BCS

BUILD. CREATE. SUCCEED.

Data Governance

Policy, Procedures, Standards, and Processes

Board Approved Date:

May 21, 2025

Approved by:

Rodney P. Green, Superintendent

Date: May 21, 2025

TABLE OF CONTENTS

These procedures, standards and processes are authorized by the following Blount County Schools policy:

Data Governance and Use Policy 5.0

The Superintendent is authorized to develop guidelines for the management, utilization and distribution of electronically stored data within the school system. These guidelines must adhere to relevant state and federal regulations and include provisions for data security (including physical security measures), access controls, quality control, and data exchange and reporting (including external data requests, and third party data use). Nothing in this policy or in any procedures authorized hereunder creates or expands any entitlement to confidentiality of records beyond that which is established by law or specific Blount County Board of Education policy.

Any unauthorized access, use, transfer, or distribution of Board data by any employee, student, or any other individual may result in disciplinary action (up to and including termination for employees) and other legal action.

Scope

These procedures, standards and guidelines apply to all data that is stored electronically by the Blount County School system. These procedures, standards and processes are intended to protect information that is deemed confidential by law from unauthorized changes, destruction, or disclosure throughout its life cycle. Additionally, these procedures aim to protect the integrity of the school system's hardware and software, including providing an appropriate level of security measures over the equipment and software used to process, store and transmit this information.

The procedures, standards and guidelines outlined herein apply to all students, and employees of the district, contractual third parties, and agents of the district who have access to district information systems or information. Information includes, but not limited to:

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

The intent of these procedures, standards and guidelines is to implement the laws governing the confidentiality of the school system's records and is not intended to create or expand any entitlement to confidentiality of records beyond that which is established by law.
Furthermore, nothing herein should be deemed to create or expand any entitlement to copies of such records beyond what is established by law. In general, Blount County Schools reserves the right to adopt, revise, interpret, amend, repeal, suspend, or apply its policies and procedures according to its assessment of the needs and interests of the school system; subject only to such limitations on the exercise of such prerogatives as may be imposed by law.

Dissemination of Data Governance Policy, Standards, Processes, and Procedures

The Blount County Board of Education Data Governance and Use Policy, Policy 5.00 is available to the public and all internal stakeholders via the District Policy Manual at https://www.blountboe.net/.

The detailed procedures, standards, processes and procedures that serve to implement that Policy 5.00 are shown below. As exposing these specific security measures to outside, unknown parties could result in greater risk to the district's data, this document will not be made publicly available. Requests for detailed information about the district's data security procedures shall be brought to the data governance committee or the Superintendent who will determine the legitimacy of the request and respond accordingly.

Data Governance Committee

Rodney P. Green, Superintendent
Christopher Lakey, Assistant Superintendent
Cindy Parker, Chief School Financial Officer
Meagan Holt, Federal Programs Director
Bridgette Murphree, Primary Curriculum Coordinator
Cindy Bartlett, Secondary Curriculum Coordinator
Gary Noles, PowerSchool Administrator
Bradley Williams, Technology Director
Peyton Richards, Network Technician
Phillip G. Hazelrig, Human Resources Coordinator

Roles and Responsibilities:

- Direct reporting to the Superintendent.
- Evaluate and respond to internal proposals relating to the use of data and information in connection with data mining, behavioral targeting and data analysis.
- Monitor implementation and compliance of processes, and, when appropriate, propose revisions to policies and procedures.
- Provide oversight to the superintendent, the Technology Director and company employees in their efforts to reinforce good business practices and maintain legal compliance.
- Be frequently and timely informed of compliance activities, training activities, communications programs, compliance audit reports and reports of alleged violations of the company's data governance policies.
- Conduct annual evaluations of the company's data governance practices.
- Consult with any advisors they deem necessary to ensure that Blount County Schools conducts its business activities in compliance with the law.

Applicable Laws and Standards

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

Alabama Data Breach Act of 2018
Alabama Law Section 8-38-1, relating to consumer protection; to require certain entities to provide notice to certain persons upon a breach of security that results in the unauthorized acquisition of sensitive personally identifying information.

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

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 Appendix A

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. See Appendix B

IDPAA
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. *In general, schools are not bound by HIPAA guidelines.*

PCIDSS
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.

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

STATE SUPERINTENDENT MEMO September 8, 2023
Cybersecurity Measures for Local Educational Agencies (LEAs) Cyber Awareness Training, Cybersecurity Incident Response Plan Development, Multi-Factor Authentication (MFA).

Information Risk Management Practices

The analysis involved in Blount County 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.

Findings from the risk analysis will be added to the Cybersecurity Action Plan, see Appendix G.

Compliance

The Data Governance Policy, Procedures, Standards and Processes apply to all users of Blount County Schools information systems, including; employees, staff, volunteers, affiliates, and contractors. Failure to comply may result in disciplinary action up to and including dismissal in accordance with applicable Blount County School procedures, or, in case of outside affiliation, termination of the affiliation.

Blount County Schools will provide training on its data governance policy for all employees, staff members, volunteers, affiliates, and contractors who are involved in the creation, utilization, or maintenance of data as required. Documentation of this training will be retained for our records.

Possible disciplinary corrective action may be instituted for violations of Blount County Schools data governance policy, procedures, standards and processes, including, but not limited to the following actions.

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

Definitions and Responsibilities

Definitions

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

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

- **Data:** Facts or information, including audio and video.

- **Entity:** Organization such as school system, school, department or in some cases business

- **Information:** Knowledge that you get about something or someone; facts or details.

- **Data Integrity:** Data or information that has been entered correctly and has not been altered or destroyed in an unauthorized manner.

- **Involved Persons:** Every user of Systems, (see below) at Blount County Schools - no matter what their status. This includes nurses, residents, students, employees, contractors, consultants, temporaries, volunteers, substitutes, student teachers, interns, etc.

- **Systems:** All data-involved computer equipment/devices and network systems that are operated within or by Blount County Schools, physically or virtually. This includes all platforms (operating systems), all computers/devices (personal digital assistants, desktops, mainframes, telephones, laptops, tablets, game consoles, etc.), and applications and data (whether developed in-house or licensed from third parties) contained on those systems.

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

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

Responsibilities

A. **Data Governance Committee:** The Data Governance Committee for Blount County Schools is responsible for working with the Technology Director 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 and Procedures annually and as required by the Alabama State Department of Education, communicating changes in policy to all involved parties.

2. Educating data custodians and managing owners and users with comprehensive information about security controls affecting system users and application systems.
3. Performing or overseeing security audits.
4. Implementing the BCS Cybersecurity Response Plan
5. Reporting regularly to the superintendent and Blount County Schools on status of information security.

B. User Management: Blount County 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 Technology Director, and the Data Governance Committee the loss or misuse of Blount County 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.

C. Information Owner: The owner of a collection of information is usually the administrator or supervisor responsible for the creation of that information. In some cases, the owner may be the primary user of that information. In this context, ownership does not signify proprietary interest, and ownership may be shared. The owner 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 State Records Disposition Authority guidelines, industry standards, Data Governance Committee guidelines, or advice from the school system 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 Technology Director the loss or misuse of Blount County Schools' data.
7. Initiating corrective actions when problems are identified.
8. Promoting employee education and awareness by utilizing programs approved by the Data Governance Committee, 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.

