ST. CLAIR COUNTY SCHOOLS DATA GOVERNANCE POLICY

INTRODUCTION

Protecting our students' and staffs' privacy is an important priority, and St. Clair County Schools is committed to maintaining strong and meaningful privacy and security protections. The privacy and security of this information is a significant responsibility, and we value the trust of our students, parents, and staff.

The St. Clair County Schools Data Governance document includes information regarding the Data Governance Committee, the actual St. Clair County Schools Data and Information Governance and Acceptable Use Policy, applicable Appendices, and Supplemental Resources.

The policy formally outlines how operational and instructional activity shall be carried out to ensure St. Clair County Schools' data is accurate, accessible, consistent, and protected. The document establishes who is responsible for information under various circumstances and specifies what procedures shall be used to manage and protect it.

The St. Clair County Schools Data Governance Policy will be a living document. Procedures to ensure document flexibility are outlined throughout this document. With the Board's permission, the Data Governance Committee may quickly modify information in the Appendices in response to changing needs. All modifications will be posted on the St. Clair County Schools' website.

I. PURPOSE

A. It is the policy of St. Clair County Schools that data or information in all its forms--written, electronic, or printed--are 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. All of this policy was written with "Need to Know" in mind.
B. The data governance policies and procedures are documented and reviewed annually by the data governance committee.
C. St. Clair County Schools conducts and documents annual training on their data governance policy.
D. The terms data and information are used separately, together, and interchangeably throughout the policy. The intent is the same.

II. SCOPE

The Superintendent and their designee 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 or data systems.

This policy applies to all forms of St. Clair County Schools' data and information, including but not limited to:

A. Speech, spoken face to face, or oral communicated by phone or any current and future technologies.
B. Hard copy data printed or written.

C. Communications sent by post/courier, fax, electronic mail, text, chat and or any form of social media, etc.
D. Data stored and/or processed by servers, PCs, laptops, tablets, mobile devices, etc.
E. Data stored on any type of internal, external, or removable media or cloud-based services.
F. Software, hardware and any peripherals used to access or store data.

III. Common Definitions and Responsibilities

Definitions

A. **Availability**: The information security concept that data, information, systems, or related are accessible and usable upon demand by an authorized person
B. **Confidentiality**: The information security concept that data, information, systems, or related are not made available or disclosed to unauthorized persons or processes, intentionally or unintentionally
C. **Integrity:** The information security concept that data, information, systems, or related are maintained in their original intended state and have not been modified or corrupted intentionally or unintentionally
D. **Entity**: Organization such as school system, school, department or in some cases business
E. **Information**: Knowledge that you get about something or someone; facts or details
F. **Data:** Facts or information; may refer to data in any state (in transmission, in transit, at rest)
G. **Involved Persons**: Every user of involved Systems (see below) at St. Clair County Schools – no matter what their status. This includes nurses, residents, students, employees, contractors, consultants, temporaries, volunteers, substitutes, student teachers, interns, etc.
H. **Systems**: All computer equipment/devices and network systems that are operated within or by the St. Clair County Schools physically or virtually. This includes all platforms (operating systems), all computer/device sizes (personal digital assistants, desktops, mainframes, telephones, laptops, tablets, game consoles, etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems – this encapsulates any technological devices or infrastructure of any kind
I. **Personally Identifiable Information (PII)**: PII is any information about an individual maintained by an agency, including:

    - 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
    - Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information

J. **Risk**: A measure of the extent to which an entity is threatened by a potential circumstance or event, including the adverse impacts that would arise if the circumstance or event occurs and the likelihood of occurrence
K. **Phishing:** the fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. Phishing, along with other *ishings such as vishing, smishing, and spear phishing, are essentially attempts to harvest information from legitimate employees by a bad actor – things like credit card number theft (then used for fraud), stealing login credentials (then used to become better poised to attack secure or private systems), etc.
L. **Business E-mail Compromise (BEC):** In a BEC scam, criminals send an email message that appears to come from a known source making a legitimate request; like a CEO who has had their credentials

compromised by an attacker asking an employee to do something malicious. This often goes together with phishing.

Responsibilities

A. **Data Governance Committee**: The Data Governance Committee for St. Clair County Schools is responsible for working with the Information Security Officer (ISO) to ensure security policies, procedures, and standards are in place and adhered to by the entity. Other responsibilities include:

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

B. **Information Security Officer**: The Information Security Officer (ISO) for St. Clair County Schools is responsible for working with the superintendent, Technology Director, Technology Team, Data Governance Committee, User Management, Owners, and Users to develop and implement prudent security policies, procedures, and controls. Specific responsibilities include:

- Providing security support for all systems and users and taking action to improve the organization's security posture
- Providing regular cyber security training to staff including but not limited to secure password training and phishing/business e-mail compromise awareness training
- Advising owners in the identification and classification of technology and data related resources
- Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation
- Performing and/or overseeing regular security audits
- Reporting regularly to the Superintendent, Technology Director and St. Clair County Schools Data Governance Committee on St. Clair County Schools' status about information security/security posture
- Maintaining ownership over disaster response plans

C. **User Management**: St. Clair County Schools' Administrators are responsible for overseeing their staff's use of information and systems.

