

IV. General Administration

4.1 *Security/Access to Schools*

- 4.1.1 Security Measures Authorized - The Superintendent, principals, and facility administrators are authorized to take reasonable and lawful measures to protect against personal injury, trespass, vandalism, theft, and like threats to personal safety, property damage, and financial loss to or on Board property or at school functions and activities. The Superintendent should be made aware of any extraordinary or special measures that may be proposed in anticipation of or in response to any unusual security threat or risk (e.g., unusual surveillance, assignment of additional security personnel).
- 4.1.2 Access Restrictions Authorized - The Superintendent, principals, and facility administrators are authorized to regulate and restrict access to Board schools, buildings, and facilities in order to maintain appropriate security, minimize disruption and distraction within the learning environment, or to avoid a potential risk of harm to a student or employee. To that end, the Superintendent, principals, and facility administrators are authorized to implement building-level requirements and procedures governing access to Board owned or controlled buildings, grounds, property, events, and activities by school and non-school personnel, including family members and relatives, vendors, attorneys, and other visitors, and to adopt “check-in” and “check-out” requirements and procedures for students and employees.
- 4.1.3 Adult Sex Offenders – Adult Sex offenders who have been convicted of a sex offense involving a minor must:
- a. Notify the principal of the school to request permission before entering school property or attending the PK-12 school activity; the principal may deny an offender’s request to come onto the school campus;
 - b. Immediately report to the principal of the school upon entering the property or arriving at the PK-12 school activity;
 - c. Cooperate with any efforts undertaken by the principal of the school to discreetly monitor their presence on school property or at the PK-12 school activity. For the purposes of this subsection, a PK-12 school activity is an activity sponsored by a school in which students in grades PK-12 are the primary intended participants or for who students in grades PK-12 are the primary intended audience including, but not limited to, school instructional time, after school care, after school tutoring, athletic events, field trips, school plays, or assemblies. Adult sex offenders have a duty to comply with this policy, and it shall not be construed as imposing

an affirmative duty of any kind on the school principal, his designee, or any other employee, agent, or representative of the school or school system; and

- d. Notify the Superintendent or his designee to request permission before attending any meeting or function held at the central office of the Board of Education. The Superintendent or his designee may deny an offender's request to come to the central office. The offender shall immediately report to the Superintendent or his designee upon entering the central office..

[Reference: ALA. CODE §15-20A-17]

4.2 *Safe School Policy (Drugs, Alcohol, Tobacco, and Weapons)*

4.2.1 Prohibition on the Possession of Firearms – The possession of a firearm in a school building, on school grounds, on Board property, on school buses, or at school-sponsored functions is prohibited except for authorized law enforcement personnel and as provided by law. For purposes of this policy, the term “firearm” has the same definition as is found in 18 U.S.C. §921.

- a. *Penalties for violations* – In addition to any criminal penalties that may be imposed, the following penalties will be imposed for unauthorized possession of firearms:
 1. *Students* – Students will be expelled for a period of one year. The expulsion requirement may be modified in writing by the Board upon recommendation of the Superintendent on a case-by-case basis. Students who are expelled for firearm possession may not attend regular school classes, but may be permitted to attend alternative schools or education programs established by the Board. Discipline of students with disabilities who violate the firearm possession policy will be determined on a case-by-case basis in accordance with federal and state law. Parents of students who violate this policy will also be notified by the principal of violations.
 2. *Employees* – Employees will be subject to adverse personnel action, which may include termination.
 3. *Other Persons* – Other persons may be denied re-entry to school property.
- b. *Notification of Law Enforcement* – The appropriate law enforcement authority, which may include the city police, county sheriff, and the local district attorney, will be notified by the principal of violations of this policy.

[Reference: ALA. CODE §16-1-24.1, 24.3 (1975); ALA. ADMIN. CODE 290-3-1-.02; Federal Gun Free Schools Act, 20 U.S.C. 7175; Federal Gun Free School Zone Act of 1995, 20 U.S.C. §922(q)]

4.2.2 Prohibition on the Possession of Weapons - The possession of a deadly weapon or dangerous instrument in a school building, on school grounds, on school property, on school buses, or at school-sponsored functions is prohibited except for authorized law enforcement personnel. For purposes of this policy, the terms “deadly weapon” and “dangerous instruments” include but are not limited to explosives, incendiary devices, projectiles, knives with a blade length of more than two (2) inches, devices designed to expel projectiles at a high rate of speed, any device so classified under state or federal law, and any device either used or intended to be used in a such manner as to inflict bodily harm, provided that the terms “deadly weapon” and “dangerous instruments” will exclude, to the extent permitted by law, devices and equipment that are used for the purpose of and in connection with school or Board sanctioned educational, team, or competitive activities.

