2016-2017

Data Governance Policy

Table of Contents

Introduction

Data Governance focuses on improving data quality, protecting access to data, establishing definitions of security, maintaining data and documenting data policies. Our role is to ensure that the highest quality data possible is delivered throughout the entire school system. Protecting our students' and staffs' privacy is an important priority. We are committed to maintaining strong and meaningful privacy and security protections. The Calhoun County School System understands that the privacy and security of this information is a significant responsibility. We appreciate the trust placed upon us by our students, parents and staff.

The policy formally outlines how operational and instructional activity shall be carried out to ensure that the Calhoun County 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 Calhoun County Data Governance policy will be annually reviewed and changes will be made as necessary to ensure state and federal guidelines are being followed. With the Board's approval, the Data Governance Committee may quickly modify information in response to changing needs. All modifications will be posted on the Calhoun County Schools' website.

Committee Meetings
The Data Governance committee will meet at a minimum of two times per year. Additional meetings will be called as needed.

2016-2017 Data Governance Committee

The Calhoun County Schools 2016-2017 Data Governance committee consists of the following:
Mr. Joe Dyar - Superintendent
Ed Roe, Deputy - Superintendent
Jenel Travis - Director of Technology
Tina Parris - Chief Schools Financial Officer
Teresa Johnson - Executive Director
Dr. Charlene Hill - Director of Special Education
Lesa Cotton - Director of Health Services
Randy Reaves - Director of Safety, Security and Risk Management
Kelli Johnson – Counselor

Other Representatives of school administration, technology, maintenance, transportation, guidance counselors, media specialists, teachers, secretaries, and bookkeepers in order to cover every aspect of shared Calhoun County Schools' data.

Traci Shaw - Library Media Specialist
Chris Hayes - High School Principal
Lance Driskell - Network Administrator and ISO for Calhoun County Schools
Zach Bennett - Data Specialist
Chris Mitchell - Technology Application Support
Brian Clifton - Assistant Maintenance Supervisor
Dr. Banyon Allison - Transportation Director
Lisa Bragg - Reading Coach
Charissa Lambert - High School Teacher
Lacey Ward - Secretary
Chad Martin - Assistant Principal
Barbara Arrington - Elementary Teacher
Kevin Lockridge - Career Tech Center Director
Trina Shackelford - Bookkeeper

All members of the Calhoun County 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.

Calhoun County Schools Data Governance Policy

I. PURPOSE

The purpose of the Data Governance policy is to protect data or information in all its forms (written, electronic, or printed) from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This includes an appropriate level of security over the equipment, software, and practices used to process, store, and transmit data or information. Data governance is documented and reviewed annually by the data governance committee. Calhoun County Schools conducts annual training on their data governance policy and documents that training. The terms data and information are used separately, together, and interchangeably throughout the policy.

II. SCOPE

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 Calhoun County Schools' data and information, including but not limited to:

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

III. REGULATORY COMPLIANCE

The district will abide by any law, statutory, regulatory, or contractual obligations affecting its data systems. Calhoun County Schools complies with all applicable regulatory acts including but not limited to the following:

A. FERPA

The Family Educational Rights and Privacy Act applies to all institutions that receive federal aid from the Secretary of Education. This regulation protects student information and accords students specific rights with respect to their data.

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

B. 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 fight waste, fraud, and abuse in health care delivery and health insurance, but it is now used to measure and improve the security of health information as well.

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

C. IDEA

The Individuals with Disabilities Education Act is a four part piece of American legislation that ensures student with a disability are provided with Free Appropriate Public Education (FAPE) that is tailored to their individual needs.

**For more information, visit* http://www.idea.ed.gov

D. PPRA

The Protection of Pupil Rights Amendment affords parents and minor students' rights regarding our use of surveys, collection and use of information for marketing purposes, and certain physical exams. These include the right to the following:

- **a.** Consent before students are required to submit 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-
  - **i.** Political affiliations or beliefs of the student or parent
  - **ii.** Mental or psychological problems of the student or student's family
  - **iii.** Sexual behavior or attitudes
  - **iv.** Illegal, antisocial, self-incriminating, or demeaning behavior
  - **v.** Critical appraisals of others with whom respondents have a close family relationship
  - **vi.** Legally recognized privileged relationships (lawyers, minister, doctors, etc.)
  - **vii.** Religious practices, affiliations, or beliefs of the student or parent
  - **viii.** Income, other than as required by law to determine program eligibility
- **b.** Receive notice and an opportunity to opt a student out of-
  - **i.** Any other protected information survey, regardless of funding
  - **ii.** Any nonemergency, invasive physical exam or screening required as a condition of attendance, administered by the school or its agent, and not necessary to protect the immediate health and safety of a student, except for hearing, vision, or scoliosis screenings, or any physical exam or screening permitted or required under state law; and
  - **iii.** Activities involving collection, disclosure, or use of personal information obtained from students for marketing or to sell or otherwise distribute the information to others

E. COPPA

The Children's Online Privacy Protection Act regulates organizations that collect or store information about children under the age of 13. Parental permission is required to obtain certain information.

**For more information, visit* www.coppa.org

F. CIPA

The Children's Internet Protection Act, enacted by Congress in 2000, addresses concerns about children's access to obscene or harmful content over the internet. CIPA imposes certain requirements on schools that receive discount 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 activity of minors; and 2) as required by the Protecting Children in the 21st Century Act, they shall provide education for minors concerning appropriate online behavior, including interacting with other individuals on social networking, websites, and chat rooms, as well as cyber bullying awareness and response.

**For more information, visit* http://www.fcc.gov/guides/childrens-internet-protection-act

G. AAC

The Alabama Administrative Code is a compilation of the rules of all state agencies covered by the Alabama Administrative Procedure Act.

* *For more information, please visit* *http://www.alabamaadministrativecode.state.al.us/alabama.html*

H. Alabama Records Disposition Authority

Alabama Law Section 41-13-23 authorized the Alabama Department of Archives and History to publish regulations for Local Government Records Destruction.