- Reviewing and approving or denying all requests for their employees' access authorizations to maintain separation of duties and least privilege
- Initiating security change requests to keep employees' secure access current with their positions and job functions to maintain separate of duties and least privilege
- Promptly informing appropriate parties of employee terminations and transfers, in accordance with local entity termination procedures
- Revoking physical access to terminated employees, i.e., confiscating keys, changing combination locks, etc.
- Providing employees with appropriate training needed to properly use systems and use them safely, securely and responsibly
- Reporting promptly to the Superintendent, Technology Director, ISO and the Data Governance Committee the loss or misuse of St. Clair County' information

- Promptly initiating corrective actions when problems are identified
- 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
- Following all privacy and security policies and procedures

D. **Student User management**: Administrators and Faculty are responsible for overseeing all student use of data and data systems, including:

- Monitoring websites and software students use to maintain a safe and secure environment
- Student use of personal devices while on school property
- Student's use of electronic and paper data
- Students use of school provided systems holistically
- Maintaining the confidentiality of school employee systems such that students may not view or interact with them while an employee or other privileged user is logged in
- Monitor student system logins and assure students are using their own credentials to login to systems and software
- Assure students are aware of privacy policies and are made aware of all avenues for reporting malicious activity and misuse of systems
- Reporting promptly to the Superintendent, Technology Director, ISO and the Data Governance Committee the loss or misuse of St. Clair County' information
- Promptly initiating corrective actions when problems are identified
- Ensure all students are following all privacy and security policies and procedures as well as the St Clair County Board of Education Acceptable Use Policy

E. **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:

- Knowing the information for which she/he is responsible
- Determining a data retention period for the information, relying on Local, State and Federal laws, ALSDE guidelines, industry standards, Data Governance Committee guidelines or advice from the school system attorney
- Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created
- Authorizing access and assigning data custodianship if applicable
- Specifying controls and communicating the control requirements to the data custodian and users of the information
- Reporting promptly to the Technology Director, Data Governance Committee and ISO the loss or misuse of St. Clair County's data
- Promptly initiating corrective actions when problems are identified
- Promoting employee education and awareness by utilizing programs approved by the ISO and Data Governance Committee, where appropriate
- Spearheading initiatives which involve said information

- 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

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

- Access information only in support of their authorized responsibilities
- Comply with all data security procedures and guidelines in the St. Clair County Schools Data Governance Policy
- Keep personal authentication devices (e.g. passwords, secure cards, PINs, access codes, etc.) confidential
- Report promptly to the ISO, Data Governance Committee, Technology Department, and/or supervising authority the loss or misuse of St. Clair County Schools' information
- Follow prompt corrective actions when problems are identified
- Adhere to the St Clair County Board of Education Acceptable Use Policy
- Always act in good faith when using systems or interacting with data; accidents happen, but malicious activity under the guise of an accident is not tolerated
- Do not engage in malicious activity on systems or on data, including but not limited to exploitation of known or unknown vulnerabilities, installation of malware, shoulder-surfing to steal credentials or other privileged information, etc.
- Always report discovered exploits, vulnerabilities, misconfigurations, or any other security-related or privacy-related issue to appropriate party if encountered

IV. REGULATORY COMPLIANCE

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

A. Children's Internet Protection Act (CIPA)
B. Children's Online Privacy Protection Act (COPPA)
C. Family Educational Rights and Privacy Act (FERPA)
D. Health Insurance Portability and Accountability Act (HIPAA)
E. Payment Card Industry Data Security Standard (PCI DSS)
F. Protection of Pupil Rights Amendment (PPRA)

Referenced Laws, Regulatory and Contractual Security Requirements

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

1. Their Internet safety policies shall include monitoring the online activities of minors; and
2. As required by the Protecting Children in the 21st Century Act, they shall provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyber bullying awareness and response

For more information see: https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

B. **COPPA**: The **Children's Online Privacy Protection Act**, regulates operators of commercial websites or online services directed to children under 13 that collect or store information about children. Parental permission is required to gather certain information.

   For more information see: https://www.ftc.gov/business-guidance/privacy-security/childrens-privacy

C. **FERPA**: The **Family Educational Rights and Privacy Act**, applies to all institutions that are recipients of federal aid administered by the Secretary of Education. This regulation protects student information and accords student's specific rights with respect to their data.