- a. *Penalties for Violations* - In addition to any criminal penalties that may be imposed, the following penalties will be imposed for unauthorized possession of deadly weapons or dangerous instruments:
 1. *Students* - Students will be disciplined in accordance with the Board’s Code of Student Conduct.
 2. *Employees* - Employees will be subject to adverse personnel action, which may include termination.
 3. *Other Persons* - Other persons may be denied re-entry to school property.
- b. *Notification of Law Enforcement* - The appropriate law enforcement authority, which may include the city police, county sheriff, and the local district attorney, will be notified by the principal of the violations of this policy.

[Reference: ALA. CODE §16-1-24.1 (1975); ALA. ADMIN CODE 290-3-1-.02(1)(b)]

4.2.3 Illegal Drugs and Alcohol - The use, possession, distribution, and sale of alcohol and the illegal use, possession, distribution, and sale of drugs in a school building, on school grounds, on Board property, on school buses, or at school-sponsored functions is prohibited.

- a. *Penalties for Violations* - In addition to any criminal penalties that may be imposed, the following penalties will be imposed for unauthorized possession of illegal drugs or alcohol:

1. *Students* – Students will be disciplined in accordance with the Board’s Code of Student Conduct.
 2. *Employees* – Employees will be subject to adverse personnel action, which may include termination.
 3. *Other persons* – Other persons may be denied re-entry to school property.
- b. *Notification of Law Enforcement* – The principal shall notify the appropriate law enforcement officials when a person violates Board policy concerning illegal drugs and alcohol. These officials may include the School Resource Officer, Juvenile Probation Officer, county sheriff or local district attorney. If any criminal charge is warranted, the principal is authorized to sign the appropriate warrant. If that person is a student in any Coosa County public school, he (she) shall immediately be suspended from attending regular classes and a hearing shall be scheduled by the Superintendent. The decision to suspend or initiate criminal charges against a student shall include a review and consideration of the student’s exceptional status, if applicable.

[Reference: ALA CODE §16-1-24.1 (1975); Ala. Admin. Code 290-3-1-.02(1)(b)]

- 4.2.4 Tobacco and E-Cigarettes – The use of tobacco products and electronic nicotine delivery system (“e-cigarettes”) and the illegal possession, distribution, and sale of tobacco and e-cigarette products in a school building, on school grounds, on school buses, or any Board property, or at school-sponsored functions is prohibited.

E-cigarette product is defined as an electronic device used to deliver nicotine or other substance, chemical or flavoring to the person inhaling from the device. The following are examples of prohibited devices: electronic cigarettes, vape pens, hookah pens, e-hookahs, vape pipes and any similar type of device designed to deliver nicotine, flavor and other chemicals or substances via inhalation.

- a. *Penalties for Violations*
1. *Students* – Students who violate the tobacco and e-cigarette prohibition will be disciplined in accordance with the Board’s Code of Student Conduct.

2. *Employees* – Employees who violate the tobacco and e-cigarette prohibition will be subject to adverse personnel action, which may include termination.
 3. *Other Persons* - Other persons who violate the tobacco and e-cigarette prohibition may be denied re-entry to school property.
- b. *Parental Notification* - Parents and guardians may be notified of actual or suspected violations of the tobacco and e-cigarette prohibition whether or not the student is charged with a violation of Board policy, which includes the Code of Student Conduct.

[Reference: ALA. CODE §16-1-24.1 (1975); ALA. ADMIN. CODE 290-3-1-.02(1)(b)]

- 4.2.5 Searches - Law enforcement agencies are permitted to make periodic visits to all schools to detect the presence of illegal drugs or weapons and may use any lawful means at their disposal to detect the presence of such substances. The visits will be unannounced to anyone except the Superintendent and the Principal.

[Reference: ALA. CODE §16-1-24.1 (1975); ALA. ADMIN. CODE 290-3-1-.02(1)(b)]

- 4.2.6 Drug and Alcohol Free Environment - All students, employees, volunteers, parents, visitors, and other persons are prohibited from possessing, using, consuming, manufacturing, or distributing illegal controlled substances and alcohol while on Board property or while attending any Board sponsored or sanctioned event, program, activity, or function. Persons who are intoxicated or impaired by the use, consumption, or ingestion of any illegal controlled substance or alcohol are not permitted to be on school property, or to attend or participate in any Board sponsored or sanctioned event, program, activity, or function.

[Reference: ALA. CODE §16-1-24.1, 25-5-330 (1975)]

- 4.2.7 Adoption of Statutory Penalties and Consequences - Persons who violate the Board's prohibition of firearms, weapons, illegal drugs, or alcohol will be subject to all notification, referral, suspension, placement, re-admission, and other provisions set forth in Alabama law.