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

1. Access information only in support of their authorized job responsibilities.
2. Comply with all data security procedures and guidelines in the Blount County Schools Data Governance Policy and Procedures 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 Technology Director and/or Data Governance Committee the loss or misuse of Blount County Schools' information.
5. Follow corrective actions when problems are identified

Data Quality: All users hold the responsibility for ensuring the accuracy, consistency, and timeliness of the data they enter and maintain. It is the duty of all District School Administrators and Supervisors to establish standards for data quality. Supervisors should immediately report incidents where data quality does not meet standards to their superior and to any other relevant department or agency, if applicable.

Data Classification Levels

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, image, 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 Blount County 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 Blount County Schools, its staff, parents, students including contract employees, or its business partners. Decisions about the provision of access to this information shall always be cleared through the information owner and/or Data Governance Committee.

C. Internal Information

1. Internal Information is intended for unrestricted use within Blount County Schools, and in some cases within affiliated organizations such as Blount County Schools' business or community partners. This type of information is already widely distributed within Blount County Schools, or it could be distributed within the organization without advance permission from the information owner. Examples of Internal Information may include: personnel directories, internal policies and procedures, most internal electronic mail messages.
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 due to legal or contractual provisions.

D. Public Information

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

Procedure for Selection/Approval of Computer Hardware and Software Connecting to the BCS Network and/or Storing PII.

Purpose of Procedure:

- To guarantee that computer hardware and software acquired by Blount County Schools will fulfill the function for which is intended.
- To guarantee that software and hardware to be purchased is compatible with existing computer hardware, software, and network infrastructure.
- To guarantee that software and hardware to be purchased is not a duplication of existing hardware and software.
- To guarantee proper planning for the implementation of computer hardware and software (i.e. testing, training, data conversion, administration, etc.).
- To guarantee that costs associated with ongoing support for software are identified.
- To guarantee costs associated with the maintenance and operation of computer hardware are identified.

Definition of Computer Hardware:
Computer equipment is defined as desktop computers, laptops, Chromebooks, server, network equipment, mobile wireless devices, and IOT (Internet of Things) devices such as monitoring equipment, VoIP, security cameras, door access controls, etc. capable of connecting to the Blount County Schools network and any peripheral devices that connects to computers, such as; printers, scanners, etc.

Definition of Software:

- All operating systems used to control the operation of the computer and peripheral devices.
- All computer software applications run on stand-alone or networked workstations, laptops and servers.
- Cloud-based software/applications.

Approval of Selected Computer Hardware:

- All computer hardware must meet specifications as defined in the Minimum Specifications and Requirements for Computer Hardware and Software document Computer hardware meeting specifications does not require additional Technology Department approval.
- The Technology Department must approve any computer hardware that is not covered by the Computer Equipment Bid Specifications document.
- The Technology Department will not support computer hardware that fails to meet specifications, and/or was not approved by the Technology Director.
- The Technology Department will take action to prevent the device from connecting to the network in accordance with the Cybersecurity Incident Response Plan.

Approval of Software:

- Computer operating system software must meet specifications as defined in the Specifications and Requirements for Computer Hardware and Software document. The Technology Department must approve all computer operating system software that does not meet specifications.

- Computer applications for use on more than one computer, either stand-alone, server based, or cloud-based must be approved by the Technology Department prior to purchase. Curriculum software will also require approval by the Curriculum department. Any software purchased that does not meet specifications and was not approved will not be supported.

Software Licensing:

1. All district software licenses owned by Blount County Schools will be:
   - Kept on file at the central office,
   - Accurate, up to date, and adequate, and
   - In compliance with all copyright laws and regulations
2. All other software licenses owned by departments or local schools will be:
   - Kept on file with the department or local school,
   - Accurate, up to date, and adequate, and
   - In compliance with all copyright laws and regulations
3. Software installed on Blount County Schools technological systems and other electronic devices:
   - Will have proper licensing on record,
   - Will be properly licensed or removed from the system or device, and
   - Will be the responsibility of each Blount County School employee purchasing and installing to ensure proper licensing
4. 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, COPPA and FERPA compliant, and are in compliance with software agreements before requesting use. Staff members are responsible for ensuring that parents have given permission for staff to act as their agent when creating student accounts for online resources.
5. Purchased software accessed from and storing data in a cloud environment will have a Memorandum of Agreement (MOA) on file, See Appendix F.

New Computer Equipment and Software Approval Process

In the Evaluate and Test phase, the computer hardware or software will be assessed based on existing standards and its potential for integration into the technology framework of Blount County Schools. Additionally, the effectiveness of the computer hardware or software will be analyzed concerning the specific tasks or services it is intended to provide.

1. Evaluation may include but is not limited to the following:
   - Conducting beta testing.
   - Determining how the software will impact the Blount County Schools IT environment such as storage, bandwidth, total cost of ownership, etc.
   - Determining hardware requirements.
   - Determining what additional hardware or software is required to support a particular piece of equipment or software package.
   - Outlining the license requirements/structure, number of licenses needed, and renewals.
   - Review vendor support/warranty.

2. Determining any Maintenance Agreements including cost.
    - Determining how the software is updated and maintained by the vendor.
    - Determining funding for the initial purchase and continued licenses and maintenance.

Virus, Malware, Phishing and SPAM Protection Procedure

Virus, Malware, and Spyware and Ransomware Protection
Blount County desktops, laptops, and file servers run Sophos endpoint security.

Phishing
KnowBe4 is in use to provide employee training related to Phishing.

Internet Filtering
Student learning using online content and social collaboration continues to increase. Blount County 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 Palo Alto Firewall (Alabama SuperComputer Authority) using the user's network credentials. This process sets the filtering level appropriately based on the role of the user, such as, student, staff or guest. All sites that are known for malicious software, phishing, spyware, etc. are blocked.

Security Patches
Windows security patches and other Windows patches are scheduled to "auto-download" and "auto- install" as updates are released.

IT Security Control and Standards

Purpose: This document outlines the IT security protocols and standards for the Blount County School District. Information Technology (IT), in this context, encompasses computer systems and related devices, networks, software, and communication infrastructure. It details the usage conditions, as well as the rights and responsibilities of both users and administrators, along with the strategies employed for implementation.The aim of this document is to ensure:

- Uninterrupted IT services
- The integrity, security and validity of data
- The ability to recover effectively and efficiently from disruption
- The protection of all Blount County Schools IT assets, including data, software and hardware

- Physical Security
    - Computer Servers
        - All servers shall be located in a secure, lockable room or secure server cabinet.
        - Access shall be restricted to authorized personnel for server and network administrative purposes only; visitors should be supervised at all times.
        - Protection from electrical failures and fluctuations shall be protected against by the installation of an uninterrupted power supply (UPS} and surge protection device.
        - Server equipment shall be adequately protected from environmental hazards including temperature, water, fire and dust.
        - It is the schools' administrators' responsibility to ensure the physical security of computer servers.
        - Non-employee, third party contractors, etc. are not allowed access to server equipment without a technology department staff member present.
    - Network Equipment
        - When financially feasible, network equipment such as switches, hubs, routers and media converters shall be secured in a lockable network cabinet or other secure location that is inaccessible by unauthorized personnel.
        - Access shall be restricted to authorized personnel. Non-employee, third party contractors, etc. are not allowed access to network equipment without a technology department staff member present.
        - All physical (twisted pair, fiber, wireless or modem), network installations and upgrades must be approved and performed, or supervised by the Technology Department.
        - It is the schools' administrators' responsibility to ensure the physical security of network equipment.
    - Computer workstations and peripheral equipment
        - Computer workstations should be protected from power fluctuations by the installation of surge protection devices.
        - All computer workstations, laptops and peripheral equipment shall be protected from environmental hazards including, temperature, water, fire, and dust.
        - All computer workstations and peripheral equipment should be shut down and powered off at the end of the day.
        - It is the individual user's responsibility to ensure the physical security of computer workstations and peripherals assigned to them.