   For more information see: https://studentprivacy.ed.gov/node/548/

D. **HIPAA**: The **Health Insurance Portability and Accountability Act**, applies to organizations that transmit or store Protected Health Information (PII). It is a broad standard that was originally intended to combat waste, fraud, and abuse in health care delivery and health insurance, but is now used to measure and improve the security of health information as well.

   For more information see: https://www.hhs.gov/hipaa/index.html

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

   For more information see: https://www.pcisecuritystandards.org/resources-overview/

F. **PPRA**: The **Protection of Pupil Rights Amendment** applies to programs that receive funding from the U.S. Department of Education (ED). PPRA is intended to protect the rights of parents and students in two ways:

   1. It seeks to ensure that schools and contractors make instructional materials available for inspection by parents if those materials will be used in connection with an ED-funded survey, analysis, or evaluation in which their children participate; and
   2. It seeks to ensure that schools and contractors obtain written parental consent before minor students are required to participate in any ED-funded survey, analysis, or evaluation that reveals information concerning:

      - Political affiliations;
      - Mental and psychological problems potentially embarrassing to the student and his/her family;
      - Sexual behavior and attitudes;
      - Illegal, anti-social, self-incriminating and demeaning behavior;
      - Critical appraisals of other individuals with whom respondents have close family relationships;
      - Legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers; or
      - Income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program)

Parents or students who believe their rights under PPRA may have been violated may file a complaint via following the instructions located at https://studentprivacy.ed.gov/file-a-complaint. For additional information or technical assistance, you may visit https://studentprivacy.ed.gov/contact.

For more information about PPRA itself, see: https://studentprivacy.ed.gov/content/ppra.

V. RISK MANAGEMENT

A. A thorough risk analysis of all St. Clair County Schools' data networks, systems, policies, and procedures shall be conducted on an annual basis or as requested by the Superintendent, ISO or Technology Director. The risk assessment shall be used as a basis for a plan to mitigate identified threats and risk to an acceptable level. This assessment shall follow an industry standard risk management framework like the NIST Risk Management Framework or similar.
B. 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.

VI. DATA CLASSIFICATION

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

A. **Personally Identifiable Information (PII)**
   1. PII is information about an individual maintained by an agency, including:
      a. Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records, etc.
      b. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information, etc.
   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 St. Clair 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 must be restricted to those with a legitimate 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 St. Clair County Schools, its staff, parents, students including contract employees, 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.

C. **Internal Information**

1. Internal Information is intended for unrestricted use within St. Clair County Schools, and in some cases within affiliated organizations such as St. Clair County Schools' business or community partners. This type of information is already widely distributed within St. Clair 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
   - Internal electronic messages

2. Any information not explicitly classified as PII, Confidential or Public (see below) shall, by default, be classified as Confidential Information until properly reclassified by the Superintendent, ISO or Data Governance Committee
3. Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions and could result in disciplinary or legal actions

D. **Public Information**

1. Public Information will only be approved and released to the public by a specifically designated authority within each entity of St. Clair County Schools. Individuals are not authorized to release information to the public in any format without prior approval. No information about emergency or legal situations can be released to the public without explicit approval from Administration.

   Examples of Public Information may include:

   - Marketing brochures and material posted to St. Clair County Schools' web pages
   - Tweets, Facebook, phone calls, emails and or information to the public regarding lockdowns etc...

2. This information may be disclosed outside of St. Clair County Schools.

E. **Directory Information**

1. St. Clair County Schools defines Directory information as follows:

   - First and last name
   - Gender
   - Home address
   - Home telephone number
   - Email address
   - Photograph

- Place and date of birth
- Dates of attendance (years)
- Student grade level
- 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

VII. 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 St. Clair County Schools and shall be protected from misuse, unauthorized manipulation and destruction. These protection measures may be physical and/or software based.

1. **Data Inventory**
   The St. Clair County School System collects individual student data directly from students and/or families through our state funded student data management system. Local student data is securely transmitted daily to the state's data management system from which state and federal reporting is completed. Each student is assigned a unique student identifier upon enrollment into the student management system to ensure compliance with the privacy rights of the student and his or her parents/guardians.

   Maintaining a complete up-to-date inventory of all records and data systems, including those used to store and process data, enables the St. Clair County Schools to target its data security and privacy management efforts to appropriately protect sensitive data. The data records inventory specifies what data elements are collected, provides a justification for their collection, and explains the intended purpose(s) for their use.