[Reference: ALA. CODE §16-1-24.1 and 24.3 (1975)]

- 4.2.8 Accident – The Board of Education shall require accidents which require more than general first aid occurring on school grounds or in school facilities to be reported immediately to the principal's office. Reasonable efforts will be made to contact the injured student's parents or legal guardian in case of accident or injury which requires more than general first aid, whenever possible. Any student suffering an accident or injury which requires more than general first aid shall not be left

unattended. The teacher or other staff member who was supervising the student at the time of the accident or injury, if the injury required more than general first aid, shall provide a written report of all circumstances surrounding the accident to the principal and Superintendent.

4.3 *Accreditation*

The Board will implement and adhere to such accreditation policies, principles, standards, and procedures as may be established or required by AdvanceED and the Division of the Southern Association of Colleges and Schools Council on Accreditation and School Improvement (“SACS/CASI”) as a condition to receiving or maintaining accreditation.

4.4 *Use of Board Property*

4.4.1 Annual Reports – Annual reports shall be provided to the Board relative to maintenance needs, safety, utility and attractiveness of school plants and grounds within the school district.

4.4.2 Equipment, Supplies, Materials, Vehicles - Equipment, supplies, materials, vehicles, and other movable or consumable property owned by or under lease to the Board may not be used by or made available to persons or entities for private or personal use, benefit, or consumption, or for any non-Board related use or purpose. Such property may not be removed from Board premises except as necessary to serve a school or Board-related function or purpose, and with the knowledge and approval of the appropriate supervisor, administrator, or the Superintendent.

4.4.3 Use of Board Facilities - Schools and other Board owned or controlled facilities may be made available for use by sanctioned or generally recognized school support organizations if the use of the facility will not disrupt school operations or be inconsistent with the purpose and mission of the school system, and if adequate advance provision is made for security, supervision, maintenance, damage prevention, post-event clean up, liability insurance, and other risk management measures appropriate to the proposed use. Use of Board facilities for non-school organizations may be approved if the foregoing conditions are satisfied and a rental contract (or the equivalent thereof) that includes a reasonable fee or rental charge and other appropriate terms and conditions is approved by the Superintendent and/or his designee. The Superintendent is authorized to develop a schedule of reasonable fees for the use of Board facilities and property by individuals, groups, or organizations.

4.5 *Naming Board Facilities*

When naming schools, school facilities, buildings on school grounds and/or any structure on property belonging to the Coosa County Board of Education, the decision will be left to

the discretion of the Board. Requests to name or rename any board property, including buildings, portions of a building, and other Board facilities should be submitted to the Superintendent with a justification giving the rationale for the name to be selected. Under most circumstances, the Board will name schools in order to reflect their location and relationship to the communities served by the school system.

4.6 *Complaints and Grievances*

- 4.6.1 General Complaints (Grievances) – Subject to the limitations set forth below, any employee or member of the public may present to the Board a concern, complaint, grievance, or request for corrective action regarding any aspect of school system operations. Before requesting corrective action or relief from the Superintendent or the Board, persons with such complaints, grievances, or requests should present them for resolution to the employee, supervisor, or administrator at the lowest administrative level who has the authority and ability to address the problem or to implement the requested action. The Superintendent is authorized to develop specific procedures that will provide for fair consideration and orderly review of complaints and grievances. Such procedures may not unreasonably burden or delay the presentation or processing of such matters, and will be subject to Board review, modification, and approval.
- 4.6.2 Limitations Regarding Availability and Application of General Complaint/ Grievance Policy – The general complaint/ grievance policy and any procedures adopted there under do not apply to specific complaint or grievance policies and procedures that are established by Board policy or law for application to special factual or legal circumstances (e.g., sexual harassment grievance procedures; review of personnel matters under the Alabama Students First Act or fair dismissal laws; “due process” hearings provided under the Individuals with Disabilities Education Act). In such instances, the specific statutory, regulatory, or policy-based process is the applicable procedure. The general complaint/ grievance procedures that are authorized under the terms of this policy may not be invoked for the purpose of challenging or seeking review or reconsideration of adverse personnel decisions that have received final Board approval. A grievance may be based on an alleged misapplication of Board policies, regulations, or procedures, but may not be used to challenge the Board’s exercise of its discretion to adopt, approve, modify, or repeal a policy, regulation, or procedure or on its failure to exercise such discretion (e.g., adoption of a school calendar, compensation policies, etc.)
- 4.6.3 Student Complaints and Grievances – Complaints, grievances, and requests for corrective action may be brought to the attention of the Board by or on behalf of students with respect to academic, athletic, extracurricular, or other non-disciplinary matters, issues, and concerns only after reasonable efforts to resolve the matter at the school and administrative levels have been exhausted and in accordance specified in the Code of Conduct. The Superintendent is authorized to develop specific procedures that will provide for fair consideration and orderly review of such complaints and grievances. Such procedures will not unreasonably

burden or delay the presentation or processing of the complaint or grievance and will be subject to review and approval by the Board. Administrative judgments concerning academic or curricular matters or participation in extracurricular activities may be set aside by the Board only upon a showing that the action or decision in question is arbitrary and capricious, fundamentally unfair, or that it violates Board policy or the student's legal rights.