**For more information, visit*
http://www.archives.alabama.gov/officials/rdas/local/EdRDA_04_14.pdf

The information below is from the Local Boards of Education Records Disposition Authority approved by the Local Government Records Commission, April 2013. 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

I. PCI DSS

The Payment Card Industry Data Security Standard was created by a consortium of payment brands including American Express, MasterCard, Visa, and Discover. It covers the management of payment card data and is relevant for any organization that accepts credit card payments.

**For more information, visit* www.pcisecuritystandards.org

J. ESEA

The Elementary and Secondary Education Act of 1965 allows military recruiters access to 11th and 12th grade students' names, addresses, and telephone listings when requested.

**For more information visit http://www.ed.gov/essa?src=rn*

K. **Acceptable Use Policy and Email Guidelines for the Use of Technology**

The Acceptable Use Policy outlines the guidelines and behaviors that users are expected to follow when using school technologies or when using personally-owned devices on the school campus or in connection with school activities.

**For more information, please visit* http://www.ccboe.us and navigate to Our District >> Policies and Reports
http://ccboe.schoolwires.net/site/handlers/filedownload.ashx?moduleinstanceid=569&dataid=3831&FileName=Staff AUP.pdf

**See also Appendix A*

IV. RISK MANAGEMENT

A thorough risk analysis of all Calhoun County Schools' data networks, systems, policies, and procedures shall be conducted on an annual basis or as requested by the Superintendent, ISO, or Technology Director. The risk assessment shall be used as a basis for a plan to mitigate identified threats and risk to an acceptable level. All vulnerabilities found during the annual risk analysis will be reviewed by the Data Governance committee and addressed based on recommendations by the Data Governance committee.

V. DATA CLASSIFICATION, ACCESS ROLES, AND PERMISSIONS

Classification is used to safeguard the confidentiality of data. Data is classified according to the most sensitive detail it includes. Data has the same classification regardless of format (source document, electronic record or report). Data is classified based on the following data classification levels:

A. **Personally Identifiable Information/Personal Information (PII)** - PII includes information that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. PII will only be accessed by individuals with permission. Unauthorized disclosure, modification, or disposal of PII may violate Alabama state laws, federal laws, result in criminal or civil penalties, or incur legal implications.

B. Restricted/Confidential Information - Includes very important or highly sensitive information. This information is private in nature and shall be restricted to those with a legitimate business need for access. Examples may include personnel information, key financial information, system access passwords, file encryption keys, access codes to secure areas housing servers or computers containing confidential or restricted information. Unauthorized disclosure, modification, or disposal of Restricted/Confidential Information may violate Alabama state laws, federal laws, result in criminal or civil penalties, or incur legal implications. The decision about the provisions of access to this information shall always be cleared through the information owner and/or Data Governance committee.

C. Internal Information - Internal information is intended for unrestricted use within Calhoun County Schools, and in some cases within affiliated organizations such as Calhoun County Schools' business or community partners. This type of information is already widely-distributed within Calhoun County 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, or most internal electronic mail messages that do not include information classified as Personally Identifiable Information/Personal Information or Restricted/Confidential Information. Unauthorized disclosure of Internal Information outside Calhoun County Schools may not be appropriate.

D. Public Information - Public Information has been specifically approved for public release by an authority within each entity of Calhoun County Schools. Examples of Public Information may include marketing brochures and material posted to Calhoun County Schools' web pages.

E. Directory Information - Calhoun County Schools may disclose appropriately designated "directory information" without written consent. Directory Information, which is information generally not considered harmful or an invasion of privacy if released, can also be disclosed to an outside organization without prior written consent. Organization may include but are not limited to: Companies that manufacture class rings, companies that publish yearbooks or military recruiters upon request. If you do not want Calhoun County Schools to disclose directory information from your child's education records without your prior written consent, you must notify the district in writing. The following information had been designated as Directory Information:

- **a.** Student first and last name
- **b.** Student gender
- **c.** Student home address
- **d.** Student home telephone number
- **e.** Student school assigned monitored and filtered email address
- **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
- **o.** Student homeroom

F. Access Roles and Permissions - The Calhoun County Schools Data Governance Policy requires the use of strictly controlled passwords for network access to secure sites and information. In addition, all users are assigned to security groups that are managed through group policies.

a. Network Roles and Permissions

i. Security Groups by location

ii. School Groups consist of the following

1. Administrators

2. Staff

3. Students

iii. Contract employees and long-term substitutes

1. All contract employees (ex. contract employees provided by Kelly Services) and interns shall read and sign the *Request for Email Account and Other Resources for Contract Employees* form. Additionally the contract employee will read the Data Governance Policy and the Acceptable Use Policy and Email Guidelines for the Use of Technology. The contract employee shall read and sign the Student Data Confidentiality Agreement. Forms are available at www.ccboe.us under the Employment page.

b. Chalkable INow Roles and Permissions

i. X Technology Administrators
ii. District Personnel Administrator
iii. School Personnel Administrator
iv. Special Assignments
v. Attendance Clerk
vi. Counselor
vii. District School Nurse
viii. Enrollment Clerk
ix. iHealth Admin
x. School Office Personnel
xi. State Reporting
xii. Census Clerk
xiii. Chalkable Pilot
xiv. Discipline Entry
xv. Health Data Personnel
xvi. PE Teacher
xvii. Teacher
xviii. Transportation Clerk
xix. Certified Unlicensed Medication Assistant
xx. INFOCUS
xxi. School Announcements
xxii. Student Office Assistant
xxiii. Substitute Office Staff
xxiv. Substitute School Nurse
xxv. Textbook Coordinator
xxvi. View Only
xxvii. System API Group