STUDENT DATA FILES

Data elements collected	Justification for collection	Intended purpose(s) for use
Basic Demographic Information: Student name, State ID #, address, phone, parent info/contact, race, gender, home language, etc.	State reporting requirements	Student Identification Athletic Assessments Drug Testing
Student info: Social security number and/or Identifying Number	State reporting requirements	Student Identification Athletic Assessments Drug Testing

Grades	State reporting requirements	Track student's achievement levels throughout their school career Athletic Assessments
Attendance	State reporting requirements	Track student's attendance throughout their school career
Discipline	State reporting requirements	Track student's discipline throughout their school career
Free/Reduced Lunch information	State reporting requirements	To determine if the student qualifies for free/reduced meals
Special Ed/504/ELL data	Data is collected to ensure proper placement of students in the educational environment	To ensure provision of a free and appropriate education for students with special needs

Assessment data from state and LEA standardized assessments	State reporting requirements	Track student's achievement levels throughout their school career to determine areas of strengths and weaknesses and college and career readiness

This information could be provided to the Judicial system for Attendance Referrals, Discipline, and various legal needs.

2. **Memorandum of Agreement**: A Memorandum of Agreement (MOA) will be completed between St Clair County Board of Education and any third party vendor or outside entity that may need access to St Clair County Board of Education, Computers, Network, files, or data (paper or electronic) and kept on file for a minimum period of 3 years. The MOA will be reviewed and updated annually.

   The MOA is available at http://www.sccboe.org/moa.

3. **Data Back-up and Retention Procedures**: St Clair County Board of Education will maintain a backup of data that has been stored on the servers in the St Clair County Board of Education network environment. Backups of data created on the local computers or local computing devices are not collected. Any data requiring to be collected in the backup systems must be stored on the St Clair County Board of Education Network drives. Backups will be retained according to type data, and the Industry Best Practices, SCCBOE Policy, Local, State and Federal Laws. Furthermore, data and

infrastructure backups will regularly be tested via “trial runs” to confirm that their state is maintained in working order and prevent incidents in which backups are required but are unable to be utilized.

4. **End User access:** All end users, including all employees, students, guest, vendors, etc., are required to have and use a unique individual Username and Password (login credential) adhering to the password policy outlined in this document, to access local computing devices, the SCCBOE domain, the SCCBOE network and all SCCBOE network resources. This username and password will be created and maintained on the SCCBOE domain. Properly created accounts will receive the appropriate rights to network drives, email, local computer rights, internet access, 3rd party software etc. This is to ensure the privacy and integrity of the User account and the security of information created and stored on the SCCBOE domain and its network, in addition to protecting and securing PII and being compliant with all rules laws and industry best practices. All accounts will be used in accordance with the SCCBOE Acceptable Use Policy and any violations could be subject to penalties, disciplinary actions and possible legal actions.

5. **Network Utilization:** No school or school facility will utilize any network or internet connectivity that is not approved and furnished by the St Clair County Board of Education Technology Department. To ensure the safety of data, students and faculty, the St Clair County Board of Education makes all efforts to maintain compliance with all procedures, laws, regulations, and industry standards. All data, network traffic, and internet connections must be protected behind the St Clair County Board of Education firewall and filtered by St Clair County Board of Education.

6. **Password Policy:** This section seeks to outline guidance for the creation of secure passwords
    1. Users are responsible for complying with the following password standards for network access or access to secure information. These standards are based on NIST Special Publication 800-63B (2023) with modification:
        a. Passwords must never be shared with another person, unless the person is a designated security manager, and it is **required under exceptional circumstances**. Passwords must never be shared via e-mail.
        b. Passwords are required to be changed upon compromise or user request, but otherwise, they must be changed every 6 months. Guest passwords, however, are changed on the first of every month.
        c. Passwords must, where applicable, have a minimum length of eight (8) characters and may be up to 64 characters (or beyond if desired); computer generated random numbers like PINs may be six (6) characters in length as per NIST 800-63B.
        d. When possible, for secure sites and/or software applications, user created passwords should adhere to the same criteria as required for network access. These criteria are defined in the SCC Network Group Policy Criteria for Passwords and is listed below:
            i. Must not contain the user's account name or parts of the user's full name that exceed two consecutive characters
            ii. Contain characters from three of the following four categories:
                - At least one English uppercase character (A through Z)
                - English lowercase characters (a through z)
                - At least one base 10 digit (0 through 9)
                - At least one non-alphanumeric characters (for example !, $, #, %)
            iii. Must not have been a previously used password within a defined time/date range.