- 4.6.4 Student Disciplinary Matters – The Board may consider appeals of student disciplinary decisions or actions in accordance with standards and procedures specified in the Code of Conduct.

4.7 *Americans with Disabilities Act Complaint Procedure*

- 4.7.1 Complaint Criteria - Persons who believe that they have been discriminated against on the basis of disability in the provision of services, activities, programs or benefits covered by Title II of the Americans with Disabilities Act may file a written complaint with the ADA Coordinator.
- 4.7.2 Complaint Form - The complaint should be in writing and contain information about the alleged discrimination including the name, address, phone number of complaining party and location, date, and description of the problem. Alternative means of filing complaints, such as personal interview or a tape recording of the complaint, will be made available for persons with disabilities upon request.
- 4.7.3 Complaint Process - The complaint should be submitted to the ADA Coordinator as soon as possible, but no later than thirty (30) days after the alleged violation. The ADA Coordinator will meet with the complaining party to discuss the complaint and possible resolutions. Within fifteen (15) calendar days of the meeting, the ADA Coordinator will respond in writing, and where appropriate, in a format accessible to the complaining party, such as large print, Braille, or audio tape. The response will explain the position of the Board and offer options for substantive resolution of the complaint.
- 4.7.4 Appeal Procedure - If the response by the ADA Coordinator does not satisfactorily resolve the issue, the complaining party may appeal the decision within fifteen (15) calendar days after receipt of the response to the Superintendent. Within fifteen (15) calendar days, the Superintendent will respond in writing and where appropriate, in a format accessible to the complainant, with a final resolution of the complaint.
- 4.7.5 Records Retention - All written complaints received by the ADA Coordinator, appeals to the Superintendent, and records relating thereto will be retained by the Board for at least three years.
- 4.7.6 Additional Procedures Authorized- The Superintendent is authorized to develop such procedures as are necessary to implement this policy

4.8 *Risk Management*

The Board may obtain such liability and other forms of insurance or enter into such risk management agreements, pools, cooperatives, and like arrangements, agreements, or undertakings as it deems necessary and appropriate to meet legal requirements or to protect the Board, its employees, or its property from risk of loss.

4.9 *Emergency Closing of Schools*

4.9.1 Authority of Superintendent to Close Schools - The Superintendent or his designee is authorized to close schools if such action is warranted by weather conditions or other circumstances that pose a risk to the safety and welfare of students and employees, or that render meaningful instruction impossible (e.g., loss of power or other utility services). The Superintendent or his designee is also authorized to declare an early dismissal, late start or closure of schools for any other reasonable event.

4.9.2 Make-Up Dates - To the extent not provided for in the school calendar, any days lost by reasons of an emergency closing will be made up and a revised school calendar approved, if necessary, to reflect any extension or adjustment of the school year required by such action.

4.10 *Technology Use and Internet Safety*

4.10.1 Introduction - It is the policy of Coosa County Board of Education to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

4.10.2 Access to Inappropriate Material - To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

4.10.3 Inappropriate Network Usage - To the extent practical, steps shall be taken to promote the safety and security of users of the Coosa County Board of Education

online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by the Children’s Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called ‘hacking’, and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

4.10.4 Education, Supervision, Monitoring - It shall be the responsibility of all employees of the Coosa County Board of Education to educate, supervise and monitor students’ appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children’s Internet Protection Act, the Neighborhood Children’s Internet Protection Act, and the Protecting Children in the 21st Century Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the technology director or designated representatives. The school technology committee member or designated representatives will provide age-appropriate training for students who use the Board’s Internet facilities. The training provided will be designed to promote the Board’s commitment to:

- a. The standards and acceptable use of Internet services as set forth in the Board’s Internet Safety Policy;
- b. Student safety with regard to:
 - 1. safety on the Internet;
 - 2. appropriate behavior while on online, on social networking Web sites, and in chat rooms; and
 - 3. cyber bullying awareness and response.
- c. Compliance with the E-rate requirements of the Children’s Internet Protection Act (“CIPA”).
- d. Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the Board’s acceptable use policies.

4.11 *Data Governance and Use*

4.11.1 Purpose

- a. Implement standards and procedures to effectively manage and provide necessary access to information while protecting the confidentiality, integrity and availability of the information.

All relevant provisions in the Responsibility Use Policies (RUP) and

Technology Standard Operating Procedures (TSOP) are also applicable.

- b. Define information classification and safeguards.
- c. Establish mechanisms for delegating authority for information access.

4.11.2 Scope

- a. These measures apply only to information in a digital format. Additional policies and laws apply to information in paper format, but no electronic control measures are needed.
- b. These measures apply to all Board employees, contract workers, visitors, students, and all information used to conduct operations of the system.
- c. These measures apply to information accessed from any location.