- Information Security
    - Data Classification - It is essential that all Blount County School data be protected. All data should be reviewed and classified at one of the following levels of classifications: See Data Classifications Levels for descriptions.
        - Personally Identifiable Information (PII)
        - Confidential
        - Internal
        - Public
        - Directory
    - Control of Access to High Risk Information
        - Access to all computers/networks that access High Risk Information must be controlled by individual and unique login names and authentication passwords.
        - Each individual user is responsible for the security of their user account and password and will be held responsible for any activity that takes place in their accounts. Any discovered violation or attempted violation of system security must be reported immediately to the Technology Department.
        - As stated in current acceptable use policies, users must not share username and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. All users must secure their username, password, and system access from unauthorized use.
        - Multi-factor authentication is highly recommended for all staff.
        - User accounts should be disabled or removed when an employee is no longer employed or assigned to a school site. It is the responsibility of the local school administrator to notify the technology department when accounts need to be closed.
        - Logins and passwords should not be coded into programs or queries unless they are encrypted or otherwise secure.
        - A screen/keyboard lock or login screen should be active on all machines when they are not in use.
        - All connections or software that access High Risk Information data must be closed when not in use. Minimizing to the task bar is not acceptable.
        - All High Risk Information data shares must be protected by share access controls that allow only authorized users' access to the shares.
        - Only authorized users should attempt access to High Risk Information.
        - Students should never be allowed access to any High Risk Information except for curriculum software where an authorized system administrator has assigned them a unique username and password that allows them access to course work or tests assigned to them.

- Computer generated printouts that contain High Risk Information must be protected from unauthorized access or copying. Printouts containing High Risk Information must be shredded prior to disposal.
- Computer removable media that contains High Risk Information must be stored in a protected area that prevents access. High Risk Information backups should be encrypted when feasible to add an extra level of security. Removable media containing High Risk Information must be destroyed prior to disposal.

- Passwords
  - All users of systems that contain High Risk Information must have a strong password.
  - All server administrator or root accounts must be given a password that conforms to the password selection criteria when a system is installed, rebuilt or reconfigured.
  - Passwords must not be placed in emails unless they have been encrypted. System - server level administrative passwords should be changed on a
  - regular basis as specified by the Technology Department.
  - User level passwords should be changed yearly at minimum or when specified by the Technology Department.
  - User passwords should meet the following standards:
    - A minimum of eight alphanumeric characters.
    - Contain both upper and lower case characters.
    - Include special characters (e.g.@#$%"&*()_+).

  Passwords should not contain:
  - A single word in any language, slang, dialect, jargon, etc.
  - Personal information, names of family, pets, etc.
  - When changing passwords the reuse of the previous three passwords is not allowed.
  - Passwords should never be written down.
  - Do not use the "Remember Password" feature of applications.
  - The use of password auditing software is restricted to the Technology Department for security auditing purposes only.
- Responsible Use of Computer and Network/Internet Resources
  - All employees of the Blount County Schools must sign a Responsible Use Policy.
  - All students and their parents must sign a Responsible Use Policy each school year.

- Information Loss Prevention
  - Data Backup (For disaster recovery only.) For data retention policy refer to the Electronic Mail Control and Standards document and The Employee AUA.
  - Backup of all High Risk Information must be completed on a regular basis and stored in a **safe** and secure manner that protects the data and meets disaster recovery requirements.
  - Backups must include multiple generations of data.

- Virus Protection
  - The willful introduction of computer viruses or disruptive/destructive programs into the Blount County Schools environment is prohibited, and violators may be subject to prosecution.
  - All desktop and laptop systems that connect to the network must be protected with approved, licensed anti-virus software that is kept updated. It is the responsibility of each individual user to ensure his/her computer is protected and has up-to-date virus definition files, and will be held accountable for any virus activity that takes place on their computer.
  - All servers that connect to the network must be protected with approved, licensed anti-virus software and kept updated. It is the responsibility of the server administrator to ensure anti-virus software is installed and active with up-to-date definition files.
  - All removable media, CD's, USB drives, etc. from an external source must be virus scanned before they are used within Blount County Schools.
  - Incoming e-mail should be scanned when financially feasible to implement.
  - When feasible, system or network administrators will inform users when a virus has been detected.
- Firewall
  - At minimum, a firewall should be installed that protects the Blount County Schools network from intrusion from the outside world.
  - When budget allows, an additional layer of firewalls should be installed to protect servers that store data categorized as High Risk Information from potential internal security vulnerabilities.
- Intrusion Detection
  - When budget allows, intrusion detection software should be installed on all servers housing data categorized as High Risk Information.
  - The use of intrusion detection software is restricted to the Technology Department for security auditing purposes only.
- Auditing
  - Operating systems and application software event logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems, must be enabled.
  - The use of LAN analyzer equipment and software is restricted to the Technology Department for security, maintenance and troubleshooting purposes only.
  - Server, firewall, and critical system logs should be reviewed frequently.
- Internet Security
  - All connections to the Internet, wired and wireless must go through a properly secured connection point to ensure the network is protected when the data is classified as High Risk or Confidential.
  - Internet and other external access is restricted to authorized personnel only. Only staff and students with signed Acceptable Use Policies are authorized to access Internet resources.
  - Personal, unapproved, obsolete devices should never be connected to any school or district network.

- System Security
    - All server installations and upgrades must be approved and performed or supervised by the Technology Department.
    - All server-networked applications must be approved and installed or supervised by the Technology Department.
    - All systems connected to the Internet should have a licensed vendor supported version of an operating system installed.
    - The use of unauthorized software and applications are prohibited. In the event of unauthorized software being discovered, it will be removed from the computer immediately. The Technology Department should be consulted if software is in question prior to installation.
    - All systems connected to the Internet must be current with security patches.
    - Regular system integrity checks of host and server systems housing High Risk Information should be performed.

- Information Security Incident and Response
    - An incident is at minimum any one or more of the following:
        - Loss of confidential information - data theft.
        - Compromise of information integrity - damage to data or unauthorized modification.
        - Theft of physical IT assets; including computers, storage devices, printers, etc.
        - Damage to physical IT assets including computers, storage devices, printers, etc.
        - Denial of service.
        - Misuse of services, information, or assets.
        - Connecting unauthorized or unapproved devices to the BCS network. Infection of systems by unauthorized or hostile software.
        - An attempt at unauthorized access.
        - Unauthorized changes to organizational hardware, software, or configuration.
        - Reports of unusual system behavior.
        - Responses to intrusion detection alarms.
    - In the event of an incident, the Cybersecurity Incident Response Plan will be implemented.

- Disaster Recovery
    - When financially feasible, a documented and tested disaster recovery plan should be established for each site and server that stores High Risk Information.
    - At minimum, backups of data and applications should be maintained at an offsite location. Data backups maintained offsite should be updated daily at minimum. Application backups should be updated as new versions are installed.