2. Passwords must never be saved when prompted by any application except for central single sign-on (SSO) systems as approved by the Technology Department. This feature must be disabled in all applicable systems.
3. Passwords must not be programmed into a PC or recorded anywhere that someone may find and use them; this includes sticky notes, notepads, QR code stickers, or any other method of storage EXCEPT in approved password management software secured with a lengthy, strong, and complex master passphrase adhering to NIST 800-63B where applicable.
4. When creating a password, do not use passwords that are easily guessed due to their association with the user (i.e., children's names, pets' names, birthdays, etc.) A combination of upper-case and lower-case letters, numbers, and special symbols including emoticons and spaces are harder to guess.
5. When creating a password, do not use passwords which are sequential ("1234", "6789", et cetera) or repetitive ("aaaaa", "ccccc", et cetera) as per NIST 800-63B.
6. When creating a password, do not use context-specific words, such as the name of the service, the username, and derivatives thereof as per NIST 800-63B.
7. When creating a password, passphrases are strongly preferred ("Man, it's a wonderful day outside!", et cetera) as per NIST 800-63B. Strong passphrases that adhere to standard English punctuation and grammar are fine, as they will include special characters (like spaces and apostrophes), capital letters (names, first letter of the phrase), lower case letters, and maintain sufficient length (passphrases should be at least a full sentence; generally, these will be sufficiently long) along with being memorable. The above **example** password would, in theory, take centuries to crack via brute-force.
8. Using an approved password management solution is strongly encouraged.
9. Where possible, system software should enforce the following password standards:
    a. Passwords routed over a network must be encrypted.
    b. Passwords must be entered in a non-display field; users should, however, have the option to display the password in cleartext if needed as per NIST 800-63B.
    c. System software must enforce the minimum length (8 characters) and allow up to the maximum length (64 characters) or beyond if desired as per NIST 800-63B.
    d. System software shall disable the user password when more than three consecutive invalid passwords are given. Lockout time shall be set at a minimum of 30 minutes.
    e. System software should maintain a history of previous passwords (and prevent their being easily guessed due to their association with the user) for the prevention of password reuse.
    f. Passwords must be digitally stored salted, hashed, and never truncated as per NIST 800-63B.
    g. Allow the pasting of passwords into password fields to encourage use of password management software as per NIST 800-63B.
    h. Where applicable, each unique service should use its own password with no relation to other passwords in use.
    i. Multi-factor authentication is required where available as per NIST 800-63B.

10. Device Transportation

a. When taking a device home, the user will utilize a protective covering or case to protect the device in transit.
b. No unauthorized peripherals will be connected to or utilized by SCCBOE provided equipment, including but not limited to Flash drives or external hard drives.
c. SCCBOE provided equipment taken home is intended to be used for Educational or School Business purposes. No personal use is authorized.

d. No users other than the borrower of the device may have access to the device for any reason.

11. Email Usage

a. All faculty will conduct School Business in the business provided school email. Faculty will not utilize personal emails to conduct School Business. Faculty will not conduct personal business over school provided email.
b. All students will utilize their school provided email for all educational needs of the student. No outside user will be permitted to email a student account unless previously approved by the Technology Department, including people or services.
c. All e-mail users will be subject to and must abide by regular cyber security testing and training. Appropriate procedures will be covered in terms of managing phishing e-mails and spam during regular training sessions.

VIII. IT Disaster Recovery

Controls shall ensure that St. Clair 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, Technology Director and/or ISO for response to a system emergency or other occurrence (for example: fire, vandalism, system failure and natural disaster) that damages data or systems. The IT Disaster Plan shall include the following:

A. A prioritized list of critical services, data, and contacts, assets, etc.
B. A process enabling St. Clair County Schools to restore any loss of data in the event of fire, vandalism, natural disaster, system failure or any other such circumstance.
C. A process enabling St. Clair County Schools to continue to operate in the event of fire, vandalism, natural disaster, system failure or any other such circumstance.
D. Procedures for periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary.

This disaster plan will be spear-headed and managed by an IT disaster plan owner.

IX. Acquisition of Software Procedures

Purchasing and Disposal Procedures

This procedure is intended to provide for the proper purchasing and disposal of software, cloud based hosted software, technology devices, any computer, laptop, mobile device, printing and or scanning device, network appliance/equipment, AV equipment, server, internal, external or cloud-based storage, communication device or any other current or future electronic or technological device or service, herein referred to as systems in this document.

For further clarification of the term technological systems contact the St. Clair County Schools' district Technology Director. All involved systems and data are assets of St. Clair County Schools and are expected to be maintained for cleanliness as well as protected from misuse, unauthorized manipulation, and destruction.

These protection measures may be physical and or software based.

X. Purchasing Guidelines

A. **Hardware**

All systems that will be purchased, received as a donation or used in conjunction with St. Clair County Schools' technology resources regardless of funding, must be from an approved list of vendors or approved to be accepted by the district Technology Director.