c. Other Roles

- **i.** Information Security Officer(ISO)
  1. The ISO is responsible for working with the superintendent, the Director of Safety, Security and Risk Management, the Technology Director, Data Government Committee, Data Specialist, Application Support Specialist, Webmaster, Data owners and users to develop and implement prudent and effective security policies, procedures and controls. This includes performing and overseeing security audits, reporting regularly to the superintendent, Technology Director, and the Director of Safety, Security and Risk Management in regards to security or safety threats.
- **ii.** Administrators
  1. Administrators are responsible for overseeing their staff use of information and systems with support from Superintendent, the Director of Safety, Security and Risk Management, the Technology Direct, and the ISO. This includes access authorizations, login changes in positions and job functions, logins for employee terminations and transfers, revoking physical access to terminated employees, providing employee training for computer systems and data systems, reporting misuse, and initiating corrective actions when problems are identified.
- **iii.** Information Owner
  1. The information owner is responsible for data retention, and ensuring prudent and effective procedures are in effect to protect the integrity, confidentiality, and availability of information used or created. It is the responsibility of the information owner to report the misuse or loss of Calhoun County Schools' data promptly.
- **iv.** Data Custodian
  1. The data custodian is assigned by an administrator or data owner based on his/her role and is generally responsible for the processing and storage of information. In addition the data custodian is responsible for the administration of controls as specified by the owner.
- **v.** User
  1. The user is any person who has been authorized to read, enter, print, or update information in support of their authorized job responsibilities. The user must comply with procedures and guidelines in the Data Governance Policy, keep authentication information secure, report the loss or misuse of information, and follow corrective actions when problems are identified.

VI. SYSTEMS AND INFORMATION CONTROL

A. Systems - 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 or assets of Calhoun County Schools shall be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

B. Software Acquisition and Usage

- **a.** All software used by Calhoun County Schools' personnel must be compliant with federal, state, and Calhoun County Schools' policy guidelines.
- **b.** Software or cloud-based software that directly accesses any Calhoun County Schools' data classified as Personally Identifiable Information/Personal Information or Restricted/Confidential Information shall be covered by the Memorandum of Agreement (MOA) signed by the software proprietor. MOA applies to both purchased and free software. A current and accurate copy of the software license agreement must be kept by the purchaser in either paper or electronic form. Financial records and agreements detailing the purchase and terms of the software acquisition will be kept, in paper or electronic form, by the Chief School Financial Officer or local bookkeeper.
- **c.** All computer software developed by Calhoun County Schools' employees or contract personnel is the property of Calhoun County Schools and shall not be copied for use at home or any other location.
- **d.** Teaching staff will ensure that classroom instructional software has been properly vetted and is appropriately aligned with current curriculum standards.
- **e.** School administration will ensure that school wide instructional software has been properly vetted and is appropriately aligned with current curriculum standards. The Technology department must approve software purchases. The local school/department designee will keep current and accurate records of any approved software.
- **f.** The district curriculum manager must approve instructional software to be used at the district level. The Technology Department must approve district software purchases. The Technology Department software support personnel will keep current and accurate records of any approved software.
- **g.** Non instructional software shall not be installed without obtaining proper permission from the Calhoun County Schools' Technology Department in writing.
- **h.** If the software must be installed by the software proprietor, the installation will be coordinated through the Technology Department in conjunction with the local school or district.
- **i.** Test Phase Software installation must be approved by the Technology Department, District Curriculum Manager, and a FERPA compliant must be signed by the software proprietor.
- **j.** Freeware installation must be approved by the local school administrator, and the Technology Department. In addition the freeware must be FERPA compliant, used for instructional purposes. Personally Identifiable Information/Personal Information should not be used or revealed when using freeware.

C. Virus, Malware, Spyware, Phishing, Ransomware, and SPAM Protection

a. Virus checking system software approved by the Calhoun County Schools' Technology Department is deployed on all computers and servers using a multi-layered approach (computers, servers, gateways, firewalls, filters, etc.) that ensures all electronic files are appropriately scanned for viruses, malware, spyware, phishing, ransomware, and SPAM. Users shall not turn off or disable Calhoun County Schools' protection systems or install other systems. Email is filtered for viruses, phishing, spam, and spoofing.

D. Internet Filtering

a. Calhoun County Schools uses Internet filtering as a way to balance safety with learning by balancing educational Internet resources and app use with student safety and network security. Internet traffic from all devices that authenticate to the network is routed through the filter using the user's network credentials. This process sets the filtering level appropriately based on the role of the user. All sites that are known for malicious software, phishing, spyware, etc. are blocked.

E. Physical and Security Controls

a. Physical and electronic access to information systems that contain personally identifiable information/personal information, restricted/confidential information, internal information, and computing resources is controlled. Access will be granted for the reason of fulfilling specific job responsibilities and shall be authorized by the superintendent, administrator, or the data governance committee with the assistance of the Technology Director or the information security officer. Unique user identification and passwords are required for all systems that maintain or access PII/PI, Confidential/Restricted Information, or Internal Information. Access to areas to which information processing is carried out shall be restricted to only appropriately authorized individuals.

b. Network systems shall be installed in an access-controlled area and shall be protected against fire, water damage, and other environmental hazards such as power outages and extreme temperatures.

c. At a minimum staff passwords should be changed every 90 days meet system password requirements. A combination of alphanumeric characters should be used. Passwords should never be saved when prompted by any application nor should they be programmed or recorded in an area from which it may be retrieved. It is the responsibility of the user not to leave any device logged in, unattended, and open to unauthorized use. **Users will be held accountable for all actions performed on the system with their user id. User accounts and passwords shall <u>NOT</u> be shared.**

d. No PII/PI, Confidential/Restricted Information 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.

e. Calhoun County Schools provides safeguards so that PII/PI, Confidential/Restricted Information, or Internal Information is not altered or destroyed in an unauthorized manner. The information is backed up to local servers and cloud based storage for needed access or disaster recovery.

f. Security mechanisms are in place to guard against unauthorized access to data that are transmitted over the network through integrity controls and/or encryption. Data integrity is important in maintaining and assuring the accuracy and consistency of data over its entire life-cycle. This also includes authorized and proper alteration or destruction of data.

g. Security patches are installed through automatic downloads.

h. Data transfers, exchange, and printing should include only the minimal amount of information necessary to fulfill the request. When sharing this information a MOA shall be in place with external entities.

i. Remote access to the Calhoun County Schools network from outside is allowed using the Calhoun county Schools portal. All other network access is prohibited without authorization from the Technology Director, Information Security Officer, or Data Governance Committee. Information that is accessed remotely shall maintain the same level of protection as information accessed within the Calhoun County Schools' network.

j. Records of information system activity, such as audit logs, access reports, and security incident tracking reports shall be reviewed as necessary.

k. Controls shall ensure that Calhoun County Schools can recover from any damage to critical systems, data, or information within a reasonable period of time. Each school, department, or individual is required to report any instances immediately to the Superintendent, Risk Management Officer, Technology Director and/or ISO for response to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages data or systems.

