mobile device to others unless authorized by Fort Payne City Schools' administration to do so. Fort Payne City Schools' employees should not attempt any physical repairs to the mobile device. Fort Payne City Schools' employees must return the mobile device to Fort Payne City Schools if their employment is ended. The mobile device may not be defaced in any way which includes stickers. Inappropriate use or care of the mobile device may result in the Fort Payne City Schools' employee losing their right to use the mobile device. If a case is supplied with the mobile device, it must be kept on the mobile device. It cannot be replaced with an alternate case. The mobile device is Fort Payne City School's property and may be requested to be turned over to school administration which includes the local school administration or central office administration at any time. Fort Payne City Schools' employees agree to make no attempts to change or allow others to change the setup or configuration of the mobile device that will interfere with the proper function and use of the mobile device. The mobile device should be charged regularly and be ready for use each school day. If stolen the Fort Payne City Schools' employee should report the theft to school officials and the police as soon as possible.

H. Illegal Activities: Fort Payne City Schools' employees will not use Fort Payne City Schools' technology, networks, and/or systems for illegal purposes or any other activity prohibited by Fort Payne City Schools' policy. Fort Payne City Schools' employees will not download and/or install illegal or illegally obtained software or personally owned software.

I. Respect for System Limitations: Fort Payne City Schools' employees will not download programs that will potentially degrade the performance of the Internet and/or network without obtaining prior permission from the Fort Payne City Schools' Network system administrator and/or his designee. (Programs like Weather Bug, Kazaa, and etc.)

J. Safety of Self and Others: Fort Payne City Schools' employees will report to their supervisor/administrator any message received that is inappropriate or makes them feel uncomfortable. Fort Payne City Schools' employees will follow appropriate etiquette for both the Fort Payne City Schools' network and the Internet to include but not limited to the following: Will not use the system to harm the reputation, harass, or threaten others. Will use appropriate language for the educational environment and for the educational activity in which they are currently involved (no swearing, vulgarity, ethnic or racial slurs, or any other inflammatory or threatening language).

K. System Security: Fort Payne City Schools' employees will not leave their computer/device logged on and unattended. For Payne City Schools employees will not attempt to harm, vandalize, or destroy equipment, data or materials. Fort Payne City Schools' employees will not intentionally infect a computer or network with a virus. Fort Payne City Schools' employees will not engage in activities that disrupt the performance of the network. Fort Payne City Schools' employees will not disclose passwords, except to authorized Fort Payne City Schools' administrative personnel. Fort Payne City Schools' employees will always report any known violations to a supervisor/administrator. Fort Payne City Schools' employees will not gain unauthorized access to system passwords in an attempt to obtain resources and information. Fort Payne City Schools' employees will not attempt to circumvent Fort Payne City Schools' network security, including but not limited to hackware, freeware, and unauthorized shareware.

L. 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 neither turn off nor disable Fort Payne City Schools' protection systems or install other systems.

See also Appendix E (Virus, Malware, Spyware, Phishing and Spam Protection)

M. 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 Fort Payne 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:

1. **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 Accountability Coordinator and/or Technology Coordinator. 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.

a. Role-based access: Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.
b. User-based access: A security mechanism used to grant users of a system access based upon the identity of the user.

2. **Identification/Authentication:** Unique user identification (user ID) and authentication 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**.
   a. At least one of the following authentication methods must be implemented:
      1. **strictly** controlled passwords
      2. biometric identification, and/or
      3. tokens in conjunction with a PIN.
      4. Smart Cards or other physical devices programmed to contain authentication information
   b. The user must secure his/her authentication control (e.g., password, token) such that it is known only to that user and possibly a designated security manager.
   c. An automatic timeout re-authentication must be required after a certain period of no activity (maximum 60 minutes).

3. **Data Integrity:** Fort Payne 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. 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

4. **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

5. **Remote Access:** Access into Fort Payne City Schools' internal network from outside is allowed using the Fort Payne City VPN service. All other network access options are strictly prohibited without explicit authorization from the Technology Coordinator, Accountability Coordinator, 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 Fort Payne City Schools' network. PII shall only be stored in cloud storage if said storage has been approved by the Data Governance Committee or its designees.