Failure to have the purchase/donation approved may result in lack of technical support, request for removal from premises, or denied access to other technology resources.

B. **Software**

The Technology Department and/ or Data Governance Committee must be involved in all software, Apps or Cloud based service purchases and decision making process regardless of funding sources. This is to help ensure all software is compatible with existing systems and software. Additionally, to help ensure that all software is compliant with all privacy laws as well as the St Clair County Board of Education Data Governance Policy and all software is legally licensed.

1. Software Installation and Use: All software packages that reside on technological systems within or used by St. Clair County Schools must comply with applicable licensing agreements and restrictions and must comply with St. Clair County Schools' acquisition of software procedures.

2. Ownership of Software: All computer software developed by St. Clair County Schools' employees or contract personnel on behalf of St. Clair County Schools, licensed or purchased for St. Clair County Schools' use is the property of St. Clair County Schools and may not be copied for use at home or any other location, unless otherwise specified by the license agreement.

C. **Unapproved Software**

Any unapproved software, Apps or Cloud-based services will not be allowed to be installed on the SCCBOE Domain or its network, any servers or local computing devices until the Technology Department and/ or the Data Governance Committee can examine all software requirements, any compatibility issues, any license issue and compliance with all privacy laws as well as the St Clair County Board of Education Data Governance Policy.

D. **Cloud Storage and Software**

Purchased software accessed from and storing data in a cloud environment will be required to have a Memorandum of Agreement (MOA) on file with the Technology Director that states or confirms at a minimum that:

1. SCCBOE student and/or staff data will not be shared, sold, or mined with or by a third party,
2. SCCBOE student and/or staff data will not be stored on servers outside the US unless otherwise approved by the SCCBOE Data Governance Committee,
3. The company must comply with SCCBOE guidelines for data transfer or destruction when contractual agreement is terminated.
4. No API will be implemented without full consent of SCCBOE and the ALSDE.

E. **Alabama Competitive Laws**

1. All electronic equipment is subject to Alabama competitive bid laws. There are several purchasing co-ops that have been approved for use by the Alabama State Examiners office: http://www.examiners.state.al.us/purchcoop.aspx. Generally for technological devices and services, St. Clair County Schools purchase from the Alabama Joint Purchasing Agreement

(ALJP): https://connect.alsde.edu/sites/eia/aljp/SitePages/ALJP%20(Alabama%20K-12%20(IT)%20Joint%20Purchasing)Home.aspx

2. If a desired product is not included in one of these agreements, St. Clair County Schools bids the item or items using the districts competitive bid process. All technological systems, services, etc. over $15,000.00 purchased with public funds are subject to Alabama's competitive bid laws.
3. The $15,000.00 rule is a cumulative number and includes all purchases of any one type product that has been purchased system wide.

F. **Inventory**

1. All technological devices or systems over $500.00 are inventoried by the Technology Department in accordance with the St. Clair County Schools' Finance Department using the inventory system.
2. There are some exceptions under $500.00, as determined by the Technology Director, such as, but not limited to peripherals that are inventoried.
3. It is the responsibility of the local school Technology Contact to inventory technological systems used in the local school and manage said inventory. The district technology staff is responsible for ensuring that any network equipment, fileservers, or district systems, etc. are inventoried.

XI. Disposal Guidelines

A. Equipment shall be considered for disposal for the following reasons:

1. End of useful life
2. Lack of continued need
3. Obsolescence or deprecation; serious vulnerability without possible mitigation
4. Wear, damage, or deterioration
5. Excessive cost of maintenance or repair

B. The local school principal, Technology Director, and or the Director of Finance shall approve school disposals list to be presented to the Board of Education for approval of disposal by discard or donation.

C. Written documentation in the form of a spreadsheet including but not limited to the following shall be provided to the District Technology Office no later than Wednesday at 9:00 a.m. prior to the next Board of Education meeting on the following Monday:

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

D. ***Methods of Disposal***

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

It is the responsibility of the local school Technology Contact to modify the inventory entry to reflect any in-school transfers, in-district transfers, donations or discards for technological systems. The department from which a computing device was purchased is responsible for modifying the inventory

records to reflect any transfers within the central offices, any transfers of central office electronic equipment to local schools, central office donations or central office discards.

E. ***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 peripheral devices, have it wiped and reimaged or configured.

F. ***Discard***
All electronic equipment in the St. Clair County Schools district must be discarded in a manner consistent with applicable environmental regulations. Electronic equipment may contain hazardous materials such as mercury, lead, and hexavalent chromium.

In addition, systems may contain Personally Identifiable Information (PII), Confidential, or Internal Information.