F. Communications

a. When communicating through email only Calhoun County Schools District supported email shall be used. This includes sharing information 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.

b. Calhoun County 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. Calhoun County 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.

G. Purchasing and Disposal Procedures

a. Purchasing

i. All systems that will be used in conjunction with Calhoun County Schools' technology resources or purchased, regardless of funding, shall be purchased from an approved list or be approved by the district Technology Director. Failure to have the purchase approved may result in lack of technical support, request for removal from premises, or denied access to other technology resources.

ii. 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 Examiner's office. (http://www.examiners.state.al.us/purchcoop.aspx) Generally for technological devices and services, Calhoun County Schools purchase from the Alabama Joint Purchasing Agreement. (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, Calhoun County Schools bids the item or items using the district's competitive bid process. All technological systems, services, etc. over $15,000 at a district level purchased with public funds are subject to Alabama's competitive bid laws.

iii. Inventory - All technological devices are inventoried by the Technology Department using the WASP inventory system. The district technology staff is responsible for ensuring that any technology equipment is inventoried. The local bookkeeper is responsible for contacting the Technology Department when ordering technology items for the local schools. Inventory must reflect any in-school transfers, in-district transfers, district awarded items, state awarded items, and/or donations.

b. Disposal

- **i.** Disposed items must be reflected on inventory at both the school level and the district level. Equipment shall be considered for disposal for the following reasons:
  1. Obsolete
  2. Broken and Beyond Repair
  3. Stolen (Send Police Report)
  4. Trade In
  5. Auction
  6. Other(Explain)
- **ii.** Written documentation in the form of the electronic version of "Request for Deletion of Fixed Assets/Supplemental Inventory", located on the Calhoun County Schools' Staff page under Forms, shall be submitted to the administrator for approval. Mice, keyboards, and other small peripherals may be boxed together and shall not be listed on the form. The form includes the following"
  1. School
  2. Quantity
  3. Control Number
  4. Description/Serial Number
  5. Location-Room Number
  6. Funding Source
  7. Reason
  8. Estimated Cost
  9. Cost Center
- **iii.** Once approved by the administrator a work request must be submitted and a technician must review the item, remove the hard drive to be degaussed and remove any other useable parts to be returned to stock. Once this is complete a pink sticker reading "Ok for Pickup" will be placed upon the item for disposal. The technician will then initial the form and return it to the office.
- **iv.** The original form should then be sent to the technology director and signed. Two copies will be made
  1. A copy is made for the Network Manager for the item to be removed from the Active Directory.
  2. A copy is made for the Application Support Specialist to be removed from the inventory.
- **v.** The original is then sent to the Chief School Financial Officer for signature/approval, forwarded to the Superintendent for signature/approval.
- **vi.** The information is submitted for final board approval. Once the equipment is board approved it is picked up by maintenance for disposal.

c. Discard

- **i.** All electronic equipment in the Calhoun County Schools district shall be discarded in a manner consistent with applicable environmental regulations. Electronic equipment may contain hazardous materials such as mercury, lead, and hexavalent chromium. In addition, systems may contain Personally Identifiable Information (PII), Confidential, or Internal Information. Systems shall be wiped clean of this information prior to leaving the school district.
- **ii.** A district-approved vendor shall be contracted for the disposal of all technological systems/equipment. The vendor shall provide written documentation verifying the method used for disposal and a certificate stating that no data of any kind can be retrieved from the hard drive or any other component capable of storing data.
- **iii.** Under no circumstances should any technological systems/equipment be placed in the trash. Doing so may make Calhoun County Schools and/or the employee who disposed of the equipment liable for violating environmental regulations or laws.

d. Donation

- **i.** Donations are prohibited to individuals outside of the school system or to current faculty, staff, or students of Calhoun County Schools.
- **ii.** The donation or sale of portable technology-related equipment is permissible to retiring employees if the following criteria have been met:
    1. The portable equipment has been used solely by the retiring employee for over two years;
    2. The equipment will not be used by the employee assuming the responsibilities of the retiring employee.
    3. The equipment has reached or exceeded its estimated life.

*All donations and/or sales shall be approved by the Superintendent, Chief School Financial Officer, and Technology Director.

VII. COMPLIANCE

A. The Data Governance Policy applies to all users of Calhoun County 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 Calhoun County 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 Calhoun County Schools' policies. 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:

- **a.** Unauthorized disclosure of PII or Confidential Information.
- **b.** An attempt to obtain a login code or password that belongs to another person.
- **c.** 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.
- **d.** Installation or use of unlicensed software on Calhoun County School technological systems.
- **e.** The intentional unauthorized alteration, destruction, or disposal of Calhoun County Schools' information, data and/or systems. This includes the unauthorized removal from Calhoun County 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.
- **f.** 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. 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.
- **g.** Changing data intentionally for fraudulent reasons may incur criminal charges.

C. Violation of Data Governance: Consequences will be determined based on the nature of the offense. Violations of the Data Governance Policy may have disciplinary repercussions, including but not limited to the following:

- **a.** Verbal warning
- **b.** Letter of concern
- **c.** Corrective action plan
- **d.** Loss of privileges
- **e.** Administrative leave
- **f.** Financial accountability
- **g.** Legal action or prosecution
- **h.** Termination

ALSDE State Monitoring Checklist

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

Acceptable Use Policy and Email Guidelines for the Use of Technology

Introduction

Calhoun County Board of Education (—the Board) recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st century technology and communication skills. To that end, we provide access to technologies for student and staff use. This Acceptable Use Policy outlines the guidelines and behaviors that users are expected to follow when using school technologies or when using personally-owned devices on the school campus or in connection with school activities. Each user will be provided access to this policy and will sign an agreement to abide by its terms before establishing an account.