4.11.3 Regulatory Compliance - The Coosa County Board of Education will abide by any law, statutory, regulatory, or contractual obligations affecting its information systems. The Board's data governance policy and procedures are informed by the following laws, rules, and standards, among others:

- *FERPA* - The Family Educational Rights and Privacy Act, applies to all institutions that are recipients of federal aid administered by the Secretary of Education. This regulation protects student information and accords students' specific rights with respect to their data. For more information: <http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html><http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
- *ALABAMA RECORDS DISPOSITION AUTHORITY* – ALA. CODE §41-13-23 authorized the Alabama Department of Archives and History to publish rules for Local Government Records Destruction. For more information: <http://www.archives.alabama.gov/officials/localrda.html>
<http://www.archives.alabama.gov/officials/localrda.html>
- *COPPA* - The Children's Online Privacy Protection Act regulates organizations that collect or store information about children under age 13. Parental permission is required to gather certain information. For more information: <http://www.coppa.org>[http://www.coppa.org/](http://www.coppa.org)

4.11.4 Committee Members - The Data Governance Committee ("DGC") for the Coosa County Board of Education will consist of representation from all schools.

4.11.5 Guiding Principles

- a. The Superintendent and/or his designees shall determine appropriate access permissions based on policies, applicable laws and best practices.
- b. Data Users granted “create” and/or “update” privileges are responsible for their actions while using these privileges. That is, all schools or other facilities are responsible for the data they create, update, and/or delete.
- c. Any individual granted access to data is responsible for the ethical usage of that data. Access will be used only in accordance with the authority delegated to the individual to conduct school related operations.
- d. Authorized users should safeguard the data they are entrusted with.
- e. These principles apply to data regardless of location. Users who transfer or transport data “off-campus” for any reason should comply with all data security measures prior to transporting or transferring the data.
- f. The DGC is responsible for reviewing this policy annually and communicating the changes to all involved parties. When requested or necessary, the DGC will provide guidance and input to the appropriate personnel (Authorized Requestors, Technology Office personnel, administrators, etc.) on matters concerning this policy.

4.11.6 Access Coordination

- a. Central Office Staff and county administrators will assist in classifying data sensitivity levels for their areas of expertise and in identifying which employees require access to which information in order to perform their duties.
- b. The District Technology Coordinator will designate individuals within the Technology Office to implement access to systems and data based on the restrictions and permissions determined by the Authorized Requestors using the technical tools and resources available.
- c. Central Office Department heads, supervisors, area specialists, and principals will train all employees under their supervision concerning data security.
- d. The local school principal and/or designee should notify the Technology Office of personnel changes in the school that affect access to information

(new hires, leaves, transfers, name changes, retirements, etc.). This notification should be done in a timely manner so that access can be established and/or terminated effectively.

e. Information Classification Levels

1. Personally Identifiable Information (**PII**)

- i. Personally Identifiable Information is information about an individual maintained by an agency that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records.
- ii. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information also qualifies as PII.
- iii. Unauthorized or improper disclosure, modification, or destruction of this information may violate state and federal laws and/or result in civil and criminal penalties.

2. Confidential Information (**CI**)

- i. 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 must be restricted to those with a legitimate business need for access.
- ii. Examples of Confidential Information may include: personnel information, key financial information, proprietary information of commercial agencies, system access passwords and information file encryption keys.
- iii. Unauthorized or improper disclosure of this information to individuals without a business need for access may violate laws and regulations. Decisions about the provision of access to this information should be cleared through the Authorized Requestor

3. Internal Information

- i. Internal Information is intended for unrestricted use within the Coosa County School System, and in some cases within affiliated organizations. This type of information is already widely distributed within the Coosa County School System, or could be distributed within the organization without advance permission from the information owner.
 - ii. Examples of Internal Information may include: personnel directories and internal policies and procedures.
 - iii. Any information not explicitly classified as PII, CI or PI will, by default, be classified as Internal Information.
 - iv. Unauthorized disclosure of this information to individuals outside of the Coosa County School System may not be appropriate due to legal or contractual provisions.
4. Public Information (**PI**)
 - i. Public Information is information that is targeted for general public use. Examples include Internet website content for general viewing, press releases, newsletters, etc.
5. Employee Directory Information
 - i. The following items are defined as employee directory information and may be released and used as directory information unless an exception is noted beside the item below.
 - ii. Employee Name
 - iii. Employee Number (excluding social security numbers)
 - iv. Address and Telephone Listing - May not be listed in a public directory or shared publicly without specific permission. May be used in a local school directory for internal use. May be used with third-parties to provide Board provided services (For example, but not limited to: telephone calling alerting system, texting alerting system, substitute placement program, time and attendance program)