6. **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 an external hard drive, mobile device of any kind, or external storage device that is not located within a secure area. It is the responsibility of the user that these devices not be left logged in, unattended, and open to unauthorized use.
   - 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.

7. **Employee Responsibilities:** Fort Payne City School employee responsibilities include but are not limited to the following:
   - Fort Payne City Schools' employees must sign a Data Governance/Employee Acceptable Use Policy annually.
   - Fort Payne City Schools' employees will use the Internet/network for work-related uses, but some limited personal use is permitted as long as the use does not interfere with the Fort Payne City Schools' employee's job responsibilities nor imposes cost on the district and are restricted to planning or non-instructional time unless there is an emergency.
   - Fort Payne City Schools' employees will not access files and/or documents of other users without permission
   - Fort Payne City Schools' employees will not harass or bully others as defined in the Fort Payne City Schools policies on harassment and bullying.
   - Fort Payne City Schools' employees will not use the school network and or property for financial gain or for political or commercial activity.
   - Fort Payne City Schools' employees will not attempt to access inappropriate content (obscene, offensive, etc.) including but not limited to images, videos, and text that contain inappropriate material for any purposes.

See also Appendix F (Physical and Security Controls Procedures.)
See also Appendix G (Password Control Standards.)
See also Appendix H (Purchasing and Disposal Procedures.)

N. Data Transfer/Exchange/Printing:

1. **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 Accountability Coordinator, and 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, unless the exception is approved by the Data Governance Committee.

See also Appendix I (Fort Payne City Schools Memorandum of Agreement.)

2. **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.

O. Oral Communications: Fort Payne 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. Fort Payne 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, sporting events, restaurants, or on public transportation.

P. Evaluation: Fort Payne 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.

VII. COMPLIANCE

A. The Data Governance Policy applies to all users of Fort Payne City Schools' information including: employees, staff, 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 Fort Payne City Schools' procedures, or, in the case of outside affiliates, termination of the affiliation. Further, penalties associated with state and federal laws may apply.

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

1. Unauthorized disclosure of PII or Confidential Information.
2. Unauthorized disclosure of a log-in code (User ID and password).
3. An attempt to obtain a log-in code or password that belongs to another person.
4. An attempt to use another person's log-in code or password.

5. 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.
6. Installation or use of unlicensed software on Fort Payne City Schools' technological systems.
7. The intentional unauthorized altering, destruction, or disposal of Fort Payne City Schools information, data and/or systems. This includes the unauthorized removal from Fort Payne 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.
8. 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.

Laws, Statutory, Regulatory, and Contractual Security Requirements

Appendix A

A. CIPA: The **Children's Internet Protection Act** was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program. Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies 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

B. 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.

C. 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

D. 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.

E. 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

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

These rights include 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) –

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

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

1. Any other protected information survey, regardless of funding;
2. Any non-emergency, invasive physical examination 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 examination or screening permitted or required under State law; and
3. 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

Definitions and Responsibilities
Appendix B

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 acquired regarding 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) in Fort Payne 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 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, or 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 Fort Payne City Schools is responsible for working with the Technology Coordinator to ensure security policies, procedures, and standards are in place and adhered to by the entity. Other responsibilities include:

1. Reviewing the Data Governance Policy annually and communicating changes in policy to all involved parties.
2. Educating data custodians and manage owners and users with comprehensive information about security controls affecting system users and application systems.

B. Technology Coordinator: The Technology Coordinator for Fort Payne City Schools is responsible for working with the Superintendent, Data Governance Committee, user management, owners, data custodians, and users to develop and implement prudent security policies, procedures, and controls. Specific responsibilities include:

1. Providing basic security support for all systems and users.
2. Advising owners in the identification and classification of technology and data-related resources. ****See also Appendix D (Data Classification Levels.)***
3. Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design through testing and production implementation.
4. Performing or overseeing security audits.

5. Reporting regularly to the Superintendent and Fort Payne City Schools Data Governance Committee on Fort Payne City Schools' status with regard to information security.

