Data Governance Policy

Talladega County Schools

in accordance with State Board of Education Resolution
Action Item No. G.2.a - October 10, 2013

TABLE OF CONTENTS

Introduction

Protecting our students' and staff members' privacy is a priority of the Talladega County School District. The school system is committed to maintaining strong and meaningful privacy and security protections. The privacy and security of all personally identifiable information is a significant responsibility, and we value the trust of our students, parents, and staff.

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

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

A data governance policy should be a living document. To make the document flexible, the procedures and processes are in the Appendices. 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 Talladega County Schools website.

2017-2018 Data Governance Committee

The Talladega County Schools 2019-2020 Data Governance committee consists of Dr. Suzanne Lacey, Superintendent; Kelvin Cunningham, Director of Operations; Dr. Karen Culver, Coordinator of Personnel; Emily Harris, Coordinator of Instruction; Mr. Griff Hill, Coordinator of Secondary Schools; Mrs. Kristin Harrell, Coordinator of Special Education; Mrs. Vicky Ozment, Deputy Superintendent; Emily Nestor, Educational Technology Specialist; Joseph Turner, Network Administrator, and Dr. Brooke Morgan, Coordinator of Innovative Learning. For the 2020-2021 school year, Dr. Brooke Morgan will be acting Information Security Officer (ISO). All members of the Talladega County Schools Administrative Team will serve in an advisory capacity to the committee and will be called upon to attend meetings when the topic of the meeting requires his or her expertise.

Committee Meetings

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

Talladega County Schools Data and Information Governance and Use Policy

I. POLICY

A. It is the policy of Talladega 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.

B. The data governance policies and procedures are documented and reviewed annually by the data governance committee.

C. Talladega County Schools conducts annual training on their data governance policy and documents that training.

D. The terms data and information are used separately, together, and interchangeably throughout the policy. The intent is the same.

II. 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 data and information, including but not limited to:

A. Speech, spoken face to face, or communicated by phone or any current and future technologies,

B. Hard copy data printed or written,

C. Communications sent by post/courier, fax, electronic mail, text, chat and or any form of social media, etc.,

D. Data stored and/or processed by servers, PC's, laptops, tablets, mobile devices, etc., and

E. Data stored on any type of internal, external, or removable media or cloud based services.

III. REGULATORY COMPLIANCE

The district will abide by any law, statutory, regulatory, or contractual obligations affecting its data systems. Talladega 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)

See also Appendix A (Laws, Statutory, Regulatory, and Contractual Security Requirements.)

IV. RISK MANAGEMENT

A. A thorough analysis of all Talladega County Schools' data networks and systems is conducted on a periodic basis to document and eliminate any threats and vulnerabilities to stored and transmitted data.

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.

**** See also Appendix B (Information Risk Management Practices)***
**** See also Appendix C (Definitions and Responsibilities)***

V. 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.

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

VI. 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 Talladega County Schools and to be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

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

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

See also Appendix E (Acquisition of Software Procedures)

C. 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 are not authorized to turn off or disable Talladega County Schools' protection systems or to install other systems.

See also Appendix F (Virus, Malware, Spyware, Phishing and SPAM Protection)

D. 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 Talladega 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 methods:

1. **Authorization:** Access will be granted on a "need to know" basis and must 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 in 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 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 IDs must NOT be shared.

3. **Data Integrity:** Talladega 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 duplicate server 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
4. **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 TCS district-supported email accounts should 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.***
    ****See also Resource 4: Excerpts from Email Guidelines***

5. **Remote Access:** Access into Talladega County Schools' SIS from outside is allowed using the TCS web portal. All other network access options are strictly prohibited without explicit authorization from the Technology Coordinator, 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 Talladega County Schools' network.

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. **Passwords are recommended to be changed on a regular basis.**

- No PII, Confidential and/or Internal Information should 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 should 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.

See also Appendix G (Physical and Security Controls Procedures.)
See also Appendix H (Password Control Standards.)
See also Appendix I (Purchasing and Disposal Procedures.)
See also Appendix J (Data Access Roles and Permissions.)