- Sanctions
    - Computers, labs or network segments on the Blount County Schools network will be disconnected if they are deemed by the Technology Department to be a security threat or danger to the remainder of the LAN/WAN.
    - The Technology Department reserves the right to remove and dispose of devices, equipment, or software that can no longer receive security updates due to cybersecurity threats.
    - Penalties for violation of this policy range from loss of computer resource usage privileges to expulsion for students or dismissal for employees. Each case will be determined separately on its own merits.

Electronic Mail Controls and Standards

Purpose
The purpose of this document is to describe the appropriate use of the Blount County School District email system, associated responsibilities, and rights of all Users of Blount County Schools email system.

I. Public Record and Privacy
The email system is the property of the Blount County School District. All email messages written, received and stored using the system are also the property of the District. The Blount County School District is not obligated to monitor the content of electronic mail messages; however, the Blount County School District reserves the right to inspect, copy, store, or disclose the contents of email messages, but will do so only when it believes these actions are appropriate to: prevent or correct improper use; ensure compliance with Blount County School policy, procedures, or regulations; satisfy a legal obligation; or ensure the proper operations of the email system. Employees of Blount County Schools shall have no expectation of privacy in anything they store, send or receive on the System's email system.

II. Acceptable Use
Blount County School District provides email for activities and associated administrative functions supporting its mission of public education. Incidental use of the email system for personal purposes is permissible. This does not include use requiring substantial expenditures of time and/or email resources, use for profit or use that would otherwise violate Board policy with regard to employee time commitments or system equipment.

Ill. Unacceptable Use
    a. Personal Use that creates a direct cost for the district is prohibited.
    b. Use for personal monetary gain or for commercial purposes that are not directly related to Blount County Schools business.
    c. Sending copies of documents in violation of copyright laws.
    d. Inclusion of the work of others into email communications in violation of copyright laws.
    e. Use of email to harass or intimidate others or to interfere with the ability of others to perform their job.
    f. Use of email for any purpose restricted or prohibited by laws or regulations.

g. "Spamming" i.e., spamming is creating or forwarding an annoying or unnecessary message to a large number of people.
h. "Spoofing," i.e., constructing an email so it appears to be from someone else.
1. "Snooping," i.e., obtaining access to the email of others for the purpose of satisfying curiosity, with no substantial System purpose.
J. Attempting unauthorized access to email or attempting to breach any security measures on any email system, or attempting to intercept any email transmissions without proper authorization.

IV. Shared Accounts
Account sharing is prohibited; all accounts will be logged onto by a single individual.

V. Accessing Another User's Email
Primary users may delegate access to their incoming email to other secondary delegated email users where appropriate. This should only be done in situations where the same delegated users might also handle the primary user's paper mail. In all cases, this should be done by means of the email systems delegation facilities, not by giving the delegate the ability to log onto the primary user's account ID.

VI. User ID Termination
All user email passwords will be revoked immediately upon a user's termination of employment with the Blount County School District or upon termination of whatever status gave the user access to the email system. The Human Resource manager is responsible for notifying the Technology Department of the user's termination.

VII. Disciplinary Action
Appropriate disciplinary action will be taken against individuals found to have engaged in prohibited use of the Blount County School District's email resources.

VIII. Legal Actions
Should any legal actions, civil or criminal, take place which require the production of Blount County Schools' employee emails or electronic files, the System will comply with properly executed legal requests to the extent possible. All legal consequences and associated penalties for civil and criminal violations, shall be the sole responsibility of the account holder and not that of the Blount County School District, unless otherwise found by a court of law.

Technology Disaster Recovery Plan

Disaster Definitions

Disaster for the purpose of this plan is defined as any loss of digital data caused by any act of nature, heat, vandalism, thief, mechanical failure, etc.

Loss of data is classified as follows:

- Level 1 - loss of data on a single workstation
- Level 2 - loss of data on a server
- Level 3 - loss of data at a site, this would include the loss of data on multiple servers and workstations.

Disaster Preparedness

All software and computers should be classified in one of the following groups for disaster recovery purposes:

- Critical - Mission Critical Software and Systems, includes SIS, CNP, HR and accounting
- Support - Support Software and Systems, includes Library circulation software, curriculum support software and E-mail
- Low Priority- Non-critical Software and Systems

Data Backups

Regular backups with multiple generations are critical to being able to recover from any level of disaster. At the very least a bad hard drive can be replaced, but the data cannot be recovered from the bad drive. Therefore, data must be backed up to media external to your computer or server.

- Local school administrators should verify that multiple generations of backups are being performed on all Critical and Support data at their school
- The district technology department is responsible for backup of District Office Critical and Support data
- It is the responsibility of the individual owners of Non-critical data to perform backups of their software and data
- Each school should maintain off-site storage of data; this is critical for recovery from a Level 3 disaster
- Each site should ensure that software installation and upgrade disk are stored off-site or available from another school in the district should their on-site copy be destroyed

Spare Computer Equipment

- When financially feasible a spare server should be maintained at the District to support recovery from a Level 2 or above disaster at any site.
- At a minimum Low Priority servers at all sites should be identified as equipment available for use to recover from a Level 2 or above disaster at any site in the district.

Technology Inventories

- All schools inventories should be kept current in the District Inventory Database as outlined in the Inventory Procedure
- An up-to-date inventory list will be critical to the long-term recovery from a level 3 disaster

Disaster Recovery Plan

The following outlines Disaster Recovery Plans for each Level of data loss:

Level 1 - Loss of data on a single computer:

- An on-line work order should be filled out for the failing workstation
- If this computer stores Critical or Support data, then notify the Technology

Department so priority can be placed on the workstation

- If the computer is not repairable or cannot be repaired in a reasonable time and it is a mission critical computer, then a non-critical computer should be used until a replacement part or computer is purchased
- Non-critical computers will be repaired or replaced according to standard repair procedures

Level 2 - Loss of data on a server:

- Non-critical servers will be repaired or replaced according to standard repair procedures
- Priority will be placed on servers with Critical or Support data
- If servers with Critical data cannot be repaired within one day, Critical software will be installed on a Non-critical server at the site until the failing server is repaired or replaced. If a Non-critical server is not available on-site, one will be borrowed from another site
- Software and data will be loaded on the loaner server from on-site software and data backups

Level 3 - Loss of all data and equipment at a school:

- In the event of a major disaster at a school site, the technology department should be notified immediately
- Every effort should be made to recover and protect remaining equipment with priority being placed on Critical systems and then Support systems followed by Non-critical systems
- Recovery priority will be placed on Critical systems and data first
- If some of the facilities are usable on-site, a temporary scaled down network will be setup to support Critical data
- If no on-site facilities are usable, a scaled down network will be setup in the technology department repair lab until temporary facilities are in place
- Non-critical servers will be borrowed from sites within the district and loaded with Critical software and data from off-site backups
- If the site link to the Wide Area Network (WAN), and Internet is lost and not repairable, or available for an extended period, the technology department will pursue an alternative means to establish a connection to the WAN
- A minimum number of workstations to support Critical systems will be borrowed from Non critical sites
- Replacement servers, network equipment and workstations will be ordered as soon as cleared by the Superintendent

Level 4 - Loss of all data and equipment at the District Office

- Every effort should be made to recover and protect remaining equipment with priority being placed on Critical systems and then Support systems followed by Non-critical systems
- Recovery priority will be placed on Critical systems and data first
- If the facilities are usable, an on-site temporary scaled down network will be setup to support Critical data
- If the facilities are a total loss, servers will be setup at one of the existing school sites

to support District Critical data. A WAN connection to the temporary District Offices will be established by the most time and cost-efficient means available

- The WAN service provider will be contacted to perform the necessary WAN re-configurations
- Non-critical servers will be borrowed from sites within the district and loaded with Critical software and data from off-site backups
- A minimum number of workstations to support Critical systems at the temporary District Office will be borrowed from Non-critical sites
- Replacement servers, network equipment and workstations will be ordered as soon as cleared by the Superintendent

Purchasing and Disposal Procedures

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 Blount County Schools' District Technology Director.