C. User Management: Fort Payne City Schools' administrators are responsible for overseeing their staff use of information and systems, including:

1. Reviewing and approving all requests for their employees' access authorizations.
2. Initiating security change requests to keep employees' secure access current with their positions and job functions.
3. Promptly informing appropriate parties of employee terminations and transfers, in accordance with local entity termination procedures.
4. Revoking physical access to terminated employees, i.e., confiscating keys, changing combination locks, etc.
5. Providing employees with the opportunity for training needed to properly use the computer systems.
6. Reporting promptly to the Accountability Coordinator, Technology Coordinator, and the Data Governance Committee the loss or misuse of Fort Payne City Schools Fort Payne City Schools' information.
7. Initiating corrective actions when problems are identified.
8. 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.
9. Following all privacy and security policies and procedures.

D. 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, as ownership may be shared. The owner of information has the responsibility for:

1. Knowing the information for which she/he is responsible.
2. Determining a data retention period for the information, relying on ALSDE guidelines, industry standards, Data Governance Committee guidelines, or advice from the school district attorney.
3. Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created.
4. Authorizing access and assigning data custodianship if applicable.
5. Specifying controls and communicating the control requirements to the data custodian and users of the information.
6. Reporting promptly to the Accountability Coordinator and/or Technology Coordinator the loss or misuse of Fort Payne City Schools' data.
7. Initiating corrective actions when problems are identified.
8. Promoting employee education and awareness by utilizing programs approved by the Accountability Coordinator and/or Technology Coordinator, where appropriate.
9. 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.

E. Data Custodian: The data custodian is assigned by an administrator, data owner, or the Accountability Coordinator and/or the Technology Coordinator 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:

1. Providing and/or recommending physical safeguards.
2. Providing and/or recommending procedural safeguards.
3. Administering access to information. Releasing information as authorized by the Information Owner and/or Accountability Coordinator, Technology Coordinator and/or Data Governance Committee for use and disclosure utilizing procedures that protect the privacy of the information.
4. Maintaining information security policies, procedures, and standards as appropriate and in consultation with the Accountability Coordinator, Technology Coordinator, and/or Data Governance Committee.
5. Promoting employee education and awareness by utilizing programs approved by the Accountability Coordinator and/or the Technology Coordinator, where appropriate.
6. Reporting promptly to the Accountability Coordinator and/or the Technology Coordinator and/or Data Governance Committee the loss or misuse of Fort Payne City Schools data.
7. Identifying and responding to security incidents and initiating appropriate actions when problems are identified.

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

1. Access information only in support of his/her authorized job responsibilities.
2. Comply with all data security procedures and guidelines in the Fort Payne City Schools Data Governance Policy and all controls established by the data owner and/or data custodian.
3. Keep personal authentication devices (e.g. passwords, secure cards, PINs, access codes, etc.) confidential.
4. Report promptly to the Accountability Coordinator, and/or the Technology Coordinator, and/or Data Governance Committee the loss or misuse of Fort Payne City Schools' information.
5. Follow corrective actions when problems are identified.

Data Classification Levels

Appendix C

A. Personally Identifiable Information (PII)

1. 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.
2. 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 Fort Payne City Schools.

B. Confidential Information

1. 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.
2. Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for Fort Payne City Schools, its staff, parents, students and others, 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.

C. Internal Information

1. Internal Information is intended for unrestricted use within Fort Payne City Schools, and in some cases within affiliated organizations such as Fort Payne City Schools’ business or community partners. This type of information is already widely distributed within Fort Payne 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, and most internal electronic mail messages.
2. Any information not explicitly classified as PII, Confidential or Public will, by default, be classified as Internal Information.
3. Unauthorized disclosure of this information to outsiders may not be appropriate because of legal or contractual provisions.

D. Public Information

A. Public Information has been specifically approved for public release by a designated authority within each entity of Fort Payne City Schools. Examples of Public Information may include marketing brochures and material posted to Fort Payne City Schools’ web pages.

B. This information may be disclosed outside of Fort Payne City Schools.

E. Directory Information

Fort Payne 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/video
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/User ID
15. Student Work Samples
16. Student Major Field of Study

Acquisition of Software Procedures
Appendix D

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 Fort Payne City Schools (Fort Payne City) as a whole; and
- Minimize the malicious code that can be inadvertently downloaded.