Systems must be wiped clean of this information prior to leaving the school district. A district-approved vendor will be contracted for the disposal of all technological systems/equipment. The vendor must 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 St. Clair County Schools and/or the employee who disposed of the equipment liable for violating environmental regulations or laws.

XII. Virus, Malware, and Spyware 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, and spyware. Users shall not turn off or disable St. Clair County Schools' protection systems or install other systems.

St. Clair County Schools' desktops, laptops, and fileservers run licensed industry standard antivirus/antimalware software. Virus definitions are updated regularly; all Microsoft PC based systems are set to scan all network files as they are accessed. Quick scans are set to run daily at 10:00 AM and a full scheduled scan runs every Friday at 2:00 PM or if missed or interrupted at the next time the computer/laptop is turned on.

XIII. Internet Filtering

Online content and social collaboration continue to increase as educational resources.

St. Clair County Schools employs Internet filtering to balance safety with learning—letting good content, resources, and connections in while blocking the bad. To balance educational Internet resources and app use with student safety and network security, the Internet traffic from all devices that authenticate to the network is routed through a web filter using the user's network credentials.

For peripheral devices and guest devices, users see a login screen that requires them to login to the web filter with their network credentials or a guest login and password to gain access to the Internet. This

process sets the filtering level appropriately based on the role of the user, such as, student, staff or guest, and more specifically for students, the grade level of the child.

All sites that are known for malicious software, phishing, spyware, advertising or have inappropriate graphics or language etc. will be blocked. Any site deemed to cause an unnecessary strain or large impact on internet bandwidth may be blocked at the Technology Department's discretion.

XIV. Phishing/BEC and SPAM Protection

In addition to the built-in spam filtering of Microsoft Exchange, email is filtered for viruses, phishing, spam, and spoofing using a combination of filtering appliances and software. The Spam filter will provide access for the end user to view and recover emails that were caught and held. While the end user can release and recover held emails this should only be done with the strictest care and if it is an email the end user was expecting. On-going phishing awareness training will be implemented as an effort to help prevent compromise via phishing and other *ishing-related attacks.

XV. Security Patches

Windows security patches and other Windows patches are researched, tested and approved before being scheduled to "auto-download" and "schedule install." The schedule installs occur during anticipated low usage time frames, in the event they are interrupted for whatever reason they will continue update attempts at the next opportunity when the system is next turned on.

For security reasons all devices are to be permitted the opportunity to update with these patches and approved updates must be applied as soon as possible to all machines to preserve device security.

XVI. Physical and Security Controls

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 St. Clair 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 PII, Confidential information, Internal information and computing resources include, but are not limited to, the following:

1. **Authorization**: Access shall be granted on a "need to know" basis and shall be authorized by the superintendent, principal, immediate supervisor, or Data Governance Committee with the assistance of the Technology Director and/or Information Security Officer (ISO.) Specifically, on a case-by-case basis, permissions may be added into 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 Data Governance Committee.
2. **Identification/Authentication**: Unique user identification (user ID) and authentication are required for all systems that maintain or access PII, Confidential information, and/or Internal Information. Users will be held accountable for all actions performed on the system with their User ID. User accounts and passwords must NOT be shared.
3. **Data Integrity**: St. Clair 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:

a. Transaction Audits
b. Disk Redundancy (RAID)
c. ECC (Error Correcting Memory)
d. Checksums (file integrity)
e. Hashing
f. Data Encryption
g. Data Wipes

4. **Transmission Security**: Technical security mechanisms are in place to guard against unauthorized access to data that is transmitted over a communications network, including wireless networks. The following features are implemented:

    a. Integrity Controls
    b. Encryption, where deemed appropriate (all SCCBOE Exchange email is encrypted via SSL certificates)

Note**: Only SCCBOE district-supported email accounts will be used for communications to and from school employees, to and from parents or other community members, to and from other educational agencies, to and from vendors or other associations, and to and from students for school business. **All School business conducted in email must only be in the SCCBOE email system.

5. **Remote Access**: Access into St. Clair County Schools' network from outside is allowed using the SCCBOE Portal. All other network access options are strictly prohibited without explicit authorization from the Technology Director, ISO, or Data Governance Committee. Further, PII, Confidential Information and/or Internal Information that is stored or accessed remotely must maintain the same level of protections as information stored and accessed within the St. Clair County Schools' network. PII must only be stored in cloud storage if said storage has been approved by the Data Governance Committee or its designees.

6. **Physical and Electronic Access and Security**: Access to areas in which information processing is carried out must be restricted to only appropriately authorized individuals.

    a. 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 properly secured.
    b. 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.
    c. It is the responsibility of the user to not leave these devices logged in, unattended, and open to unauthorized use. It is also the responsibility of the user to be aware of shoulder-surfing and their surroundings.