E. Data Transfer/Exchange/Printing:

1. **Electronic Mass Data Transfers:** Downloading, uploading or transferring PII, Confidential Information, and Internal Information between systems must be strictly controlled. Requests for mass download of, or individual requests for, information for research or any other purposes that include PII must be in accordance with this policy and be approved by the data governance committee. All other mass downloads of information must 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) or Privacy Policy, provided by the receiving party, 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. Any Privacy Policy provided by the external entity must outline and ensure compliance to FERPA and any other applicable laws and policies. All points in the attached sample MOA must be referenced in the Privacy Policy.

See also Appendix K (Talladega County Schools Memorandum of Agreement.)

2. **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 must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise. PII that is downloaded for educational purposes where possible should be de-identified before use.

F. Oral Communications: Talladega County Schools' staff should 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. Talladega County Schools' staff should not discuss PII or

Confidential Information in public areas if the information can be overheard. Caution should be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.

G. 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.

H. Evaluation: Talladega County Schools requires that periodic technical and non-technical evaluations be performed in response to environmental or operational changes affecting the security of electronic PII to ensure its continued protection.

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

VII. COMPLIANCE

A. The Data and Information Governance and Use Policy applies to all users of Talladega 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 in accordance with applicable Talladega 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 Talladega County Schools' policies. Further, penalties associated with state and federal laws may apply.

B. Possible 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 login code (User ID and password).
3. An attempt to obtain a login 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 software on Talladega County Schools technological systems.
7. The intentional unauthorized alteration, destruction, or disposal of Talladega County Schools' information, data and/or systems. This includes the unauthorized removal from TCS 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.

8. An attempt to gain access to log-in codes for purposes other than official business, including the completion of fraudulent documentation to gain access.
9. Unauthorized installation of software licensed to Talladega County Schools on non-TCS computers or other systems.

Laws, Statutory, Regulatory, and Contractual Security Requirements
Appendix A

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 must include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.
For more information, see: http://www.fcc.gov/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,
See www.coppa.org for details.

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 students specific rights with respect to their data.
For more information, see: http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

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: http://www.hhs.gov/ocr/privacy/hipaa/understanding/
In general, schools are not bound by HIPAA guidelines.

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

Consent before students are required to submit to a survey that concerns one or more of the following protected areas ("protected information survey") if the survey is funded in whole or in part by a program of the U.S. Department of Education (ED)–

1. Political affiliations or beliefs of the student or student's parent;

2. Mental or psychological problems of the student or student's family;
3. Sex behavior or attitudes;
4. Illegal, antisocial, self-incriminating, or demeaning behavior;
5. Critical appraisals of others with whom respondents have close family relationships;
6. Legally recognized privileged relationships, such as with lawyers, doctors, or ministers;
7. Religious practices, affiliations, or beliefs of the student or parents; or
8. Income, other than as required by law to determine program eligibility.

Receive notice and an opportunity to opt a student out of –

1. Any other protected information survey, regardless of funding;
2. Any nonemergency, invasive physical exam or screening required as a condition of attendance, administered by the school or its agent, and not necessary to protect the immediate health and safety of a student, except for hearing, vision, or scoliosis screenings, or any physical exam or screening permitted or required under State law; and
3. Activities involving collection, disclosure, or use of personal information obtained from students for marketing or to sell or otherwise distribute the information to others.

For more information, see: http://www2.ed.gov/policy/gen/guid/fpco/ppra/index.html

Information Risk Management Practices
Appendix B

The analysis involved in Talladega County Schools Risk Management Practices examines the types of threats – internal or external, intentional or unintentional, natural or manmade, electronic and nonelectronic – 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 and Responsibilities

Appendix C

Definitions

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

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

C. Data: Facts or information

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

E. Data Integrity: Data or information has not been altered or destroyed in an unauthorized manner.

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

G. Involved Systems: All data-involved computer equipment/devices and network systems that are operated within or by the Talladega 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.