All involved systems and information are assets of Blount County 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 Blount 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.

B. Alabama Competitive Bid Laws

All electronic equipment is subject to Alabama competitive bid laws. Generally, for technological devices and services, Blount County Schools purchase from the Alabama Joint Purchasing Agreement (ALJP): In the event that a desired product is not included in one of these agreements, Blount County Schools bids the item or items using the district's competitive bid process. All technological systems, services, etc. over $40,000 purchased with public funds are subject to Alabama's competitive bid laws.

C. Disposal Guidelines

Equipment/Software shall be considered for disposal for the following reasons:

1. End of useful life, no longer receive software updates.
2. Lack of continued need,
3. Obsolescence,
4. Wear, damage, or deterioration,
5. Excessive cost of maintenance or repair.

The Blount County School Board shall approve school disposals by discard or donation.

D. Methods of Disposal

Once equipment has been designated and approved for disposal, it shall be handled according to one of the following methods.

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

- **Discard**
  All electronic equipment in the Blount 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 (PU), Confidential, or Internal Information. Systems shall be wiped clean of this information prior to leaving the school district.

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

  Under no circumstances should any technological systems/equipment be placed in the trash. Doing so may make Blount County Schools and/or the employee who disposed of the equipment liable for violating environmental regulations or laws.

Data Access Roles and Permissions Student Applications

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

Only the PowerSchool Administrator will have responsibility over the District Student Information Systems, which will determine appropriate roles and access to the data and will enforce compliance with these roles and permissions.

Student Information System (SIS) Access

STUDENT INFORMATION SYSTEM enables authorized users to access the application from any device with internet access.

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

The technology department will monitor all use of the STUDENT INFORMATION SYSTEM.

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

are input into the STUDENT INFORMATION SYSTEM. Then one person in the district authorizes rights that reflect the requisition that is submitted.

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

Types of Users:

Personnel: All personnel must agree to the personnel acceptable use policy. Only long-term subs that have been approved per the board and have signed the acceptable use policy will have access to the STUDENT INFORMATION SYSTEM.

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

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

STUDENT INFORMATION SYSTEM Group (February 25, 2025)

1 Unassigned	No Access	0
2 State use 2	No Access	0
3 State use 3	No Access	0
4 State use 4	No Access	0
5 State use 5	No Access	0
6 State use 6	No Access	0
7 State use 7	No Access	0
8 State use 8	No Access	0
9 PowerSchool Administrator/DDA	Edit	2
10 PowerSchool Administrator/DDE	Edit	2
11 District Leaders	Read Only	2
12 District Curriculum	Read Only	1
13 District Special Education	Read Only	8

STUDENT INFORMATION SYSTEM Group (February 25, 2025)

14 District Nurse Supervisor	Edit	1
15 District Human Resources	Edit	3
16 District Federal Programs	Edit	4
17 District Lookup	Read Only	7
18 Career Tech Director	Read Only	2
19 Transportation Supervisors	Read Only	3
20 School Social Worker	Read Only	2
21 Assessment	Edit	2
22 Alternative School	Read Only	2
23 BCCTC-Bridge Counselor	Edit	1
24 N/A	N/A	0
25 SDE Health	Read Only	17
26 SIS Specialist	Edit	15
27 Principal	Edit	16
28 Assistant Principal	Edit	16
29 Counselor	Edit	6
30 Counselor	Read Only	13
31 Front Desk Lookup	Read Only	13
32 Front Desk Attendance	Edit	11
33 Sped-EL-Gifted	Read Only	1
34 School Nurse	Edit	20
35 SIS Specialist + Med Assist	Edit	1
36 Counselor+Attendance Queues Write	Edit	1
37 Substitute Nurse	Edit	23

STUDENT INFORMATION SYSTEM

38 Medication Assistants	Read Only	1
39 Helping Families Initiative	Edit	2
40 CNP Central Office	Read Only	2
41 Librarians	Read Only	14
42 RTI Facilitators	Read Only	2
43 Reading Coaches	Read Only	9
44 Transportation Lookup	Read Only	3
45 Health Aide - Advanced	**Edit**	1

Permissions for each group are further limited by page and field level permissions that limit access to only pages and fields required by users assigned to groups.

Security & Confidentiality Contract

Blount County Board of Education

This document serves as a binding **agreement** between the **State of Alabama, Blount County Board of Education and the employee of the Blount County Board of Education (signee) listed on the bottom of this contract. The employee agrees that he/she fully understands the critical nature of the security and confidentiality issues regarding student and staff personally identifiable information as well as information contained within PowerSchool SIS and all components thereof. The signature** on **this contract indicates that the signee agrees to abide by the security procedures established** in **Blount** County **Board of Education Policy 5.0** Technology **Responsible Use Policy, The Family Education Rights and Education** Act **of 1974 FERPA**, **as** well **as procedures outlined** in **Board Policy** 5.17.

The Alabama Department of Education provides educational data through the internet as it relates to student data/management, Special Programs, Health and assessment. PowerSchool SIS and its components contain confidential student and staff information including but not **limited to personally identifiable information, test scores, demographics, exceptionalities,** homeless **status, lunch programs, grades, attendance** and **discipline**. All **student/staff information is to be considered personal and confidential for use by** school **officials, administration, teachers, and other school personnel in the performance of their school related duties only (see below). The systems/data are not for public use. Student information from the system must not be** disclosed **to** anyone **other than a state, system or full time school official defined by the Family Education Rights and Privacy** Act **of 1974 (FERPA). Posting any personally identifiable information (PII) for a student or staff member on a website or including that PII** in **e-mail communication is a breach of this security agreement**.

> **An official as defined in the law** is **a person employed** full **time by the state, system, or** school **such as an administrator, supervisor, system test coordinator, building test coordinator, principal, teacher, and counselor, School Resource Officer, and/or support personnel (including health or medical staff and law enforcement unit personnel).** It **is a requirement that** this individual **have a legitimate** educational **interest if he/she needs to review an educational record in *order* to fulfill his or her professional responsibility. Curiosity does not qualify as a right to know**.

The student management system PowerSchool **SIS and all components thereof are password protected and require a user** ID **and an assigned password for access. School officials who are granted access to the system must abide by FERPA law/guidelines. Disclosure of passwords or access of any nature to the programs and contents to unauthorized personnel is prohibited and may result in disciplinary action** by the **Blount County Board of Education, and possible termination. Any individual responsible for allowing or** aiding in **the illegal access** to **any** portion **of the data systems by unauthorized personnel is subject to disciplinary action and possible termination. Usernames and passwords should remain confidential. Any school official that requests,** or **accesses/acquires illegally, another individual's username or password is subject to disciplinary action and possible termination**.