XVII. Social Networking

While an absolute ban on electronic communications (IM, Facebook, Snapchat, Email, etc.) between a student and faculty member may seem extreme, everyone should be aware that great caution should be taken in this practice. The St Clair County Board of Education does not recommend faculty having this type communication with students. However, the SCCBOE does recognize there may be an occasional need.

a. Professional and business topics should only be discussed. It is suggested this only be school related communications and such things as a friend request should be avoided.
b. Never discuss private or personal issues.
c. Maintain a record of all conversations.
d. Notify an administrator if a student uses electronic communications to report a crime or abuse.
e. Social Networking is not an approved forum to communicate PII or Student Progress,
f. Social Networking is not an approved forum to communicate Emergency, Legal situations or school status unless approved by Administration.

XVIII. The Following Physical and Security Controls Must Be Adhered To:

A. **Network systems must be installed in an access-controlled area.** The area in and around the computer facility shall afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations outside of industry accepted operational standards.
B. **Monitor and maintain data centers' temperature and humidity levels.** The American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) recommends an inlet temperature range of 68 to 77 degrees and relative humidity of 40% to 55%.
C. **File servers** and or storage containing PII, Confidential and or Internal Information shall be installed in a secure area to prevent theft, destruction or access by unauthorized individuals.
D. **Computers and other systems must be secured** against use by unauthorized individuals. It is the responsibility of the user to not leave these devices logged in, unattended, and open to unauthorized use.
E. **Ensure network systems and network equipment are properly secured** to prevent unauthorized physical access and data is properly safeguarded to protect from loss. A record must be maintained of all personnel who have authorized access.
F. **Maintain a log of all visitors** granted entry into secured areas or areas containing sensitive or confidential data (e.g., data storage facilities). Record the visitor's name, organization, and the name of the person granting access. Retain visitor logs for no less than 6 months. Ensure visitors are escorted by a person with authorized access to the secured area.

G. **Monitor and control the delivery** and removal of all asset-tagged and or data-storing technological equipment or systems. Maintain a record of all such items entering or exiting their assigned location using the district approved technology inventory program. No technology equipment regardless of how purchased or funded shall be moved without the explicit approval of the technology department.
H. **Ensure that technological equipment or systems being removed** for transfer to another organization or being designated as surplus property is appropriately sanitized in accordance with applicable policies and procedures.

XIX. Data Transfer/Exchange/Printing/Storage

A. **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 ISO and include only the minimum amount of information necessary to fulfill the request. A Memorandum of Agreement (MOA) must 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.

B. **Other Electronic Data Transfers and Printing**: PII, Confidential Information, and Internal Information must 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. Secure file transfer software will be used to transmit any confidential information over a secure, encrypted, method of delivery.

C. **Oral Communications**: St. Clair County Schools' staff shall be aware of their surroundings when discussing PII and Confidential Information. This includes but is not limited to the use of cellular telephones in public areas. St. Clair County Schools' staff must not discuss PII or Confidential Information in public areas if the information can be overheard. Caution must be used when conducting conversations in semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation etc.

D. **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 annually. 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.

E. **Evaluation**: St. Clair 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.

F. **Physical Storage**: Physical storage devices, such as flash drives, will not be used to store files on for transport, unless otherwise approved by the Technology Department. Users will utilize provided means of document storage on the cloud and/or server storage for all document storage.

G. **Approved Software**: All software, regardless of whether it is free or purchased, must be vetted and approved by the Information Technology Department. This is to ensure that all software follows the standards to include but not limited to data quality, security, privacy, compliance, and integration with existing tools, along with ease of use and scalability. A list of approved software is located on the district website.

XX. COMPLIANCE

A. The Data Governance Policy applies to all users of St. Clair 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 St. Clair County Board of Education EMPLOYEE HANDBOOK 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 St. Clair County Schools' policies. Further, penalties associated with state and federal laws may apply.

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

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

5. Unauthorized use of an authorized password to invade student or employee privacy by examining records or information for which there has been no request for review
6. Installation or use of unlicensed or unapproved software on St. Clair County Schools' technological systems, including cloud systems.
7. The intentional unauthorized altering, destruction, or disposal of St. Clair County Schools' information, data and/or systems. This includes the unauthorized removal from SCCBOE any technological systems such as but not limited to laptops, internal or external storage, computers, servers, backups or other media, copiers, etc. that contain PII or confidential information.
8. An attempt to gain access to log-in codes for purposes other than for support by authorized technology staff, including the completion of fraudulent documentation to gain access.

End of Document

Questions

If you have any questions or comments about these guidelines, please contact your principal or immediate supervisor. If you do not have any questions, the St. Clair County School System presumes that you understand and are aware of the rules and guidelines and must adhere to them.