H. 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.

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

Responsibilities

A. Data Governance Committee: The Data Governance Committee for Talladega 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:

1. Reviewing the Data and Information Governance and Use Policy annually and communicating changes in policy to all involved parties.
2. 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 Talladega County Schools is responsible for working with the Superintendent, 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. Advising owners in the identification and classification of technology and data related resources.

See also Appendix D (Data Classification Levels.)

3. 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.
4. Performing or overseeing security audits.
5. Reporting regularly to the superintendent and Talladega County Schools Data Governance Committee on Talladega County Schools' status with regard to information security.

C. User Management: Talladega 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, changing security system passcodes, etc.
5. Providing employees with the opportunity for training needed to properly use the computer systems.
6. Reporting promptly to the ISO and the Data Governance Committee the loss or misuse of Talladega 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.

D. 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 the Talladega County Schools Information Owner Delegation/Transfer Request Form and submitting the form to the Data Governance Committee for approval. The owner of information has the responsibility for:

1. Knowing the information for which she/he is responsible.
2. Determining a data retention period for the information, relying on 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 ISO the loss or misuse of Talladega County Schools' data.
7. Initiating corrective actions when problems are identified.
8. Promoting employee education and awareness by utilizing programs approved by the ISO, 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.

E. Data Custodian: The data custodian is assigned by an administrator, data owner, or the ISO 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:

1. Providing and/or recommending physical safeguards.
2. Providing and/or recommending procedural safeguards.
3. Administering access to information.
4. Releasing information as authorized by the Information Owner and/or the ISO and/or Data Governance Committee for use and disclosure using procedures that protect the privacy of the information.
5. Maintaining information security policies, procedures and standards as appropriate and in consultation with the ISO and/or Data Governance Committee.
6. Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
7. Reporting promptly to the ISO and/or Data Governance Committee the loss or misuse of Talladega County Schools data.
8. Identifying and responding to security incidents and initiating appropriate actions when problems are identified.

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:

1. Access information only in support of their authorized job responsibilities.
2. Comply with all data security procedures and guidelines in the Talladega County Schools Data and Information Governance and Use Policy and all controls established by the data owner and/or data custodian.
3. Keep personal authentication devices (e.g. passwords, secure cards, PINs, access codes, etc.) confidential.
4. Report promptly to the ISO and/or Data Governance Committee the loss or misuse of Talladega County Schools' information.
5. Follow corrective actions when problems are identified.

Data Classification Levels

Appendix D

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.
   b. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
2. Unauthorized or improper disclosure, modification, or destruction of this information could violate state and federal laws; result in civil and criminal penalties, and cause serious legal implications for Talladega 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 business need for access.**
   Examples of Confidential Information may include: personnel information, key financial information, proprietary information of commercial research sponsors, system access passwords and information file encryption keys.
2. Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for Talladega County Schools, its staff, parents, students, contract employees, or 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 Talladega County Schools, and in some cases within affiliated organizations such as Talladega County Schools’ business or community partners. This type of information is already widely distributed within Talladega County Schools, or it could be distributed within the organization without advance permission from the information owner.
   Examples of Internal Information may include: personnel directories, internal policies and procedures, most internal electronic mail messages.
2. Any information not explicitly classified as PII, Confidential or Public will, by default, be classified as Internal Information.
3. Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.

D. Public Information

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

E. Directory Information

1. Talladega County Schools defines Directory information as follows:
2. Student first and last name
3. Student home address
4. Student telephone number
5. Student date of birth
6. Major field of student
7. Official activities
8. Student dates of attendance (from and to)
9. Dates of enrollment
10. Student weight and height for members of school athletic teams
11. Student diplomas, honors, awards received
12. Student photograph
13. Student gender
14. Student school-assigned monitored and filtered email address
15. Student grade level
16. Student participation in school activities or school sports
17. Student most recent institution/school attended
18. Student ID number

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

Acquisition of Software Procedures
Appendix E

The purpose of the Acquisition of Software Procedures is to:

- Ensure proper management of the legality of information systems,
- Allow all academic disciplines, administrative functions, and athletic activities the ability to utilize proper software tools,
- Minimize licensing costs,
- Increase data integration capability and efficiency of Talladega County Schools as a whole, and
- Minimize the malicious code that can be inadvertently downloaded.