A. Software Licensing:

1. All district software licenses owned by Fort Payne City shall be:
    - kept on file at the central office;
    - accurate, up to date, and adequate; and
    - in compliance with all copyright laws and regulations.
2. All other software licenses owned by departments or local schools will be:
    - kept on file with the department or local school technology office;
    - accurate, up to date, and adequate; and
    - in compliance with all copyright laws and regulations.
3. Software installed on Fort Payne City 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 Fort Payne City employee purchasing and installing to ensure proper licensing
4. Purchased software accessed from and storing data in a cloud environment shall have a Memorandum of Agreement (MOA) on file that states or confirms at a minimum that:
    - Fort Payne City student and/or staff data will not be shared, sold, or mined with or by a third party,
    - Fort Payne City student and/or staff data will not be stored on servers outside the U.S. unless otherwise approved by Fort Payne City Schools' Data Governance Committee,
    - The company will comply with Fort Payne City guidelines for data transfer or destruction when contractual agreement is terminated, and
    - No API will be implemented without full consent of Fort Payne City and the ALSDE.

5. 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 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.

B. Supported Software:

In an attempt to prevent software containing malware, viruses, or other security risk, software is categorized as Supported and Non-Supported Software. For software to be classified as Supported Software downloads and/or purchases shall be approved by the district Technology Coordinator or his designee, such as a local school technology coordinator or member of the technical staff.

1. Unsupported software is considered New Software and shall be approved or it will not be allowed on Fort Payne City-owned devices.
2. When staff recommends apps for the Fort Payne City Mobile Device Management Apps Catalog or software for installation, it is assumed that the staff has properly vetted the app or software and that it is instructionally sound, is in line with curriculum or behavioral standards, and is age appropriate.
3. Software that accompanies adopted instructional materials shall be vetted by the Textbook Coordinator and the Technology Coordinator or his designee and is thereby supported.

C. New Software:

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

1. Evaluation may include, but is not limited to, the following:
    - Conducting beta testing.
    - Determining how the software will impact the Fort Payne City technology environment such as storage, bandwidth, etc.
    - Determining hardware requirements.
    - Determining which 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.
2. When staff recommends apps for the Fort Payne City Mobile Device Management Apps Catalog or software for purchase and/or testing, it is the responsibility of the appropriate staff to properly vet the app or software to ensure that is instructionally sound, is in line with curriculum or behavioral standards, and is age appropriate.

Virus, Malware, Spyware, Phishing and Spam Protection
Appendix E

Virus, Malware, and Spyware Protection
Fort Payne City desktops, laptops, and fileservers run the Enterprise Level Security software. Virus definitions are updated every daily and an on-access scan is performed on all files upon opening. A full, scheduled scan runs every weekly. A full, scheduled scan is performed on all fileservers daily.

Internet Filtering
Student learning using online content and social collaboration continues to increase. Fort Payne 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 Internet filter using the user's network credentials. This process sets the filtering level appropriately, based on the role of the user (e.g., student, staff, or guest, and, more specifically for students, the grade level of the user.) All sites that are known for malicious software, phishing, spyware, etc. are blocked. Fort Payne City Schools will filter the Internet using software and/or hardware products in order to protect against access to inappropriate material on the Internet as required by CIPA. Fort Payne City Schools will monitor attempts to bypass the filter system to access inappropriate material. If a filtered site is needed for educational purposes the site can be unfiltered if deemed appropriate by the administrative staff.

Phishing and Spam Protection
Email is filtered for viruses, phishing attempts, spam, and other threats for staff by Microsoft Exchange Online Protection and, for students, by Google Mail.

Security Patches
Windows security patches and other Windows patches are scheduled to automatically download and install. The schedule install occurs during the following maintenance window: 3:00 a.m. every day. Updates that miss this window are applied on the next system startup.