- v. Electronic mail address
- vi. Photograph
- vii. HQT Status - As needed to comply with Federal reporting requirements
- viii. Degree/Certification
- ix. Salary Schedule
- x. Job Position

f. Compliance

- 1. Users are expected to respect the confidentiality and privacy of individuals whose records they access; to observe any restrictions that apply to data; and to abide by applicable laws, policies, procedures and guidelines with respect to access, use, or disclosure of information. The unauthorized use, storage, disclosure, or distribution of data in any medium is expressly forbidden; as is the access or use of any data for one's own personal gain or profit, for the personal gain or profit of others, or to satisfy one's personal curiosity or that of others.
- 2. Each Board employee should be familiar with the Data Governance and Use Policy and these measures as they relate to his or her position and job duties.
- 3. Employees, including Authorized Users, should notify the Technology Office prior to installing any program or granting access to anyone within any program to data.
- 4. Violations of these compliance measures may result in loss of data access privileges, administrative actions, and/or personal civil and/or criminal liability.

g. Implementation of Controls and Protections and Physical Security

- 1. Shared Responsibilities

2. The Technology Office will work with Authorized Requestors to implement access controls and protections for data stored in managed systems such as INOW, SETS, network drives, etc.
3. Board employees, including Authorized Requestors, shall not select or purchase software programs that will utilize or expose PII without first consulting the Technology Office to determine whether or not adequate controls are available within the application to protect that data. (The exception to this would be any software program purchased or utilized by the Alabama State Department of Education. In this case, the Alabama State Department of Education shall assume all security responsibility for data it accesses or receives from the Coosa County Board of Education.)
4. The Technology Office staff and/or the Authorized Requestor will provide professional development and instructions for employees on how to properly access data to which they have rights, when necessary. However, providing these instructions to employees will be the shared responsibility of the supervisor(s) of the Authorized User(s) and the Technology Office.
5. Technical controls and monitoring cannot ensure that unauthorized access never occurs. Therefore, it is the shared responsibility of all employees to cooperatively support the effectiveness of the established technical controls through their actions.

h. Authorized Requestors

1. Authorized Requestors should be knowledgeable in all policies, laws, rules, and best practices relative to the data for which they are granting access; including, but not limited to FERPA, HIPAA, etc.
2. Authorized Requestors should inform appropriate Technology Office Personnel about information they will need to use and store in order to allow the Technology Office to determine the best physical and/or logical controls available to protect the data.
3. This shall include:
 - i. Which data should be classified as PII
 - ii. Where that data resides (which software program(s) and servers)

- i. Who should have access to that data (**Authorized Users**)
 - iv. What level of control the Authorized User should have to that data (i.e. read only, read/write, print, etc.)
3. Location of Data and Physical Security
- i. PII and CI data shall be stored on servers/computers which are subject to network/workstation controls and permissions.
 - ii. Serving devices (servers) storing sensitive information shall be operated by professional network system administrators, in compliance with all security and administration standards and policies, and shall remain under the oversight of the Technology Office.
 - iii. Persons who must take PII and CI data out of the protected network environment (transport data on a laptop, mobile device, etc.) should obtain the permission of their supervisor prior to doing so. Permission to do so will be granted only when absolutely necessary. The user responsible for the device shall take proper care to isolate and protect files containing sensitive information from inadvertent or unauthorized access (passwords, PINS, encryption, etc.).
 - iv. Storage of PII and CI on laptops, mobile devices, and devices that are not used or configured to operate as servers is prohibited, unless such information is encrypted. Assistance for encryption may be requested from the Technology Office. There may also be additional costs involved for software and hardware.
 - v. District staff who must print reports that contain PII or CI shall keep this material in a secure location, such as a vault, locked file cabinet, etc. In addition, all printed material containing PII or CI documentation shall be shredded when no longer in use.
 - vi. No PII or CI is authorized to be stored on personally owned equipment.
- i. Disposal of Hardware containing System Data

1. Prior to disposal of any computer, the user will follow the computer recycling procedures outlined in the Coosa County Policy Manual.
2. All schools and departments which purchase or lease copy machines or multifunction printers should maintain procedures for the destruction of data on the device's hard drive or the destruction of the hard drive itself prior to disposing of the copier or MFP or its return to the leasing agency.

j. Application of Network and Computer Access Permissions

1. The Technology Office Staff shall implement network protection measures including, but not limited to:
 2. Maintaining firewall protection access to the network and/or workstations.
 3. Protecting the network from unauthorized access through wireless devices or tapping of wired media, including establishing 'guest' wireless networks with limited network permissions.
 4. Implementing virus and malware security measures.
 5. Application of Security Patches.
 6. Establishing and maintaining password controls on access to the network workstations, and other data depositories.
 7. Categorizing and/or re-classifying data elements and views.
 8. Granting selective access to data as directed by Authorized Requestors.
 9. Documenting any deviation from mandatory requirements and implementing adequate compensating control(s).
10. Transfer of Data to External Service Provider
11. Student directory information may be transferred to an external service provider, such as an online website that teachers wish students to use for educational purposes, provided that:

- i. The teacher notifies the Technology Office about the use of the site so it may be added to the Board site that notifies parents about sites the Board uses.
 - ii. The Board notifies parents about their right to restrict their child's data from being shared with such sites annually via the Code of Conduct/RUP.
- k. No PII data, CI data, or FERPA protected educational records will be transferred to an external service provider without prior approval of the DGC. (The exception to this would be the Alabama State Department of Education.)
- l. No school or department should enter into a contract for the use of any program that requires the import of Board data without first consulting and receiving approval from the DGC.
- m. The DGC will determine which type of agreement should be required of the service provider and assist in ensuring these requirements are met prior to any data transfer. Examples of agreement types are:
 - 1. Provider Terms of Use - Acceptable as Provided
 - 2. Contract
 - 3. Designating the service provider as an "Official" as defined in FERPA
 - 4. Memorandum of Understanding
 - 5. Memorandum of Agreement
 - 6. Non-Disclosure Agreement
 - 7. Reporting Security Breaches
- n. All employees should timely report suspected or actual breaches of data security to their immediate administrator or technology coordinator whether due to inappropriate actions, carelessness, loss/theft of devices, failures of technical security measures, or any other intentional or unintentional act(s) that led to the breach.
- o. Data Governance Training

1. Principals and Central Office Administrators will receive refresher training on FERPA and other data security procedures annually at principals meetings.
2. Principals and Central Office Administrators shall contact the Technology Coordinator when in doubt about how to handle data information.
3. Principals and Central Office Administrators will be kept aware of emerging issues pertaining to data security.
4. Principals, Central Office Administrators and Department Heads should educate their staff on data governance and technology policies.

p. Data Quality Controls

1. Employees whose responsibilities include entering, maintaining, or deleting data shall provide data that is accurate, timely, confidential and complete. This includes, but is not limited to: school registrars, counselors, special education staff, and CNP staff handling free and reduced lunch data.
2. All employees shall enter data relevant to their area accurately and in a timely manner.
3. School administrators shall enter discipline information accurately and in a timely manner.

q. Supervisory Responsibilities

1. It is the responsibility of all Supervisors (principals, department, and central office) to set expectations for data quality and to evaluate their staff's performance relative to these expectations.
2. Supervisors should immediately report incidents where data quality does not meet standards to their superior and to any other relevant department, including the State Department of Education, if applicable.

r. Student Information Systems – Application Access Roles and Permissions

1. Any software system owned or managed by the Board which is used to store, process, or analyze student educational records as defined by FERPA or used to store PII or CI shall be subject to strict security measures. Examples of these systems are:
2. Information Now – General student information system
3. SetsWeb – Special Education information system
4. CNP Software – Child nutrition information system
5. Accounting and Payroll Software

Administrators with supervisory responsibilities over the Board's Student Information Systems shall determine the appropriate access rights to the data and evaluate compliance with these roles and permissions. Principals and department heads will be consulted by the appropriate administrator as needed in determining access level permissions needed at the school level for these systems.

6. School Level Information Applications
 - i. Any software system owned and/or managed by the School which is used to store, process, or analyze student educational records as defined by FERPA or used to store PI data or CI data shall be subject to strict security measures.
 - ii. Principals will determine appropriate roles and access to the data and will evaluate compliance with these roles and permissions. Supervisory personnel will be consulted as needed in determining access level permissions needed at the school level for these systems.

4.12 *Political Activity*

Board employees may participate in political activities to the full extent permitted by the United States Constitution and federal and state laws securing the right to engage in such activities, subject to the following restrictions:

- a. Employees may not appropriate Board property or resources for use in political campaigns, and may not engage in partisan political activities (including but not limited to the distribution of campaign material or literature) during regular school or duty hours or at Board-sponsored or sanctioned events, functions, or at activities at which the employee is on duty or assigned official responsibilities.
- b. Employees may not represent their political beliefs or positions on political matters to be those of the Board or other Board officials, or to falsely assert or imply that their political activities or positions are endorsed by or undertaken in the name of the Board or other Board officials;
- c. Employees may not invite or allow announced candidates for political office to address student groups except when such candidates are participating in a forum or like format that is designed to provide all candidates the opportunity to participate. Such forums may be conducted only for appropriate age groups, and with the advance approval of the school principal and the Superintendent.
- d. Political signs may not be placed on schools or school board property. Campaign literature and other material may not be distributed on Board property during the regular school or work day, and may not be distributed at school or Board-sponsored events or activities in a manner that impedes the normal and safe movement of pedestrian or vehicular traffic, that creates any other safety hazard or risk, or that disturbs or disrupts the function, activity, or event.