A. Software Licensing:

1. All district software licenses owned by TCS will be:
   - kept on file at the central office,
   - accurate, up to date, and adequate, and
   - in compliance with all copyright laws and regulations
2. All other software licenses owned by departments or local schools will be:
   - kept on file with the department or local school technology office,
   - accurate, up to date, and adequate, and
   - in compliance with all copyright laws and regulations
3. Software installed on TCS technological systems and other electronic devices:
   - will have proper licensing on record,
   - will be properly licensed or removed from the system or device, and
   - will be the responsibility of each TCS employee purchasing and installing to ensure proper licensing
4. Purchased software and solutions accessed from and storing data in a cloud environment will have a Memorandum of Agreement (MOA) on file that states or confirms at a minimum that:
   - TCS student and/or staff data will not be shared, sold, or mined with or by a third party,
   - the company will comply with TCS guidelines for data transfer or destruction when contractual agreement is terminated, and
   - No API will be implemented without full consent of TCS and the ALSDE.
5. Software with or without physical media (e.g. downloaded from the Internet, apps, or online) must still be properly evaluated and licensed if necessary and is applicable to this procedure. It is the responsibility of staff to ensure that all electronic resources are age appropriate, FERPA compliant, and are in compliance with software agreements before requesting use. Staff members are responsible for ensuring that parents have given permission for staff to act as their agent when creating student accounts for online resources.

B. Supported Software:

In an attempt to prevent software containing malware, viruses, or other security risk, software is categorized as Supported and Not Supported Software. For software to be classified as Supported,

Software downloads and/or purchases must be approved by the district technology director or designee such as a local school technology coordinator or member of the technical staff.

1. A list of supported software will be created and maintained on the TCS District Technology site.
2. It is the responsibility of the TCS Technology Team members to keep the list current and for staff to submit apps or other software to the Technology Team for approval.
3. Unsupported software is considered New Software and must be approved or it will not be allowed on TCS owned devices.
4. When staff recommends apps for the TCS Mobile Device Management Apps Kiosk (Filewave) or software for installation, **it is assumed that the staff has properly vetted the app or software and that it is instructionally sound, is in line with curriculum or behavioral standards, and is age appropriate.**
5. Software that accompanies adopted instructional materials will be vetted by the Coordinator of Instruction and the Coordinator of Instructional Technology and is therefore supported.

C. New Software:

In the Evaluate and Test Software Packages phase, the software will be evaluated against current standards and viability of implementation into the TCS technology environment and the functionality of the software for the specific discipline or service it will perform.

1. Evaluation may include but is not limited to the following:
   - Conducting beta testing.
   - Determining how the software will impact the TCS technology environment such as storage, bandwidth, etc.
   - Determining hardware requirements.
   - Determining what additional hardware is required to support a particular software package.
   - Outlining the license requirements/structure, number of licenses needed, and renewals.
2. Determining any Maintenance Agreements including cost.
   - Determining how the software is updated and maintained by the vendor.
   - Determining funding for the initial purchase and continued licenses and maintenance.
3. When staff recommends apps for the TCS Mobile Device Management Apps Kiosk (Filewave) or software for purchase and/or testing, it is the responsibility of the appropriate staff to properly vet the app or software to ensure that is instructionally sound, is in line with curriculum or behavioral standards, and is age appropriate.

Virus, Malware, Spyware, Phishing and SPAM Protection
Appendix F

Virus, Malware, and Spyware Protection
Talladega County Schools Windows OS desktops, laptops, and file-servers run the Kaspersky Software Suite. Virus definitions are updated regularly and an on-access scan is performed on all "read" files continuously. A full scheduled scan runs every day or at the next time the computer/laptop is turned on. A full scheduled scan is performed on all file-servers daily.