Physical and Security Controls
Appendix F

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. Temperature and humidity levels in the data centers shall be monitored and maintained. 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 not to leave these devices logged in, unattended, or otherwise open to unauthorized use.
5. Network systems and network equipment shall be properly secured to prevent unauthorized physical access and to ensure that data are properly safeguarded to protect from loss.
6. Visitors shall be escorted by a person with authorized access to the secured area.
7. The delivery and removal of all asset-tagged and/or data-storing technological equipment or systems shall be monitored and controlled. A record of all such items entering or exiting their assigned location shall be maintained, 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. Technological equipment or systems being removed for transfer to another organization or being designated as surplus property shall be appropriately sanitized in accordance with applicable policies and procedures.

See also Appendix H (Purchasing and Disposal Procedures.)

Password Control Standards
Appendix G

The Fort Payne City Schools Data Governance Policy requires the use of strictly controlled passwords for network access and for access to secure sites and information. In addition, all users are assigned to Microsoft security groups. The security groups include separate groups at each school for Office Staff, Tech Staff, Instructional Staff, Students, and Users.

Password Standards:

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

1. Passwords shall never be shared with another person, unless the person is a designated security manager.
2. Every password shall, where possible, be changed yearly if not more frequently for staff.
3. Passwords shall, where possible, have a minimum length of eight (8) characters.
4. When possible, for secure sites and/or software applications, user-created passwords should adhere to the same criteria as required for network access.
    - Shall not contain the user's account name
    - Shall contain characters from three of the following four categories:
        - English uppercase characters (A through Z)
        - English lowercase characters (a through z)
        - Base 10 digits (0 through 9)
        - Non-alphabetic characters (for example, !, $, #, %)
5. When creating a password for secure information or sites, it is important not to use passwords that are easily guessed based on their association with the user (i.e. children's names, pets' names, birthdays, etc.). A combination of alpha and numeric characters is more difficult to guess.

B. Where possible, system software should enforce the following password standards:

1. Passwords routed over a network shall be encrypted.
2. Passwords shall be entered in a non-display field.
3. System software shall enforce the changing of passwords and the minimum length.
4. System software shall disable the user password when more than five consecutive invalid passwords are given. Lockout time shall be set at a minimum of 30 minutes.
5. System software should maintain a history of previous passwords and prevent their being easily guessed due to their association with the user. A combination of alpha and numeric characters is more difficult to guess.

Purchasing and Disposal Procedures
Appendix H

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 Fort Payne City Schools' district Technology Coordinator.

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

A. Purchasing Guidelines

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

B. Alabama Competitive Bid Laws

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: among them is http://www.examiners.state.al.us/purchcoop.aspx which is generally for technological devices and services, Fort Payne City Schools purchases from the Alabama Joint Purchasing Agreement (ALJP): https://connect.alsde.edu/sites/eia/aljp/SitePages/ALJP%20(Alabama%20K-12%20(IT)%20Joint%20Purchasing)Home.aspx.

In the event that a desired product is not included in one of these agreements, Fort Payne City Schools bids the item or items using the district's competitive bid process. All technological systems, services, etc. over $15,000 purchased with public funds are subject to Alabama's competitive bid laws.

C. Inventory

All technological devices or systems over $500 are inventoried by the Technology Department in accordance with the Fort Payne City Schools' Finance Department. There are some exceptions under $500 determined by the Technology Coordinator, such as, but not limited to, companion devices or peripherals that are inventoried. It is the responsibility of the local school Technology Coordinator to inventory technological systems used in the local school and manage said inventory. The district technology staff is responsible for ensuring that any network equipment, fileservers, district systems, etc. are inventoried.

D. 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; and
5. Excessive cost of maintenance or repair.

- The Superintendent, Local School Principal, Supervisor, Chief Financial Officer and/ or Technology Coordinator, shall approve school equipment disposals. Written documentation in the form of a spreadsheet including, but not limited to, the following shall be provided to the Technology Coordinator.

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

E. Methods of Disposal

Once equipment has been designated and School Board approved for disposal, it shall be handled according to school board equipment policy.

F. Required Documentation and Procedures

1. When equipment is donated by Fort Payne City Schools, a copy of the letter requesting the equipment shall be on-file with the district technology office prior to the donation.