4.13 *Copyright Restrictions*

It is the policy of the Board to abide by and enforce at every school and work site all copyright laws and regulations, in all formats, including electronic-based works or processes.

4.14 *Service Animals In Schools*

The Board acknowledges its responsibility to permit students and/or adults with disabilities to be accompanied by a “service animal” in its school buildings, in classrooms, and at school functions, as required by the Americans with Disabilities Act, 28 CFR Part 35. A “service animal” is an animal that has been individually trained to do work or perform tasks for the benefit of an individual with a disability.

4.15 *State Law*

If the Coosa County Board of Education has not adopted a policy required by any future state law requiring such a policy, the Board adopts as its policy the state law requiring such policy.

4.16 *Conflicts of Interest (Adopted 7/14/2016)*

Generally, a conflict of interest exists when a board member, board employee, or agent of the board participates in a matter that is likely to have a direct effect on his or her personal and financial interests. A financial interest may include, but is not limited to, stock ownership, partnership, trustee relationship, employment, potential employment, or a business relationship with an applicant, vendor, or entity. A board member, board employee, or agent of the board may not participate in his or her official capacity in a matter that is likely to have direct and predictable effects on his or her financial interests.

A board member, board employee, or agent of the board will abide by the Federal and state laws and regulations that address conflict of interest standards. In general, the Federal rules provide that:

No employee, officer, or agent of the board shall participate in selection, or in the award or administration of a contract supported by Federal funds if he or she has a real or apparent conflict of interest. Such a conflict would arise when the employee, officer, or agent, any member of his or her immediate family, his or her partner, or an organization which employs, or is about to employ any of the parties indicated herein, has a financial or other interest in or a tangible personal benefit from the firm considered for a contract. The board's officers, employees, or agents will neither solicit nor accept gratuities, favors or anything of monetary value from contractors, potential contractors, or parties to subcontracts.

The board's conflict of interest policies include adherence to the Alabama Ethics Law, which defines conflict of interest as:

A conflict on the part of a public official or public employee between his or her private interests and the official responsibilities inherent in an office of public trust. A conflict of interest involves any action, inaction, or decision by a public official or public employee in the discharge of his or her official duties which would materially affect his or her financial interest or those of his or her family members or any business with which the person is associated in a manner different from the manner it affects the other members of the class to which he or she belongs.

A board member, board employee, or agent of the board may not review applications, proposals, or participate in the evaluation or selection process where his or her participation in the review process would create the appearance that he or she is: (a) giving preferential treatment; (b) losing independence and impartiality; (c) making decisions outside official

and appropriate channels; or (d) harming the public's confidence in the integrity of the board.

Situations and circumstances presenting an actual conflict or the appearance of a conflict should be brought to the immediate attention of superintendent. A board employee, board member, or agent of the board who has knowledge of a possible conflict of interest should identify the conflict and notify the superintendent. The superintendent will document his or her actions related to the reported conflict of interest. Resolution can consist of disqualification, recusal, waiver, or other appropriate measures. Appropriate measures may include reporting a conflict of interest to the State Ethics Commission, the Alabama State Board of Education, or the appropriate federal agency.

4.17 Procurement Policy (Adopted 7/14/2016)

The board will follow state laws for the procurement of property and services. The primary state procurement laws for Alabama school boards are:

- *Alabama Competitive Bid Laws (Chapter 13B of Title 16, Code of Alabama 1975);*
- *Joint Information Technology Purchasing Agreement (Chapter 13B of Title 16, Code of Alabama 1975); and,*
- *Public Works Law (Title 39, Code of Alabama 1975).*

To the extent allowed by state laws, the board will utilize state, local, regional, and national purchasing agreements where appropriate for the procurement or use of goods and services. All procurement transactions are subject to the board's *Conflict of Interest Policy* and the procurement decisions of the board will:

- Avoid acquisition of unnecessary or duplicative goods and services;
- Use the most economical and efficient approach for acquisitions;
- Award acquisition contracts only to responsible contractors possessing the ability to perform successfully under the terms and conditions of the proposed procurement;
- Consider contactor integrity, compliance with public policy, record of past performance, and financial and technical resources prior to awarding procurement contracts;
- Maintain records sufficient to document the history of the procurement; and,
- Conduct procurement transactions in a manner that provides full and open competition.

Procurement transactions that are not subject to the state procurement laws, but exceed the aggregate amount of the federal micro-purchase threshold, will be obtained by utilizing price or rate quotes from two or more qualified sources. State procurement laws include

requirements that comply with the Uniform Administrative Requirements for procurement of property and services.

The board will request proposals for professional service contracts (excluding architectural and engineering services) that are not subject to the state procurement laws. The board will utilize a team of three or more qualified individuals to conduct a technical evaluation of proposals received and for selecting recipients. As a part of the evaluation, the individuals on the evaluation team will sign an assurance that each of the individuals is in compliance with the board's conflict of interest policy.