- The school board‘s network is intended for educational purposes.
- All activity over the network or when using district technologies may be monitored and retained. Access to online content via the network may be restricted in accordance with our policies and federal regulations, such as the Children‘s Internet Protection Act (CIPA).
- Students are expected to follow the same rules for good behavior and respectful conduct online as offline.
- The Board‘s policies, regulations, and rules of conduct apply not only to use of school-owned resources, but also to personally-owned technology resources brought on school property or used in connection with school activities.
- The Board‘s disciplinary jurisdiction may include off-campus activity that threatens the school‘s ability to maintain a safe and orderly environment (Board Disciplinary Jurisdiction, 5.16 in Policy Manual and page 3 in Student Handbook).
- Misuse of school resources or personal devices can result in disciplinary action. Users may be financially liable for damage / loss from misuse or negligence.
- The Board makes a reasonable effort to ensure students‘ safety and security online, but will not be held accountable for any harm or damages that result from use of school technologies.
- Users of the district network or other technologies are expected to alert the Technology Department or local administrative staff immediately of any concerns for safety or security.

Technologies Covered

The Board may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more. As new technologies emerge, The Board will attempt to provide access to them. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed. This includes personally-owned devices, such as cell phones or other mobile devices, when used on the school campus or in connection with school activities.

Usage Policies

All technologies provided by the district are intended for education purposes. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, careful and kind; do not try to get around technological protection measures; use good common sense; and ask if you don‘t know.

Web Access

The Board provides its users with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with CIPA regulations and school policies. Web browsing may be monitored and web activity records may be retained indefinitely. Users are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn‘t be, the user should follow district protocol to alert a technology staff member or submit the site for review.

Email

The Board may provide users with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies.

If users are provided with email accounts, they should be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown or questionable origin; should use appropriate language; and should only communicate with other people as allowed by the district policy. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

Social / Web 2.0 / Collaborative Content

Recognizing the benefits collaboration brings to education, The Board may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally-identifying information online.

Mobile Devices

The Board may provide users with mobile computers or other devices to promote learning outside of the classroom. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network.

Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users should report any loss, damage, or malfunction to the Technology Department or local administrative staff immediately. Users may be financially accountable for any damage or loss resulting from negligence or misuse. Use of school-issued mobile devices off the school network may be monitored.

Personally-Owned Devices

Users should keep personally-owned devices (including laptops, tablets, smartphones, and cell phones) turned off and put away during school hours except as authorized or directed by school personnel.

In all matters involving the use or possession of personally-owned devices, students are expected to abide by the Code of Student Conduct, the Cell Phone Policy, and all other applicable school policies and rules.

Because of security concerns, when personally-owned mobile devices are used on campus, they should not be used over the school network without express permission from Technology staff.

Security

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or questionable origin.

If you believe a computer or mobile device you are using might be infected with a virus, please alert the Technology Department. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

Downloads

Users should not download or attempt to download or run programs over the school network or onto school resources without express permission from school personnel. For the security of our network, users should download only authorized files from reputable sites, and only for educational purposes.

Netiquette

Users should always use the Internet, network resources, and online sites in a courteous and respectful manner. Users should also recognize that among the valuable content online there is unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet. Users should also remember not to post anything online that they would not want parents, teachers, or future colleges or employers to see. Once something is online, it‘s out there—and can sometimes be shared and spread in ways you never intended.

Plagiarism

Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Users should not take credit for things they didn‘t create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Personal Safety

Users should never share personal information, including phone number, address, social security number, birth date, or financial information, over the Internet without adult permission.
Users should recognize that communicating over the Internet or other electronic means brings certain risks, and should carefully safeguard personal information. Users should never agree to meet with someone that they met online —in real life without parental permission. If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult. Students should immediately bring any threatening or unwelcome communications to the attention of school personnel.

Cyberbullying

Cyberbullying will not be tolerated. Harassing, threatening, insulting, impersonating, excluding, and cyberstalking are all examples of cyberbullying. Do not send or post electronic communications with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviors or any online activities intended to physically or emotionally harm another person will result in serious disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.

Access and Privacy

All users will be provided with network storage space and should use only those accounts, files, software, and technology resources that are assigned to him/her. Network storage areas will be treated like school lockers. Network administrators will review files and communications to maintain system integrity and ensure that users are using the system responsibly. Users of school technology resources have no personal right of privacy or confidentiality with respect to the use of such resources and should not expect files, information, or communication stored on school resources to be private.

Unauthorized Access

Individuals shall not attempt to log in to the network by using another user's account and/or password, or allow someone to use his/her password to access the network, email, or the Internet. Individuals must not attempt to modify technology resources, utilities, and configurations, or change the restrictions associated with his/her accounts, or attempt to breach any technology resources security system, either with or without malicious intent. Individuals must not attempt to disrupt any computer services or data by spreading viruses, spamming, hacking, or any other means.

Data Integrity

Individuals shall not attempt to make fraudulent changes or modify data maliciously. Individuals shall not trespass or make changes in another user’s work, folders, or files.

Inappropriate Materials or Language

No profane, obscene, lewd, inflammatory, abusive, harassing, threatening, discriminatory, or impolite language should be used, nor should materials be accessed which are not in line with the rules of school behavior. Materials placed on or linked to system or school-sponsored Web pages must be preapproved by an administrator or authorized designee. Sending or displaying offensive, obscene, or sexually explicit messages or pictures is not permitted.

Examples of Acceptable Use:

Users will:

- Use school technologies for school-related activities.
- Follow same guidelines for respectful, responsible behavior online that students are expected to follow offline.
- Treat school resources carefully and alert staff if there is any problem with operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher or other staff member of threatening, inappropriate, or harmful content (images, messages, posts) online.
- Use technologies at appropriate times, in approved places, for educational pursuits. Cite sources when using online sites and resources for research.
- Recognize that use of school technologies is a privilege and treat it as such. Be cautious to protect the safety of self and others.
- Help to protect the security of school resources.

*This is not intended to be an exhaustive list.