Internet Filtering
Student learning while using online content and social collaboration continues to increase. Talladega County Schools views Internet filtering as a way to balance safety with learning—letting good content, resources, and connections in, while blocking the bad. To balance educational Internet resource and app use with student safety and network security, the Internet traffic from all devices that authenticate to the network is routed through the selected filtering solution using the user's network credentials. For companion devices and guest devices, users see a "pop-up screen" that requires them to login to network and thus, the Internet filter with his/her 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, etc. are blocked.

Phishing and SPAM Protection
In addition to the built in spam filtering for Google Mail, email is filtered by Barracuda Email Filtering Software for viruses, phishing, spam, and spoofing.

Security Patches
Windows security patches and other Windows patches are scheduled to "auto-download" and "schedule install." The schedule install occurs daily at 3:00 a.m. File-servers are scheduled to "auto-download" and are automatically updated 3:00 a.m. after which the file-server is automatically re-booted.

Physical and Security Controls
Appendix G

The following physical and security controls must be adhered to:

At this time, various network systems are installed in an access-controlled area. However, not all systems meet this criteria. The goal of the Talladega County School System is that all network systems, including the area in and around the computer facility, be adequately protected against environmental hazards such as power outages and extreme temperature situations. Fire and water damage prevention will be implemented where applicable. The goal for this level of physical security to be implemented is Spring of the 2020-2021 academic year.

Data centers must be monitored and maintain acceptable 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%.

File servers and/or storage containing PII, Confidential and/or Internal Information must be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.

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.

Systems and network equipment are properly secured to prevent unauthorized physical access and data is properly safeguarded to protect from loss. A record shall be maintained of all personnel who have authorized access.

Visitors are never granted entry into secured areas or areas containing sensitive or confidential data (e.g., data storage facilities). Should a secured area require access by a third party (e.g., contracted repair technicians, inspectors), information regarding the visitor must be recorded and include the visitor's name, date, time, organization, and the name of the person granting access. This information will be forwarded to the Coordinator of Technology and the Maintenance and Operations Director within 24 hours. Any visitors must be escorted by person(s) with authorized access to the secured area.

*The delivery and removal of all asset-tagged and/or data-storing technological equipment or systems must be controlled and documented. Records of all such items entering or exiting their assigned location must be kept using the district approved technology inventory program. No technology equipment regardless of purchasing or funding method should be moved without the explicit approval of the Coordinator of Technology.

See also Appendix I (Purchasing and Disposal Procedures.)

Password Control Standards

Appendix H

Password Standards:

The Talladega County Schools Data Governance and Use Policy require the use of strictly controlled passwords for network access and for access to secure sites and information. In addition, all users are assigned to Microsoft security groups that are managed through Microsoft Group Policies. The security groups include separate groups for **Staff** and **Students**.

Password Standards:

A. Users are responsible for complying with the following password standards for network access or access to secure information:

1. Passwords must never be shared with another person, unless the person is designated technology personnel, and there is a legitimate need to know.
2. Every password must, where possible, be changed yearly if not more frequently for staff and when there is an identified need for students. Student passwords are generated through an automated process, but may be changed if a student's account(s) are compromised.
3. Passwords must, where possible, have a minimum length of eight (8) characters.
4. When possible, for secure sites and/or software applications, **user created** passwords should adhere to the same criteria as required for network access. This criteria is defined in the TCS Network Group Policy Criteria for Passwords and is listed below:
   - Should NOT contain the user's account name or parts of the user's full name that exceed two consecutive characters.
   - MUST contain characters from three of the following four categories:
     1. English uppercase characters (A through Z)
     2. English lowercase characters (a through z)
     3. Base 10 digits (0 through 9)
     4. Non-alphabetic characters (for example, !, $, #, %)
5. Passwords must never be saved when prompted by any application with the exception of central single sign-on (SSO) systems as approved by the Technology Department. This feature should be disabled in all applicable systems.
6. Passwords must not be programmed into public access digital devices or recorded anywhere that someone may find and use them.
7. When creating a password for secure information or sites, it is important not to 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 alpha and numeric characters is more difficult to guess. Using phrases that are easy to remember, but not commonly associated together are the most difficult to guess.

