Blount County Schools' Data Governance Policy



# Rodney P. Green, Superintendent

BoardApprovedDate:*3/16/2016*

1. **PURPOSE**

# Blount County Schools Data Governance Policy

* 1. It is the policy of Blount County Schools that data or information in all its forms--written, electronic, or printed--is protected from accidental or intentional unauthorized modification, destruction, or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment, software, and practices used to process, store, and transmit data or information.
  2. The data governance policies and procedures are documented and reviewed annually by the Data Governance Committee, consisting primarily of District Improvement Team members.
  3. Blount County Schools conducts annual training on its data governance policy and documents that training.
  4. The terms data and information are used separately, together, and interchangeably throughout the policy. The intent is the same.

### SCOPE

The superintendent is authorized to establish, implement, and maintain data and information security measures. The policy, standards, processes, and procedures apply to all students and employees of the district, contractual third parties and agents of the district, and volunteers who have access to district data systems or data. This policy applies to all forms of Blount County Schools' data and information, including but not limited to the following:

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

### REGULATORY COMPLIANCE

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

* 1. Children's Internet Protection Act (CIPA)
  2. Children's Online Privacy Protection Act (COPPA)
  3. Family Educational Rights and Privacy Act (FERPA)
  4. Health Insurance Portability and Accountability Act (HIPAA)
  5. Payment Card Industry Data Security Standard (PCI DSS)
  6. Protection of Pupil Rights Amendment (PPRA)

#### RISK MANAGEMENT

* 1. A thorough risk analysis of all Blount County Schools' data networks, systems, policies, and procedures shall be conducted on an annual basis or as requested by the Superintendent, Assistant Superintendent, or Technology Coordinator. The risk assessment shall be used as a basis for a plan to mitigate identified threats and risk to an acceptable level.
  2. The Superintendent or designee administers periodic risk assessments to identify, quantify, and prioritize risks. Based on the periodic assessment, measures are implemented that mitigate the threats by reducing the amount and scope of the vulnerabilities. See Appendix B.

#### DATACLASSIFICATION

Classification is used to promote proper controls for safeguarding the confidentiality of data. Regardless of classification, the integrity and accuracy of all classifications of data are protected. The classification assigned and the related controls applied are dependent on the sensitivity of the data. Data are classified according to the most sensitive detail they include. Data recorded in several formats (e.g., source document, electronic record, report) have the same classification regardless of format. See Appendix D.

#### SYSTEMS AND INFORMATION CONTROL

Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, AV equipment, server, internal or external storage, communication device or any other current or future electronic or technological device may be referred to as systems. All involved systems and information are assets of Blount County Schools and shall be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

* 1. **Ownership of Software:** All computer software developed by Blount County School employees or contract personnel on behalf of Blount County Schools, licensed or purchased for Blount County Schools use is the property of Blount County Schools and shall not be copied for use at home or any other location, unless otherwise specified by the license agreement.
  2. **Software Installation and Use:** All software packages that reside on technological systems within or used by Blount County Schools shall comply with applicable licensing agreements and restrictions and shall comply with Blount County Schools' acquisition of software procedures.
  3. **Virus, Malware, Spyware, Phishing and SPAM Protection:** Virus checking systems approved by the District Technology Department are deployed using a multi-layered approach (computers, servers, gateways, firewalls, filters, etc.) that ensures all electronic files are appropriately scanned for viruses,

malware, spyware, phishing and SPAM. Users shall not tum off or disable Blount County Schools' protection systems or install other systems.

* 1. **Access Controls:** Physical and electronic access to information systems that contain Personally Identifiable Information (PII), confidential information, internal information and computing resources is controlled. To ensure appropriate levels of access by internal workers, a variety of security measures are instituted as recommended by the data governance committee and approved by Blount County Schools. In particular, the data governance committee shall document roles and rights to the student information system and other like systems. Mechanisms to control access to PIJ, confidential information, internal information and computing resources include, but are not limited to, the following methods:
     1. **Authorization:** Access shall be granted on a "need to know" basis and shall be authorized by the Superintendent, Assistant Superintendent, principal, immediate supervisor, or Data Governance Committee with the assistance of the Technology Coordinator and/or Information System Specialist (ISS.) Specifically, on a case-by-case basis, permissions may be added to those already held by individual users in the student management system, again on a need-to-know basis and only in order to fulfill specific job responsibilities, with approval of the Superintendent, Assistant Superintendent, and/or Data Governance Committee.