For more information on FERPA, see the U. S. Department of Education's Web page at https://www2.ed.gov/policy/gen/quid/fpco/ferpa/index.html

The signee below, by his/her signature certifies that:

- **I will maintain the** security, **integrity** and **confidentiality of student/staff information/and or student management data accessed through data systems PowerSchool SIS and components thereof past and present, shared verbally, electronically, visually, or through** school **communications.**
- **I will not share any password** nor **will I allow access visually or physically to the programs or their contents by any individual other than a school official** in the **performance of** school **related duties** (school **official as indicated by FERPA -above).**
- **By my signature I understand and confirm that disciplinary actions, including termination, will be taken in regards to breach of this security and confidentiality agreement.** If I **leave the position that allowed me access to student/staff information in any form, electronic, printed** or **in the process of** school **communications, I will neither share** nor **disclose any information accessed. To disclose any component of student/staff information** including **but not exclusive of PowerSchool SIS** and all **components** thereof would be in **violation of federal law, state and local directives.**

Name: (please print): _____

Signature: _____

School Location: _____

Date: _____

(Board Approved August 6, 2013)

Revised July 18, 2016

Appendix.A

FERPA - Overview

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.
- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.
- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):
    - School officials with legitimate educational interest;
    - Other schools to which a student is transferring;
    - Specified officials for audit or evaluation purposes;
    - Appropriate parties in connection with financial aid to a student;
    - Organizations conducting certain studies for or on behalf of the school;
    - Accrediting organizations;
    - To comply with a judicial order or lawfully issued subpoena;
    - Appropriate officials in cases of health and safety emergencies; and
    - State and local authorities, within a juvenile justice system, pursuant to specific State law.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article} is left to the discretion of each school.

Appendix B

COPPA - Information from the Federal Trade Commission

What is the Children's Online Privacy Protection Rule?
Congress enacted the Children's Online Privacy Protection Act (COPPA} in 1998. COPPA required the Federal Trade Commission to issue and enforce regulations concerning children's online privacy. The Commission's original COPPA Rule became effective on April 21, 2000. The Commission issued an amended Rule on December 19, 2012. The amended Rule took effect on July 1, 2013.

The primary goal of COPPA is to place parents in control over what information is collected from their young children online. The Rule was designed to protect children under age 13 while accounting for the dynamic nature of the Internet. The Rule applies to operators of commercial websites and online services (including mobile apps) directed to children under 13 that collect, use, or disclose personal information from children, and operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13. The Rule also applies to websites or online services that have actual knowledge that they are collecting personal information directly from users of another website or online service directed to children. Operators covered by the Rule must:
Post a clear and comprehensive online privacy policy describing their information practices for personal information collected online from children;

1. Provide direct notice to parents and obtain verifiable parental consent, with limited exceptions, before collecting personal information online from children;
2. Give parents the choice of consenting to the operator's collection and internal use of a child's information, but prohibiting the operator from disclosing that information to third parties (unless disclosure is integral to the site or service, in which case, this must be made clear to parents);
3. Provide parents access to their child's personal information to review and/or have the information deleted;
4. Give parents the opportunity to prevent further use or online collection of a child's personal information;
5. Maintain the confidentiality, security, and integrity of information they collect from children, including by taking reasonable steps to release such information only to parties capable of maintaining its confidentiality and security; and
6. Retain personal information collected online from a child for only as long as is necessary to fulfill the purpose for which it was collected and delete the information using reasonable measures to protect against its unauthorized access or use.

Who is covered by COPPA?
The Rule applies to operators of commercial websites and online services (including mobile apps) directed to children under 13 that collect, use, or disclose personal information from children. It also applies to operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13.

The Rule also applies to websites or online services that have actual knowledge that they are collecting personal information directly from users of another website or online service directed to children.

What is Personal Information?
The amended Rule defines personal information to include:

- First and last name;
- A home or other physical address including street name and name of a city or town;
- Online contact information;
- A screen or user name that functions as online contact information;
- A telephone number;
- A social security number;
- A persistent identifier that can be used to recognize a user over time and across different websites or online services;
- A photograph, video, or audio file, where such file contains a child's image or voice;
- Geolocation information sufficient to identify street name and name of a city or town; or
- Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described above.

When does the amended Rule go into effect? What should I do about information I collected from children prior to the effective date that was not considered personal under the original Rule but now is considered personal information under the amended Rule?

The amended Rule, which goes into effect on July 1, 2013, added four new categories of information to the definition of personal information. The amended Rule of course applies to any personal information that is collected after the effective date of the Rule. Below we address, for each new category of personal information, an operator's obligations regarding use or disclosure of previously collected information that will be deemed personal information once the amended Rule goes into effect:

If you have collected **geolocation information** and have not obtained parental consent, you must do so immediately. Although geolocation information is now a stand-alone category within the definition of personal information, the Commission has made clear that this was simply a clarification of the 1999 Rule. The definition of personal information from the 1999 Rule already covered any geolocation information that provides information precise enough to identify the name of a street and city or town. Therefore, operators are required to obtain parental consent prior to collecting such geolocation information, regardless of when such data is collected.

If you have collected **photos or videos containing a child's image or audio files with a child's voice from a child** prior to the effective date of the amended Rule, you do not need to obtain parental consent. This is consistent with the Commission's statement contained in the 1999 Statement of Basis and Purpose for the COPPA Rule that operators need not seek parental

consent for information collected prior to the effective date of the Rule. However, as a best practice, staff recommends that entities either discontinue the use or disclosure of such information after the effective date of the amended Rule or, if possible, obtain parental consent.

Under the original Rule, a **screen or user name** was only considered personal information if it revealed an individual's email address. Under the amended Rule, a screen or user name is personal information where it functions in the same manner as online contact information, which includes not only an email address, but any other "substantially similar identifier that permits direct contact with a person online." As with photos, videos, and audio, any newly-covered screen or user name collected prior to the effective date of the amended Rule is not covered by COPPA, although we encourage you as a best practice to obtain parental consent if possible. A previously-collected screen or user name is covered, however, if the operator associates new information with it after the effective date of the amended Rule.

Persistent identifiers were covered by the original Rule only where they were combined with individually identifiable information. Under the amended Rule, a persistent identifier is covered where it can be used to recognize a user over time and across different websites or online services. Consistent with the above, operators need not seek parental consent for these newly covered persistent identifiers if they were collected prior to the effective date of the Rule. However, if after the effective date of the amended Rule an operator continues to collect, or associates new information with, such a persistent identifier, such as information about a child's activities on its website or online service, this collection of information about the child's activities triggers COPPA. In this situation, the operator is required to obtain prior parental consent unless such collection falls under an exception, such as for support for the internal operations of the website or online service.

COPPA AND SCHOOLS

1. Can an educational institution consent to a website or app's collection, use or disclosure of personal information from students?

Yes. Many school districts contract with third-party website operators to offer online programs solely for the benefit of their students and for the school system - for example, homework help lines, individualized education modules, online research and organizational tools, or web-based testing services. In these cases, the schools may act as the parent's agent and can consent to the collection of kids' information on the parent's behalf. However, the school's ability to consent for the parent is limited to the educational context - where an operator collects personal information from students for the use and benefit of the school, and for no other commercial purpose. Whether the website or app can rely on the school to provide consent is addressed in FAQ M.2. FAQ M.5 provides examples of other "commercial purposes."

In order for the operator to get consent from the school, the operator must provide the school with all the notices required under COPPA. In addition, the operator, upon request from the school, must provide the school a description of the types of personal information collected; an opportunity to review the child's personal information and/or have the information deleted; and the opportunity to prevent further use or online collection of a child's personal information. As

long as the operator limits use of the child's information to the educational context authorized by the school, the operator can presume that the school's authorization is based on the school's having obtained the parent's consent. However, as a best practice, schools should consider making such notices available to parents, and consider the feasibility of allowing parents to review the personal information collected. See FAQ M.4. Schools also should ensure operators to delete children's personal information once the information is no longer needed for its educational purpose.