Examples of Unacceptable Use:

Users will not:

- Use technologies to hurt, harass, attack or harm other people or their work.
- Attempt to find or access inappropriate web sites, images, or content.
- Use language online that would be unacceptable in the classroom.
- Engage in cyberbullying, harassment, or disrespectful conduct toward others
- Damage computers, computer systems, or computer networks in any way (this includes changing workstation configurations such as screen savers, backgrounds, printers, BIOS information, preset passwords, etc.).
- Install software or download unauthorized files, games, programs, or other electronic media. Attempt to hack or access sites, servers, or content not intended for my use.
- Attempt to circumvent school safety measures and filtering tools.
- Send spam, electronic chain letters, or other useless information.
- Waste limited resources such as disk space, printing capacity and bandwidth.
- Post personally-identifying information about myself or others.
- Agree to meet in real life with someone that the student met online.

- Use technologies for illegal activities, to pursue information about such activities, or to access illegal materials (i.e. threats, instructions on how to perform an illegal act, child pornography, drug dealing, fake identifications, purchase of alcohol, gang activities, etc.)
- Plagiarize content found online or violate copyright laws.
- View, send, display, or use racist, discriminatory, profane, lewd, vulgar, rude, disrespectful, threatening, or inflammatory language, messages or pictures.
- Share password with others or attempt to find out the password of others.
- Post false or damaging information about other people, the school system, or school organizations.
- Trespass in another user's work, folders, or files.
- Use system network resources for personal gain or commercial purposes. This is not intended to be an exhaustive list.
- Incur unauthorized financial obligations for the school or school system

Limitation of Liability / Disclaimers

The Calhoun County School System makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the Board's technology resources will be error-free or without defect. Although the Board employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness. The Board will not be responsible, financially or otherwise, for unauthorized transactions conducted or financial obligations incurred on the system network. The Board will not be responsible for damage or harm to persons, files, data, or hardware. Neither the school nor the Calhoun County Board of Education will be responsible for any damages or losses incurred, including but not limited to: loss of data resulting from delays or interruption of service; loss of data stored on system resources; damage to personal property used to access system resources; the accuracy, nature, or quality of information stored on system resources; or unauthorized financial obligations incurred through system-provided access. Further, even though the system will use technical or manual means to limit student access, these limits do not provide a foolproof means for enforcing the provisions of this policy.

Adoption of Rules and Procedures

The Superintendent or designee is authorized to develop additional or more specific rules, procedures, or guidelines regarding acceptable use of technology to facilitate implementation of this policy.

Search and Inspection of Technology Resources and Devices

All technology resources, including but not limited to network and Internet resources, accounts, email systems, computers, and 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 to determine if a user is in violation of Board policies or rules 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 and administration of the school system, or for any other reason not prohibited by law. In addition, any device (regardless of ownership) brought onto school grounds by a student is subject to immediate inspection when there is a reasonable suspicion that the contents or recent utilization of the device is in violation of any of the Board's policies, rules or regulations regarding access to and use of technology resources.

Violations of Acceptable Use Policy

Student use of the computer network, the Internet, and other technology resources is a privilege not a right. Violations of this policy may have disciplinary repercussions, including, but not limited to, the following:

- Suspension or termination of network, technology, or computer privileges
- Completion of online course regarding acceptable use or similar corrective or rehabilitative measures
- Loss of privilege of bringing personally-owned technology devices to school
- Notification of and/or conference with parents
- In-school detention, out-of-school suspension, suspension from school bus, or other disciplinary actions as authorized by the Code of Student Conduct
- Financial accountability for damage or loss
- Legal action and/or prosecution

Staff and contract employee use of the computer network, the Internet, and other technology resources is a privilege not a right. Violations of this policy may have disciplinary repercussions, including, but not limited to, the following:

- Verbal Warning
- Corrective action plan
- Loss of privileges
- Administrative leave
- Financial accountability
- Legal action or prosecution
- Termination

Email

Legal Risks

- Email is a school business or educational communication tool, and users are obliged to use this tool in a responsible, effective, and lawful manner. Email lends itself to a kind of informality yet, from a legal perspective, may have the same implications as would any written communication. Any email is discoverable in a due process situation or other legal action. In addition, any email exchanged by a school system employee is public record. Other legal risks of email for Calhoun County Schools and/or their network users include the following:
    - Sending emails with any libelous, defamatory, offensive, racist or obscene remarks.
    - Forwarding emails with any libelous, defamatory, offensive, racist or obscene remarks.
    - Transmitting or forwarding confidential information;
    - Forwarding or copying messages without permission or implied permission.
    - Knowingly sending an attachment that contains a virus that severely affects another network or other users.
- By following the guidelines in this document, the email user can minimize the legal risks involved in the use of email. If any user disregards the rules set out in these guidelines, the user will be fully liable and Calhoun County Schools will disassociate itself from the user as far as legally possible.
- Do not send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks. If you receive an email containing libelous, defamatory, offensive, racist or obscene remarks, promptly notify your supervisor.
- Use caution if you forward a message without implied permission or without acquiring permission from the sender first, especially if it contains sensitive or private information.
- Do not forge or attempt to forge email messages.
- Do not send email messages using another person's or a bogus email account.
- Do not copy a message or attachment belonging to another user without the permission or implied permission of the originator.
- Do not disguise or attempt to disguise your identity when sending email.

Best Practices

Calhoun County Schools considers email as an important means of communication and recognizes the importance of proper email content and of speedy replies in conveying a professional image and in delivering good service. The use of email in education, however, is proliferating and the precise legal issues regarding appropriate use are yet to be determined. We are confident that—

- Any email exchanged by school system employees about individual students is public record.
- Any email pertaining to a particular student is discoverable in a due process situation or other legal action.
- The nature of email lends itself to impulsive, overly informal, and sometimes unprofessional communication.

Note: The Technology Director is authorized to monitor and report inappropriate behaviors to the employee's supervisor who will take appropriate disciplinary action. Any other reports of inappropriate behavior, violations, or complaints will be investigated and routed to the employee's supervisor for appropriate action. Violations may result in a loss of access and/or appropriate disciplinary action up to and including termination. When applicable, law enforcement agencies may be involved.