1. **Identification/Authentication:** Unique user identification (user ID) and authentication are required for all systems that maintain or access PII, confidential information, and/or internal information. Users shall be held accountable for all actions performed on the system with their User ID. User accounts and passwords shall NOT be shared.
2. **Data Integrity:** Blount County Schools provides safeguards so that PII, confidential, and internal information is not altered or destroyed in an unauthorized manner. Core data are backed up to a private cloud for disaster recovery. In addition, listed below are methods that are used for data integrity in various circumstances:
   * transaction audit
   * disk redundancy (RAID)
   * ECC (Error Correcting Memory)
   * checksums (file integrity)
   * data encryption
   * data wipes
3. **Transmission Security:** Technical security mechanisms are in place to guard against unauthorized access to data that are transmitted over a communications network, including wireless networks. The following features are implemented:
   * integrity controls and
   * encryption, where deemed appropriate

*Note: Only BCS district-supported email accounts shall be used for communications to and. from school employees, to and. from parents or other community members, to and. from other educational agencies, to and. from vendors or other associations, and lo and from students for school business.*

1. **Remote Access:** Access into Blount County Schools' network from outside is allowed using the BCS Portal. All other network access options are strictly prohibited without explicit authorization from the Superintendent, Assistant Superintendent, Technology Coordinator, or Data Governance Committee. Further, PII, confidential information and/or internal information that is stored or accessed remotely shall maintain the same level of protections as information stored and accessed within the Blount County Schools' network. PU shall only be stored in cloud storage if said storage has been approved by the Data Governance Committee or its designees.
2. **Physical and Electronic Access and Security:** Access to areas in which information processing is carried out shall be restricted to only appropriately authorized individuals. Staff passwords shall be changed as recommended by the Technology Coordinator.
   * No PII, confidential and/or internal information shall be stored on a device itself such as a hard drive, mobile device of any kind, or external storage device that is not located within a secure area.
   * No technological systems that may contain information as defined above shall be disposed of or moved without adhering to the appropriate Purchasing and Disposal of Electronic Equipment procedures.
   * It is the responsibility of the user to not leave these devices logged in, unattended, and open to unauthorized use.

##### Data Transfer/Exchange/Printing:

l. **Electronic Mass Data Transfers:** Downloading, uploading, or transferring PII, confidential information, and internal information between systems shall be strictly controlled. Requests for mass download of, or individual requests for, information for research or any other purposes that include PII shall be in accordance with this policy and be approved by the data governance committee. All other mass downloads of information shall be approved by the committee and/or its designees and include only the minimum amount of information necessary to fulfill the request. A Memorandum of Agreement (MOA) shall be in place when transferring PII to external entities such as software or application vendors, textbook companies, testing companies, or any other web-based application, etc. unless the exception is approved by the Data Governance Committee.

2. **Other Electronic Data Transfers and Printing:** PII, confidential information, and internal information shall be stored in a manner inaccessible to unauthorized individuals. PII and confidential information shall not be downloaded, copied or printed indiscriminately or left unattended and open to compromise. PII that is downloaded for educational purposes where possible shall be de-identified before use.

* 1. **Oral Communications:** Blount County Schools' staff shall be aware of their surroundings when discussing PU and confidential information. This includes but is not limited to the use of cellular telephones in public areas. Blount County Schools' staff shall not discuss PII or confidential information in public areas if the information can be overheard. Caution shall be used when conducting conversations in semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.
  2. **Audit Controls:** Hardware, software, services and/or procedural mechanisms that record and examine activity in information systems that contain or use PII are reviewed by the Data Governance Committee.

Further, the committee also regularly reviews records of information system activity, such as audit logs, access reports, and security incident tracking reports. These reviews shall be documented and maintained for six (6) years.

* 1. **Evaluation:** Blount County Schools requires that periodic technical and non-technical evaluations of access controls, storage, and other systems be performed in response to environmental or operational changes affecting the security of electronic PII to ensure its continued protection.
  2. **IT Disaster Recovery:** Controls shall ensure that Blount County Schools can recover from any damage to critical systems, data, or information within a reasonable period of time. Each school, department, or individual is required to report any instances immediately to the Superintendent, Assistant Superintendent, Technology Coordinator, and/or ISS for response to a system emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages data or systems. The IT Disaster Plan shall include the following:
     1. A prioritized list of critical services, data, and contacts.

1. A process enabling Blount County Schools to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.
2. A process enabling Blount County Schools to continue to operate in the event of fire, vandalism, natural disaster, or system failure.
3. Procedures for periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary.

#### COMPLIANCE

* 1. The Data Governance Policy applies to all users of Blount County Schools' information including: employees, staff, students, volunteers, and outside affiliates. Failure to comply with this policy by employees, staff, volunteers, and outside affiliates may result in disciplinary action up to and including dismissal in accordance with applicable Blount County Schools' procedures, or, in the case of outside affiliates, termination of the affiliation. Failure to comply with this policy by students may constitute grounds for corrective action in accordance with Blount County Schools' policies. Further, penalties associated with state and federal laws may apply.
  2. Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:
     1. Unauthorized disclosure of PII or confidential information.

1. Unauthorized disclosure of a log-in code (User ID and password).
2. An attempt to obtain a log-in code or password that belongs to another person.
3. An attempt to use another person's log-in code or password.
4. Unauthorized use of an authorized password to invade student or employee privacy by examining records or information for which there has been no request for review.
5. Installation or use of unlicensed software on Blount County Schools' technological systems.
6. The intentional unauthorized altering, destruction, or disposal of Blount County Schools' information, data and/or systems. This includes the unauthorized removal from BCS of technological systems such as but not limited to laptops, internal or external storage, computers, servers, backups or other media, copiers, etc. that contain PII or confidential information.
7. An attempt to gain access to log-in codes for purposes other than for support by authorized technology staff, including the completion of fraudulent documentation to gain access.