B. Where possible, system software should enforce the following password standards:

1. Passwords routed over a network must be encrypted.
2. Passwords must be entered in a non-display field.
3. System software must enforce the changing of passwords and the minimum length.
4. Where applicable, users are expected to set a lockout time/lock screen time to begin no longer than 30 minutes from the last time the device was accessed.
5. System software should maintain a history of previous passwords and prevent their being easily guessed due to their association with the user. A combination of alpha and numeric characters is more difficult to guess.

Purchasing and Disposal Procedures

Appendix I

This procedure is intended to provide for the proper purchasing and disposal of technological devices only. Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, AV equipment, server, internal or external storage, communication device or any other current or future electronic or technological device may be referred to as **systems** in this document. For further clarification of the term technological systems contact the Talladega County Schools' (TCS) district Coordinator of Technology.

All involved systems and information are assets of Talladega County Schools and must be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

A. Purchasing Guidelines

All systems that will be used in conjunction with Talladega County Schools' technology resources or purchased, regardless of funding, should be **purchased from an approved list** and **be approved by the district Coordinator of Technology or designee**. *Failure to have the purchase approved may result in lack of technical support, request for removal from premises, or denied access to other technology resources*. Note: These guidelines assist in ensuring the TCS Technology Department can support the system, the purchased systems are compatible with existing systems, the TCS district or local school will not be required to purchase additional components or systems to ensure the purchased systems operate correctly, and the purchases are being made in accordance with the Alabama Competitive Bid Laws. See section B, below, for information on these laws.

B. Alabama Competitive Bid Laws

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,

Talladega 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. In the event that a desired product is not included in one of these agreements, Talladega County Schools bids the item or items using the district's competitive bid process or may use an approved alternative joint purchasing cooperative to meet the competitive bid law requirements. **All technological systems, services, etc. that will exceed $15,000 in one purchase OR cumulative purchases within a single fiscal year, and which are purchased with public funds are subject to Alabama's competitive bid laws. Cumulative purchases and single purchases are identified as purchases made by the TCS district office AND all local schools… COMBINED.**

C. Inventory

All technological devices or systems over $500 are inventoried by the Technology Department in accordance with the Talladega County Schools' Finance Department using a fixed asset system. There are some exceptions under $500, as determined by the Technology Coordinator, that are also inventoried, but not using the fixed asset system. It is the responsibility of the local school Principal or his or her designee to inventory technological systems used in the local school and to manage said inventory. The district technology staff is responsible for ensuring that any **network equipment**, file servers, or district systems, etc. are inventoried.

D. Disposal Guidelines

Equipment should be considered for disposal for the following reasons:

1. End of useful life
2. Lack of continued need
3. Obsolescence
4. Wear, damage, or deterioration,
5. Excessive cost of maintenance or repair

The local school Principal, Coordinator of Technology, and the Director of Finance must approve school disposals by discard or donation. Disposal must follow all appropriate financial procedures, applicable state and federal laws, and environmental requirements. Contact the Coordinator of Technology before disposing of any technological systems.

E. Methods of Disposal

Once equipment has been designated and approved for disposal, it should be handled according to one of the following methods. It is the responsibility of Principal or his or her designee to make changes to the inventory that reflect any in-school transfers, in-district transfers, donations, or discards for technological systems. Fixed assets must be changed using the fixed asset system within the District Business Office. The district technology staff is responsible for modifying the inventory records to reflect any transfers within the central offices, transfers of central office technology systems to local schools, central office donations, or central office discards. Licensing of software products used on the device must be removed.