Therefore Calhoun County Schools urges users to adhere to the following guidelines:

Guidance on Email between School Employees and Parents/Guardians

- Examples of generally appropriate use of email between school employees and parents/guardians:
    - Teachers invite parents to provide email addresses and then send out emails to those addresses reporting on classroom activities, projects, and assignments. These messages are generic and do not refer to specific students.
    - Teachers may initiate or respond to email from a parent or guardian about a specific child, exchanging objective not subjective information such as the student's attendance, participation, homework, and performance in class.
- Examples of inappropriate use of email between school employees and parents/guardians:
    - Using email to report on serious problems regarding individual students.
    - Using email to discuss confidential and sensitive matters, including:
    - Medical/psychiatric/psychological diagnoses and treatments.
    - Contents of special education and/or Section 504 evaluations, intervention plans, IEPs, 504 plans, disciplinary matters.
    - Family problems and other sensitive family information.
    - Using language that is subjective, judgmental, unprofessional, pejorative, and/or labeling. Examples:
        - "Have you considered that Johnny might have ADHD?"
        - "Overall, I think that Johnny is unmotivated/lazy."
        - "I don't think there is anything wrong with Johnny except his negative attitude."
        - "I think this child's problem is his home life."
- Email between teachers and parents shall be positive and/or general in nature when possible. Discussions involving serious problems and any and all protected information (medical, psychological, psychiatric, Special Education, and Section 504, and disciplinary matters) should occur in person or by telephone.
- Parents may initiate inappropriate email exchanges. Example: "Johnny is in your American History class and is failing. His father is an alcoholic and we are divorced. Johnny has ADHD and clinical depression. Can you please tell me how he is doing in your class and what I can do to help him?"
    - That kind of message shall be deleted and the teacher receiving it should call the parent who sent it. Alternately, the teacher could reply to it, deleting everything from the body of the email sent by the parent, and then respond with directions about how the teacher can be reached by telephone or in person. Do not regard a parent or guardian's initiation of this kind of email exchange as constituting permission for you to discuss these matters via email.

General Best Practices involving all email are as follows:

Writing emails:

- Use short, descriptive Subject: lines.
- Avoid lengthy, detailed email messages. Consider using an attachment for "How To" information, directions, procedures, processes, or similar types of information.
- Avoid unnecessary attachments or large file attachments such as multiple pictures, mini movies, etc. AVOID USING ALL CAPITALS.
- If using cc or bcc feature, take steps to inform the cc or bcc recipient of any action expected unless the action is explicit in the email. The bcc option is often used to avoid revealing recipient email addresses to the entire group receiving the email; otherwise, the bcc option shall be used sparingly if at all.
- If you forward emails, state clearly what action you expect the recipient to take.
- Use the spell checker before you send out an email.
- If the content of an email is not of a public nature, consider using another form of communication or protect the information by using a password.
- Only mark emails as important if they really are important.

Replying to emails:

- Emails shall be answered within 24 hours, and at minimum employees are expected to check email at least once per day.
- Responses shall not reveal confidential information and shall be professional.

Electronic Social Networking, Instant Messaging including Texting, etc.

- Electronic social networking and/or instant messaging, such as but not limited to Twitter, IM, or texting, among staff and students is a particularly sensitive matter in a time when growing numbers of school employees maintain social networking accounts, email extensively in their personal lives, and are accustomed to using instant messaging services.
- An absolute prohibition of communicating electronically with students seems excessive. On the other hand, teachers and school staff shall maintain the highest standards should they choose to interact with students through electronic media. Below are some typical situations on which employees might need guidance.
    - Guidelines below are presented in a Q&A format.
        - Q: Is it ok for me to initiate electronic communications with a student?
        - A: If a teacher initiates overly personal contact with students outside of school, whether in person or electronically, he or she may create an impression of an unhealthy interest in that student's personal life and may leave himself or herself open to an accusation of inappropriate conduct. Therefore, caution shall be exercised in this type of communication.

        - Q: What if I receive an email or other electronic message such as a text from a student?
        - A: This very much depends on the nature of the communication received. We would strongly discourage any use of texting, instant messaging or "chat"-type communication with students for purposes other than school related communications. Do not engage in social "chat" with students. If a communication is received which appears to be a social greeting, you might do best just to acknowledge it in an appropriate way at school. A very brief acknowledging electronic response might be appropriate in some circumstances. However, it is perfectly OK not to respond to such greetings. If you choose to not respond, making an extra effort to cheerfully greet the student at school might be appropriate.
    - If a student sends a message with disturbing content, you should discuss this with your administrator or supervisor, including a school counselor in the discussion as needed.
    - If a student sends a message that appears to suggest an emergency (an allegation of abuse or a student sharing suicidal thoughts or plans), try to contact your administrator or supervisor at once.
- Q: What about Facebook accounts or other social networking sites? Should I respond to an invitation to become a student's "Friend"?
- A: We recommend that you not engage in online social networking with students unless the site is used for school information or academic reasons only. This would only be an issue, of course, if you choose to maintain a Facebook, or similar account. If you do so, we recommend that you be extremely cautious about the content of your profiles and pages. If you are strictly using a social networking site for school related topics and stay away from personal content then these sites shall be treated much like any other educational blog. (However, the use of comments, "writing on walls," and so on, would be likely to lead to major problems if an approval process is not in place before posting.) You may find that it is easier to simply tell your students that you have a policy not to accept students as "friends."

General Email Information

- Virus Protection and Filtering
    - Incoming and outgoing emails sent to or received from Calhoun County Schools' Exchange email server are scanned for viruses, spam, and content. However, users are expected to exercise caution when opening emails from unknown users or when using the web-based email client from home computers.
    - Incoming emails may be blocked if the message size is over 100,000 KB or if there are multiple attachments.

- Disclaimer
    - Calhoun County Schools recommends that employees add a disclaimer to outgoing emails or automatically attach a disclaimer such as the one below to each email sent outside the school system.
    - "This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this email in error please notify the system manager. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the Calhoun County Schools. Finally, the recipient should check this email and any attachments for the presence of viruses. The company accepts no liability for any damage caused by any virus transmitted by this email."

System Monitoring

- Although Calhoun County Board policy permits personal use of school email accounts, users shall have no expectation of privacy in anything they create, store, send or receive on the Calhoun County Schools' computer system. Emails may be monitored without prior notification if Calhoun County Schools deems this necessary. If there is evidence that users are not adhering to the guidelines set out in this policy, Calhoun County Schools reserves the right to take disciplinary action, including termination and/or legal action.