5

**Data Governance Board Policy**

##### Appendix A

The Superintendent is authorized to establish procedures governing the storage, use, and sharing of data maintained electronically by the school system. Such procedures shall comply with applicable state and federal law and shall 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 Board 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.

## Information Risk Management Practices

##### Appendix B

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 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. 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.

**Definitions**

## Definitions and Responsibilities

##### Appendix C

* 1. **Availability:** Data or information is accessible and usable upon demand by an authorized person.
  2. **Confidentiality:** Data or information is not made available or disclosed to unauthorized persons or processes.
  3. **Customers:** Staff, parents, employees (including contract), and students are

considered customers of the school district.

* 1. **Data:** Facts or information
  2. **Information:** Knowledge that you get about something or someone; facts or details.
  3. **Data Integrity:** Data or information that has not been altered or destroyed in an unauthorized manner.
  4. **Involved Persons:** Every user of Involved 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.
  5. **Involved Systems:** All data-involved computer equipment/devices and network systems that are operated within the Blount County Schools physical or virtual (cloud) environment. This includes all platforms (operating systems), all computer/device sizes (personal digital assistants, desktops, mainframes, telephones, laptops, tablets, game consoles, etc.}, and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.
  6. **Personally, Identifiable Information (PII):** PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
  7. **Risk:** The probability of a loss of confidentiality, integrity, or availability of information resources.

# Responsibilities

1. **Data Governance Committee:** The Data Governance Committee for Blount County Schools is responsible for working with the Technology Coordinator and information System Specialist to ensure that security policies, procedures, and standards are in place and adhered to by entity. Other responsibilities include:
   1. Reviewing the Data Governance and Security Policy annually and

communicating changes in policy to all involved parties.

* 1. Educating data custodian and user management with comprehensive information about security controls affecting system users and application systems.

1. **Information System Specialist:** The Information System Specialist (ISS) for Blount County Schools is responsible for working with the Superintendent, Assistant Superintendent, Technology Coordinator, Data Governance Committee, user management, owners, data custodians, and users to develop and implement prudent security policies, procedures, and controls. Specific responsibilities include:
   1. Providing basic security support for all systems and users.
   2. Assisting owners in the identification and classification of technology and data related resources.

**See *also Appendix D (Data Classification.)***

* 1. Assisting systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation.
  2. Performing or overseeing security audits with the Technology Coordinator.
  3. Reporting regularly to the Superintendent, Assistant Superintendent, and Blount County Schools' Data Governance Committee on status with regard to information security.

1. **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 ISS 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.

##### 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 may delegate ownership responsibilities to another individual by completing a Blount County Schools Information Owner Delegation/Transfer Request in writing and submitting it to the Superintendent and/or the Data Governance Committee for approval. The owner of information has the responsibility for the following:

1. Knowing the information for which she/he is responsible.
2. Determining a data retention period for the information, relying on ALSDE guidelines, industry standards, Data Governance Committee guidelines, or advice from the school 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 ISS 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 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.
   1. **Data Custodian:** The data custodian is assigned by an administrator, data owner, or the ISS based his/her role and is generally responsible for the processing and storage of the information. The data custodian is responsible for the administration of controls as specified by the owner. Responsibilities may include:
10. Providing and/or recommending physical safeguards.
11. Providing and/or recommending procedural safeguards.
12. Administering access to information.
13. Releasing information as authorized by the Information Owner and/or the Information System Specialist for use and disclosure using procedures that protect the privacy of the information.
14. Maintaining information security policies, procedures and standards as appropriate and in consultation with the ISS.
15. Promoting employee education and awareness by utilizing programs approved by Data Governance Committee, where appropriate.
16. Reporting promptly to the ISS the loss or misuse of Blount County Schools' data.
17. Identifying and responding to security incidents and initiating appropriate actions when problems are identified.
    1. **User:** The user is any person who has been authorized to read, enter, or update information. A user of information is expected to comply with the following:
18. Access information only in support of their authorized job responsibilities.
19. Comply with all data security procedures and guidelines in the Blount County Schools Data Governance and Use Policy and all controls established by the data owner and/or data custodian.
20. Keep personal authentication devices (e.g. passwords, secure cards, PINs, access codes, etc.) confidential.
21. Report promptly to the ISS the loss or misuse of Blount County Schools' information.
22. Follow corrective actions when problems are identified.

## Data Classification Levels

##### Appendix D

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

* 1. 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 customers, or its business partners. Decisions about the provision of access to this information must always be cleared through the information owner and/or data governance committee.

1. **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 so distributed within the organization without advance permission from the information owner.

Examples of Internal information may include: personnel directories, internal policies and procedures, most internal electronic mail messages.

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

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

##### Directory Information

Blount County Schools defines Directory information as follows: Student first and last name

Student gender Student home address

Student home telephone number Student school-assigned email address Student photograph

Student place and date of birth Student dates of attendance (years) Student grade level

Student diplomas, honors, awards received

Student participation in school activities or school sports Student weight and height for members of school athletic teams Student most recent institution/school attended

Student ID number