Transfer/Redistribution
If the equipment has not reached the end of its estimated life, an effort should 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. Helpdesk requests may be entered to have the equipment moved, reinstalled and, in the case of computers, laptops, or other, have it wiped and reimaged or configured.

Discard
All electronic equipment in the Talladega 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. The local school Principal or his or her designee must ensure that discarded systems no longer contain any PII and must sign a confirmation document stating such upon retrieval of the discard by local Technology Department personnel or other.

A district-approved vendor must 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 Talladega County Schools and/or the employee who disposed of the equipment liable for violating environmental regulations or laws or violating privacy laws, should the systems contain PII.

Donation
If the equipment is in good working order, but no longer meets the requirements of the site where it is located, and cannot be put into use in another part of a school or system, it may be donated upon the written request of the receiving public school system's superintendent or non-profit organization's director. The Chief Financial Officer, the Coordinator of Technology, and the Superintendent must approve any donation.

It should be made clear to any school or organization receiving donated equipment that TCS is not agreeing to and is not required to support or repair any donated equipment. It is donated AS IS.

TCS staff should make every effort before offering donated equipment, to make sure that it is in good condition and can be reused. Microsoft licenses or any other software licenses are not transferred outside the Talladega County School System.

Donations are prohibited to any individual person (must be an organization).

Systems that are donated TO the Talladega County School system, its local schools, or any teacher of an individual classroom where the systems will be used for daily operations or for the instruction of students becomes the property of the Talladega County School system and must be managed appropriately according to procedures in place for fixed assets, device management, Internet safety protocols, etc.

For purchases, transfers and redistributions, donations, and disposal of technology-related equipment, it is the responsibility of the appropriate technology department member to create/update the inventory to include previous location, new school and/or room location, and to note the transfer or disposal information. When discarding equipment, any fixed asset tag is removed from the equipment and turned in with other documentation to the local school bookkeeper. When equipment is donated, a copy of the letter requesting the equipment must be on-file with the district technology office prior to the donation. Equipment is donated in order of request.

Any equipment donated should be completely wiped of all data. This step will not only ensure that no confidential information is released, but also will ensure that no software licensing violations will inadvertently occur. For non-sensitive machines, all hard drives should be fully erased using an approved method by the district technology office, followed by a manual scan of the drive to verify that zeros were written.

Any re-usable hardware that is not essential to the function of the equipment that can be used as spare parts should be removed: special adapter cards, memory, hard drives, CD drives, etc.

A district-approved vendor MUST handle all disposals that are not redistributions, transfers, or donations. Equipment should be stored in a central location prior to pick-up. Summary forms must be turned into district technology office and approved by the Chief Financial Officer prior to the scheduled retrieval day. Mice, keyboards, and other small peripherals may be boxed together and should not be listed on summary forms.

Data Access Roles and Permissions

Appendix J

Talladega County Schools maintain the following permission groups in INow:

1. Administrators
2. 504 Coordinator - School level
3. Attendance Clerk
4. Career Tech teacher
5. Certified UnLicensed Medication Assistant
6. Chalkable Group
7. Clerical
8. Contract Help
9. Counselor
10. District School Nurse
11. District Personnel Administrator
12. Enrollment Clerk
13. Health Data Personnel
14. IHealth Admin
15. Oscar Inst
16. PE Teacher
17. Principals Asst Prin
18. SETS Staff
19. Substitute School Nurse
20. Teacher
21. View Only

***Complete list of Permissions available upon request.**

Resource 3: Record Disposition Requirements

The information below is from the Local Boards of Education Records Disposition Authority approved by the Local Government Records Commission, October 2, 2009. The complete document can be found at: http://www.archives.alabama.gov/officials/localrda.html.

The following sections are of special interests:
1.04 Administrative Correspondence
4.02 20-Day Average Daily Membership Reports
4.04 Principals Attendance Reports
6.01 Student Handbooks
6.03 Daily/Weekly Teacher Lesson Plans
9.14 Websites
10.04 Purchasing Records
10.05 Records of Formal Bids
10.06 Contracts
10.08 Grant Project Files