In addition, the school must consider its obligations under the Family Educational Rights and Privacy Act (FERPA), which gives parents certain rights with respect to their children's education records. FERPA is administered by the U.S. Department of Education. For general information on FERPA, see https://studentprivacy.ed.gov/. Schools also must comply with the Protection of Pupil Rights Amendment (PPRA), which also is administered by the Department of Education. *See* https://studentprivacy.ed.gov/.

Student data may be protected under state law, too. For example, California's Student Online Personal Information Protection Act, among other things, places restrictions on the use of K-12 students' information for targeted advertising, profiling, or onward disclosure. States such as Oklahoma, Idaho, and Arizona require educators to include express provisions in contracts with private vendors to safeguard privacy and security or to prohibit secondary uses of student data without parental consent.

2. Under what circumstances can an operator of a website or online service rely upon an educational institution to provide consent?

Where a school has contracted with an operator to collect personal information from students for the use and benefit of the school, and for no other commercial purpose, the operator is not required to obtain consent directly from parents, and can presume that the school's authorization for the collection of students' personal information is based upon the school having obtained the parents' consent. However, the operator must provide the school with full notice of its collection, use, and disclosure practices, so that the school may make an informed decision.

If, however, an operator intends to use or disclose children's personal information for its own commercial purposes in addition to the provision of services to the school, it will need to obtain parental consent. Operators may not use the personal information collected from children based on a school's consent for another commercial purpose because the scope of the school's authority to act on behalf of the parent is limited to the school context.

Where an operator gets consent from the school rather than the parent, the operator's method must be reasonably calculated, in light of available technology, to ensure that a school is actually providing consent, and not a child pretending to be a teacher, for example.

3. Who should provide consent - an individual teacher, the school administration, or the school district?

As a best practice, we recommend that schools or school districts decide whether a particular site's or service's information practices are appropriate, rather than delegating that decision to the teacher. Many schools have a process for assessing sites' and services' practices so that this task does not fall on individual teachers' shoulders.

4. When the school gives consent, what are the school's obligations regarding notifying the parent?

As a best practice, the school should consider providing parents with a notice of the websites and online services whose collection it has consented to on behalf of the parent. Schools can identify, for example, sites and services that have been approved for use district-wide or for the particular school.

In addition, the school may want to make the operators' direct notices regarding their information practices available to interested parents. Many school systems have implemented Acceptable Use Policies for Internet use (AUPs) to educate parents and students about in-school Internet use. The school could maintain this information on a website or provide a link to the information at the beginning of the school year.

5. What information should a school seek from an operator before entering into an arrangement that permits the collection, use, or disclosure of personal information from students?

In deciding whether to use online technologies with students, a school should be careful to understand how an operator will collect, use, and disclose personal information from its students. Among the questions that a school should ask potential operators are:

- What types of personal information will the operator collect from students?
- How does the operator use this personal information?
- Does the operator use or share the information for commercial purposes not related to the provision of the online services requested by the school? For instance, does it use the students' personal Information in connection with online behavioral advertising, or building user profiles for commercial purposes not related to the provision of the online service? If so, the school cannot consent on behalf of the parent.
- Does the operator enable the school to review and have deleted the personal information collected from their students? If not, the school cannot consent on behalf of the parent.
- What measures does the operator take to protect the security, confidentiality, and integrity of the personal information that it collects?
- What are the operator's data retention and deletion policies for children's personal information?

Schools also should keep in mind that under the Protection of Pupil Rights Amendment, Local Educational Agencies (LEAs) must adopt policies and must provide direct notification to parents at least annually regarding the specific or approximate dates of, and the rights of parents to opt their children out of participation in, activities involving the collection, disclosure, or use of personal information collected from students for the purpose of marketing or selling that information (or otherwise providing the information to others for that purpose).

Appendix D

CYBERSECURITY INCIDENT RESPONSE PLAN

The master copy of the IRP is stored in the Administrative Hallway fireproof room and is a confidential document.

APPENDIX F

ADDENDUM TO PRINCIPAL AGREEMENT BETWEEN

BLOUNT COUNTY BOARD OF EDUCATION AND

Contractor Name: _____

WHEREAS, the **Blount County Board of Education** (the "Board) and

_____(the "Contractor") are entering or may have entered a Principal Agreement;

WHEREAS, under the Principal Agreement, the Contractor will perform an institutional service or function for which the Board would otherwise use employees, and it has been determined that the Contractor is a school official with a legitimate educational interest in education records;

WHEREAS, it may be necessary for the Board to provide the Contractor with information contained in student education records as defined by the Family Educational Rights and Privacy Act (FERPA) in order for Contractor to perform the services outlined in the Principal Agreement;

WHEREAS, the Board desires to ensure that any student education records in Contractor's possession are used and maintained in accordance with FERPA and that the Contractor's use and maintenance of education records is under the direct control of the Board; and

WHEREAS, the Board desires to outline the Contractor's responsibilities regarding student educational records and other matters pertaining to the Contractor's use and maintenance of Data shared, created, or maintained pursuant to the Principal Agreement; and

WHEREAS, the Board and Contractor desire to enter into this **Addendum to Principal Agreement** ("Addendum") and that this Addendum be annexed, incorporated into or otherwise made a part of the Principal Agreement.

WHEREFORE

In consideration for the covenants herein and other good and valuable consideration, the receipt and sufficiency of which is acknowledged, the Parties agree as follows:

I. **Definitions.** The defined terms used in this Addendum shall have the following meaning:

a) The term "Principal Agreement" is the contract, agreement, clickwrap agreement, clickthrough agreement, "Terms of Service," or other document(s) setting form the basic terms and conditions under which the Contractor is engaged to furnish goods, materials, services, work or other consideration. This term includes all exhibits, attachments, other addenda or understandings and writings incorporated into or made a part of the Principal Agreement.

b)The term "Contractor Forms" shall mean any written contract, agreement, quotation, proposal, invoice or other written document or form of any type that Contractor has prepared and submits to the Board in connection with the Principal Agreement.

c) The term "Data" includes all Personally Identifiable Information (PIO pertaining to Board students or employees or other non-public information that (I) is provided to Contractor by the Board or (2) is collected, accessed, used, created or maintained by the Contractor in conjunction with the Principal Agreement. Data includes, but is not limited to, employee data, student data, student education records as defined by FERPA, metadata, and user content.

d) The term "Sensitive Personally Identifying Information" has the same meaning as the definition given to that term in the Alabama Data Breach Notification Act of 2018.

2. Data Security and Confidentiality.

A. *Data Ownership:* The Board will provide to Contractor the Data that Contractor attests is the minimum necessary information for Contractor to fulfill its duties as outlined in the Principal Agreement. The Contractor has a limited, nonexclusive license to such Data solely for the purpose of performing its obligations as outlined in the Principal Agreement. Any such Data is not owned by Contractor and, upon expiration or termination of the Principal Agreement, such Data shall remain the property of the Board.

B. *Data Collected or Created by Contractor:* Any Data collected, created, or maintained by the Contractor while fulfilling its duties under this Addendum and the Principal Agreement *is* subject to the terms of this Addendum.