2. Any equipment donated 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. The hard drives or removable storage devices shall be removed and destroyed.

3. Any reusable hardware that is not essential to the function of the equipment but that can be used as spare parts shall be removed. Examples include: special adapter cards, memory, hard drives, zip drives, CD drives, etc.

4. Mice, keyboards, and other small peripherals may be boxed together and shall not be listed on spreadsheet forms.

Fort Payne City Schools Technological Services and Systems Memorandum of Agreement (MOA)
Appendix I

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 Fort Payne City Schools **(FORT PAYNE CITY)**, 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 Fort Payne City Student Records. The Company hereby agrees that it shall maintain, in strict confidence and trust, all Fort Payne City 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 Fort Payne City Student Records during the term of the Agreement (collectively, the "Authorized Representatives") to maintain in strict confidence and trust all Fort Payne City Student Information. The Company shall take all reasonable steps to insure that no Fort Payne City Student information is disclosed to any person or entity except those who (a) are Authorized Representatives of the Company performing functions for Fort Payne City under the Agreement and have agreed to be bound by the terms of this Agreement; (b) are authorized representatives of FORT PAYNE CITY, or (c) are entitled to such Fort Payne City student information from the Company pursuant to federal and/or Alabama law. The Company shall use Fort Payne City 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 Fort Payne City 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 Fort Payne City 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 Fort Payne City 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 Fort Payne City of planned system changes that may impact the security of Fort Payne City data; (g) return or destroy Fort Payne City data that exceed specified retention schedules; (h) notify Fort Payne City of any data storage outside the US; (i) in the event of system failure, enable immediate recovery of Fort Payne City information to the previous business day. The Company should guarantee that Fort Payne City data will not be sold to, accessed by, or moved by third parties. In the event of a security breach, the Company shall (a) immediately take action to close the breach; (b) notify Fort Payne City 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 Fort Payne City student information compromised by the breach; (c) return compromised Fort Payne City data for review; (d) provide communications on the breach to be shared with affected parties and cooperate with Fort Payne City efforts to communicate to affected parties by providing Fort Payne City 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 Fort Payne City 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 Fort Payne City 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 Fort Payne City 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 Fort Payne City data of any kind, failure to follow security requirements and/or failure to safeguard Fort Payne City data. The Company’s compliance with the standards of this provision is subject to verification by Fort Payne City 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 Fort Payne City 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 Fort Payne City student data and/or staff data. The Company hereby acknowledges and agrees that, solely for purposes of receiving access to Fort Payne City 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 Fort Payne City 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 Fort Payne City 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.

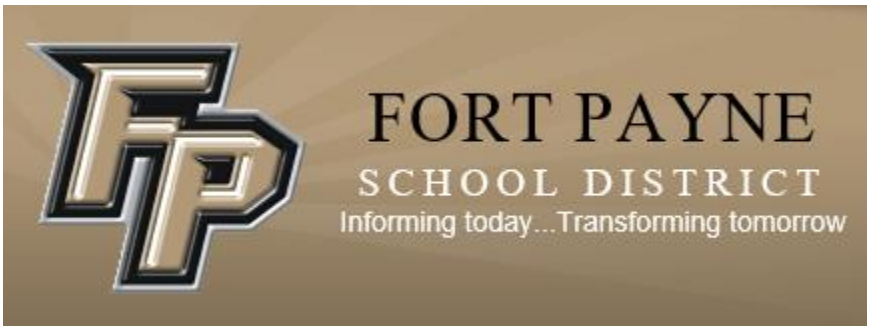
IN WITNESS WHEREOF, the parties hereto have caused this Addendum to be executed by their duly authorized officers effective as of the date first written above.

[COMPANY NAME]

By: _____
[Name] [Title]

Fort Payne City Schools

By: _____
Jim Cunningham Superintendent
Fort Payne City Schools



Data Governance/Employee Acceptable Use Form

By signing below, I acknowledge that I have read, understand, and agree to accept all terms and conditions of the Fort Payne City Schools Data Governance/Employee AUP Policy.

Name of Employee _____

Signature of Employee _____

School _____

Job Title _____

Date _____

Adopted by FPCS on 3-24-2016