Email Accounts

- Email accounts are assigned to new employees when their employment is approved by the Board of Education and when the new employee has read and signed the Acceptable Use Policy. and has understanding of the Acceptable Use Policy. All email accounts maintained on the Calhoun County email and Internet communication systems are property of Calhoun County Schools. Calhoun County maintains student accounts and employee accounts.
- Passwords shall not be given to other people and shall be changed if the user believes his/her password is no longer secure. Email accounts are deleted immediately when employees retire, resign, or take leave from the school system for a period of six months or more. Only Calhoun County employees are given email accounts. Upon request by the administration, Calhoun County employee sponsored accounts, such as PTA accounts or accounts for contract employees may be created. Employee-sponsored accounts are subject to these guidelines and it is the responsibility of the sponsoring employee to educate the user of this and all other relevant technology-related policies and guidelines.
- Email is not to be utilized by employees to share confidential information about students or other employees. Email messages are not entirely secure and should not be considered private. Messages may sometimes be diverted accidentally to a destination other than the one intended. Privacy in these communications is not guaranteed. The district reserves the right to access stored records in cases where there is reasonable cause for misuse.

Electronic Communications for Personal Use

- Although Calhoun County Schools' email and Internet communication systems is meant for school business, Calhoun County Schools allows the reasonable use of email for personal use if certain guidelines are adhered to:
    - Personal use of email shall not interfere with work.
    - Personal emails shall also adhere to the guidelines in this policy.
    - Personal emails shall be deleted regularly so as not to clog the system.
- The forwarding of chain letters, junk mail, inappropriate jokes and executable files is strictly forbidden.
    - Do not send personal mass mailings.
    - Do not send emails for personal gain, to solicit business for friends, family, etc., or for political purposes.
    - All messages distributed via the school system's email and Internet communication systems, even personal emails, are Calhoun County Schools' property.
    - Recognize the diversity of co-workers when sending emails. For example, some employees would regard emails of a religious nature, including invitations to religious events or services – even prayer requests – as inappropriate or offensive.

Questions

- If you have any questions or comments about these guidelines, please contact your principal or immediate supervisor. If you do not have any questions Calhoun County Schools presume that you understand and are aware of the rules and guidelines and will adhere to them.

School Year:_____

Employee Technology Information Agreement

Legal First Name: _____ Nickname: _____

Middle Initial: __ Last Name: _____

Last Four Digits of SS# _____ Date of Birth: _____

Home Phone: _____ Current Email Address: _____

Grade/Subject/Position: _____School:_____

Would you like for Calhoun County Schools to request a transfer of your STI PD professional development records? _____ If yes, in which school system were you employed?

I have received and am knowledgeable of the content in the Data Governance Policy including the Acceptable Usage Policy and Email Guidelines.

Name: _____ Date: _____

**Accounts are disabled on the last day of active employment or when on leave for more than 6 months.*

Student Data Confidentiality Agreement

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

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

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

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

_____ **Date**_____

Signature of Employee

_____ **School**_____

Job Title

Request for Email Account and Other Resources for Contract Employees

For contract employees to qualify for an email account in the ccboe.us/calhoun.k12.al.us domain, they shall have a contract on file with Personnel and perform work for Calhoun County Schools on a regular basis. If Calhoun County Schools has a contract with an agency to send "consultants" to Calhoun County Schools on an as needed basis, they generally do not qualify and should use the email account provided to them by the agency. However, we will review all requests.

Contract Employee legal Name: _____ _____ _____
(First Name) (Middle Name) (Last Name)

Requester: _____ Department/School:_____

Start Date: **_____ End Date: _____**

Work to be Performed or Position: _____

Is contract employed through Kelly Services? _____ Yes _____ No _____Other

Has contract employee had background check? _____ Yes _____ No

Has contract employee been E-Verified? _____ Yes _____ No _____ NA

Other Access Requested: Inow-should have permissions equal to ____ Teacher____ Office____ Other If other, please specify: _____

SETS Account with permissions equal to _____ Staff ____ Office _____ User

Reason for Request: _____

Signature of Requester: _____

Signature of Administrator: _____

_____Denied _____ Approved Date: _____
_____Initials

Calhoun County Schools Technological Services and Systems Memorandum of Agreement (MOA)

Appendix C

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 **CALHOUN COUNTY SCHOOLS** (CCS), 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 CCS Student Records. The Company hereby agrees that it shall maintain, in strict confidence and trust, all CCS 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 CCS Student Records during the term of the Agreement (collectively, the "Authorized Representatives") to maintain in strict confidence and trust all CCS Student Information. The Company shall take all reasonable steps to insure that no CCS Student information is disclosed to any person or entity except those who (a) are Authorized Representatives of the Company performing functions for CCS under the Agreement and have agreed to be bound by the terms of this Agreement; (b) are authorized representatives of CCS, or (c) are entitled to such CCS student information from the Company pursuant to federal and/or Alabama law. The Company shall use CCS 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 CCS 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 CCS 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 CCS 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 CCS of planned system changes that may impact the security of CCS data; (g) return or destroy CCS data that exceed specified retention schedules; (h) notify CCS of any data storage outside the US; (i) in the event of system failure, enable immediate recovery of CCS information to the previous business day. The Company should guarantee that CCS 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 CCS 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 CCS student information compromised by the breach; (c) return compromised CCS data for review; (d) provide communications on the breach to be shared with affected parties and cooperate with CCS efforts to communicate to affected parties by providing CCS 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 CCS 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 CCS 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 CCS 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 CCS data of any kind, failure to follow security requirements and/or failure to safeguard CCS data. The Company’s compliance with the standards of this provision is subject to verification by CCS 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 CCS 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 CCS student data and/or staff data. The Company hereby acknowledges and agrees that, solely for purposes of receiving access to CCS 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 CCS data in accordance with all federal state and local laws, rules and regulations regarding the confidentiality of such records. In addition, all data on company premises shall be destroyed after all required documentation and data has been returned to CCS. The non-disclosure obligations of the Company and its Authorized Representatives regarding the information contained in CCS 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]

By:_____

Joe Dyar Superintendent Calhoun County Schools