C. *Data Use:* Contractor will use Data only for the purpose of fulfilling its duties and providing services under the Principal Agreement, for improving services under the Principal Agreement, and for no other commercial purpose.

D. *Data Confidentiality:* Contractor agrees to limit access to Data to its representatives (e.g. officers, directors, employees) who need access to the Data in order to fulfill the Contractor's duties or to provide services to the Board according to the terms of the Principal Agreement or this Addendum. In addition, the Contractor may disclose Data to authorized representatives of the Board and to anyone entitled to the Data pursuant to federal or Alabama law.

The Board understands that Contractor may rely on one or more subcontractors to perform services under the Principal Agreement. Contractor agrees to share the names of these subcontractors with the Board upon request. All subcontractors and successor entities of Contractor will be subject to the terms of this Addendum.

Contractor's obligation to maintain the confidentiality of the Data will survive the termination of the Principal Agreement and this Addendum.

E. *Security Controls:* Contractor agrees to designate an employee or employees to coordinate the Contractor's security measure to protect against a breach of security.

Contractor agrees to take appropriate administrative, technical and physical safeguards to protect the Data from any unauthorized use or disclosure not provided for in this agreement and to protect Data according to commercially reasonable standards and no less rigorously than they protect their own confidential information. This includes appropriate administrative, physical, and technical safeguards to secure Data from unauthorized access, disclosure, and use. The Contractor agrees to evaluate and adjust its security measures to account for changes in circumstances affecting the security of Data. Contractor will

conduct periodic risks assessments to identify internal and external risks of a breach of security and remediate any identified security vulnerabilities in a timely manner.

Contractor agrees to notify the Board if it stores any Data outside of the United States of America or it makes changes to its data security procedures that may impact the security of Data it maintains on behalf of the Board.

F. *Access:* Any Data held by Contractor pursuant to the Principal Agreement or this Addendum will be made available to the Board upon request by the Board.

G. *Data De-Identification:* Contractor may use de-identified Data for product development, research, or other purposes. De-identified Data will have all direct and indirect personal identifiers removed. This includes, but is not limited to, name, ID numbers, date of birth, demographic information, location information, and school ID. Furthermore, Contractor agrees not to attempt to re-identify de-identified Data and not to transfer de-identified Data to any party unless that party agrees not to attempt re-identification.

H. *Data Collection:* Contractor will only collect Data necessary to fulfill its duties as outlined in the Principal Agreement.

I. *Data Mining:* Contractor is prohibited from mining Data for any purposes other than those agreed to by the parties. Data mining or scanning of user content for the purpose of advertising or marketing to employees, students, or their parents is prohibited.

J. *Data Breach:* In the event of a data or security breach that may affect the security or confidentiality of Data maintained by Contractor on behalf of the Board, the Contractor will:

1. promptly notify the Board of the breach;
2. immediately act to close the breach;
3. take all legally required, reasonable, and customary measures to remediate the breach;
4. promptly identify any Board Data that was affected by the breach;
5. return compromised Board Data to the Board for review upon request;
6. provide information regarding the breach that can be used to communicate with affected parties;
7. provide any information regarding the breach to the Board and/or persons whose Data was breached that is required by law;
8. provide information, records, and witnesses needed to respond to any government investigation or litigation regarding the breach or to comply with any legal requirements to inform affected persons of the breach.

Contractor shall defend, indemnify and hold the Board and its members, officers, employees, contractors or agents harmless from all claims, liability, injury, loss, cost, damage and expense (including, but not limited to, reasonable attorneys' fees and expenses) with respect to a data or security breach that affects the Data maintained by Contractor on behalf of the Board.

If the Board determines that a breach of security may have occurred with regard to any "Sensitive Personally Identifying Information" maintained by the Contractor pursuant to this Addendum or the Principal Agreement, the Contractor will provide the Board with any information in the Contractor's possession that the Board needs to comply with its

obligations under any applicable data breach law, including Information necessary to conduct a good faith and prompt investigation that includes all of the following:

I. An assessment of the nature and scope of the breach.

2. Identification of any sensitive personally identifying Information that may have been involved in the breach and the identity of any individuals to whom that information relates.

3. A determination of whether the sensitive personally identifying Information has been acquired or is reasonably believed to have been acquired by an unauthorized person, and is reasonably likely to cause substantial harm to the individuals to whom the information relates.

4. Identification and implementation of measures to restore the security and confidentiality of the systems compromised in the breach.

K. *Data Transfer or Destruction:* Once the Data is no longer needed for purposes of fulfilling the Contractor's duties under the Principal Agreement or upon the termination or expiration of the Principal Agreement, the Contractor must destroy any Data in its possession in a manner that utilizes proper disposal methods or return the records to the Board. Before destroying or disposing of the Data, Contractor must contact the Board and provide the Board with an opportunity to obtain a copy of the Data

In general, proper disposal methods may include, but are not limited to:

1. For Data in paper records: shredding, burning, pulping, or pulverizing the records so that PII is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.

2. For Data on electronic media; clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding)

3. Other methods of disposal also may be appropriate, depending on the circumstances.

L. *Modification of Terms of Service:* Contractor will not change how Data are collected, used or shared under the terms of this Addendum or the Principal Agreement in any way without advance notice to and consent from the Board.

4. **COPPA Compliance.** Contractor is solely responsible for ensuring its compliance with the Children's Online Privacy Protection Act (COPPA) if applicable. In addition, the Board is not required to obtain specific, verifiable parental consent in order to share student Data with Contractor or to utilize Contractor's services, programs, or products.

5. **Conflicting Provisions.** If any provisions, terms or conditions in this Addendum conflict or are inconsistent with those in Principal Agreement or in any Contractor Forms, the terms herein supersede, control and take precedence over the conflicting provisions in the Principal Agreement or Contractor Forms.

6. **Term of Addendum.** The term of this Addendum shall run concurrently with that of the Principal Agreement. It shall remain in full force and effect if the Parties amend, extend, or supplement the Principal Agreement, whether or not any of those expressly acknowledge, reference or incorporate this Addendum at the time of any such amendment, extension or supplementation.

7. **Termination.** Contractor's failure with the provisions of this Addendum will be considered a material breach of the Principal Agreement. In such event, the Board may terminate the Principal Agreement effective immediately upon written notice to the Contractor without further liability or obligation to Contractor.

8. **Governing Law.** Contractor agrees that the meaning, legal effect, and enforcement of terms and provisions of this Addendum, and the resolution of any disputes arising thereunder or relating thereto shall be governed by the laws of the State of Alabama.

9. **Modification.** No official, agent, employee, or representative of the Board is authorized to modify, waive or suspend the operation of this Addendum or any of its terms or provisions without the express approval of the Board.

DATED this_ day of _____,20_.

Contractor/Company Name: **BLOUNT COUNTY BOARD OF EDUCATION**

By: _____ By: _____

Its: _____ Its: _____

GLOSSARY

- COPPA- Children's Online Privacy Protection Rule.
- Directory Information - Information such as name, date and place of birth, grade level, etc. For a complete list of directory information see the current Student Handbook. FERPA allows parents the choice to not allow the release of directory information.
- FERPA- Family Educational Rights and Privacy Act.
- MOA - Memorandum of Agreement signed by Resource Provider and Superintendent.
- Online Resources - Internet based programs, Apps, Applications, Games, etc.
- PII Data - Personally, identifiable information is any information/data/educational records that could potentially be identified to a specific individual.