TUSCALOOSA COUNTY
School System

Data Governance and Use Policy & Procedures

Introduction

Data Governance focuses on improving data quality, protecting access to data, establishing definitions of security, maintaining data and documenting data policies. The role of all employees is to ensure that the highest quality of data possible is delivered throughout the entire school system. Protecting our students' and staff's privacy is an important priority. The Tuscaloosa County School System understands that the privacy and security of personal identifiable information and data is a significant responsibility.

The Tuscaloosa County Schools Data Governance document includes information regarding the Data Governance Committee, the Tuscaloosa County School System Data Governance and Use Policy and Procedures, applicable Appendices, and Supplemental Resources. Tuscaloosa County Schools expects its employees to abide by the requirements of these procedures; however, nothing herein shall be construed to create any liability, legal entitlement, or duty to a third party not specifically provided by law.

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

The procedures are a living document, and the Data Governance Committee may quickly modify them in response to changing needs or a change in technology. All modifications will be posted on the Tuscaloosa County Schools website.

The Tuscaloosa County School System Data Governance Policy will be reviewed annually, and changes will be made as necessary to ensure state and federal guidelines are being followed. All modifications will be posted on the Tuscaloosa County School System's website.

Committee Meetings

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

Committee Members

2021 – 2022 Data Governance Committee

The Tuscaloosa County Schools 2021-2022 Data Governance committee consists of the following members:
Dr. Keri Johnson – Superintendent
Mr. Michael Townsend – Director of Information Technology
Mr. Kirk Junkin – Technology Data Manager
Mr. Mark Franks - Director of Federal Funds
Dr. David Scott – Director of Elementary Education
Dr. Lillie Lewis – Coordinator of Elementary Education
Dr. Daniel Bray – Director of Secondary Education
Mrs. Deidra Crain – Coordinator of Secondary Education
Mr. Ben White – Principal, Cottondale Elementary School
Mrs. Autumn Franks – Principal, Northside Middle School
Dr. John Hooper, – Principal, Sipsey Valley High School
Mrs. Cristal Avent – School Technology Team Leader, Northport Elementary School
Mr. Daniel Wolfe – School Technology Team Leader, Echols Middle School
Mr. Robby Workman – School Technology Team Leader, Tuscaloosa County High School

Mr. Michael Townsend will serve as Chairman and shall be acting Information Security Officer (ISO).
Mr. Kirk Junkin is the Data Manager, for the Data Governance Committee.

All members of the Tuscaloosa County Schools Administrative Team and the Information Technology Department 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.

Tuscaloosa County Schools' Data Governance and Use Policy

A. PURPOSE

The purpose of the Data Governance and Usage policy is to protect data or information in all its forms (written, electronic, or printed) from accidental or intentional unauthorized modification, destruction, and/or disclosure throughout its life cycle. This includes an appropriate level of security over the equipment, software, and practices used to process, store, and transmit data or information. The intent of these procedures is to implement the laws governing the confidentiality of the Tuscaloosa County Schools' records and to protect the integrity and accuracy of the system's electronic data. Nothing in these procedures is intended to create or expand any entitlement to confidentiality of records beyond that which is established by law. Furthermore, nothing herein should be deemed to create or expand any entitlement to copies of such records beyond what is established by law. In general, Tuscaloosa County Schools reserves the right to adopt, revise, interpret, amend, repeal, suspend, or apply its policies and procedures according to its assessment of the needs and interests of the school system; subject only to such limitations on the exercise of such prerogatives as may be imposed by law.

These procedures are authorized by the Tuscaloosa County Board of Education 5.90 Technology Acceptable Use policy:

> "The Superintendent is authorized to establish procedures governing the storage, use, and sharing of data maintained electronically by the school system. Such procedures shall comply with applicable state and federal law and shall include provisions for data security (including physical security measures), access controls, quality control, and data exchange and reporting (including external data requests, and third-party data use). Nothing in this policy or in any procedures authorized hereunder creates or expands any entitlement to confidentiality of records beyond that which is established by law or specific Board policy.
>
> Any unauthorized access, use, transfer, or distribution of Board data by any employee, student, or any other individual may result in disciplinary action (up to and including termination for employees) and other legal action."

The data governance policies and procedures will be documented and reviewed annually by the Data Governance Committee. Each of the Tuscaloosa County Schools will conduct annual training on the district data governance policy and procedures, and document that training. The terms data and information are used separately, together, and interchangeably throughout the policy. The intent is the same.

B. SCOPE

The Superintendent is authorized to establish, implement, and maintain data and information security measures. These procedures apply to all electronically stored forms of Tuscaloosa County Board of Education data and information and are intended to protect information that is deemed confidential by law and to prevent unauthorized modification, destruction, or disclosure of the system's electronic records. The policy, standards, processes, and procedures outlined herein 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 includes all forms of such records and/or information derived from such records, 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, desktop computers, laptops, tablets, mobile devices, etc.; and/or

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

C. REGULATORY COMPLIANCE

The district will abide by any law, statutory, regulatory, or contractual obligations affecting its data systems. Tuscaloosa 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. Payment Card Industry Data Security Standard (PCI DSS)

E. Health Insurance Portability and Accountability Act (HIPAA)

F. Protection of Pupil Rights Amendment (PPRA)

* **See also *Appendix A: Laws, Statutory, Regulatory, and Contractual Security Requirements***

D. RISK MANAGEMENT

I. A thorough analysis of Tuscaloosa County Schools' data networks, systems, policies, and procedures will be conducted on an annual basis. All vulnerabilities found during the annual risk analysis will be reviewed by the Data Governance committee and addressed based on the recommendations by the Data Governance committee.

II. Periodic risk assessments to identify, quantify, and prioritize risks may be conducted at the request of the Superintendent, Internet Security Officer (ISO), or Director of Technology. The risk assessment shall be used as the basis for a plan to mitigate identified threats and risks by reducing the amount and scope of the vulnerabilities. The Data Governance Committee will be informed of periodic assessments and resulting the corrective action plan, if needed.

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

E. 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 it includes. 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***

F. SYSTEMS AND INFORMATION CONTROL

Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, audio-visual equipment, server, internal or external storage, communication device or any other current or future electronic or technological device may be referred to as systems for purposes of these procedures. All involved systems and information are assets of Tuscaloosa County Schools and are expected to be protected from misuse, unauthorized modification, and/or destruction. These protection measures may be physical and/or software based.

A. Ownership of Software

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

B. Software or Cloud-based Software

Software or cloud-based software that directly accesses any Tuscaloosa County Schools' data classified as Personally Identifiable Information (PII) or Restricted/Confidential Information shall be covered by the Memorandum of Agreement (MOA) signed by the software proprietor. The MOA applies to both purchased and free software. A current and accurate copy of the software license agreement must be kept by the purchaser in either paper or electronic form. Financial records and agreements detailing the purchase and terms of the software acquisition will be kept, in paper or electronic form, by the Chief School Financial Officer or local bookkeeper.

C. Software Installation and Use

All software packages that reside on technological systems within or used by Tuscaloosa County Schools must comply with applicable licensing agreements and restrictions and must comply with Tuscaloosa County Board of Education acquisition of software procedures.

* **See also *Appendix E: Acquisition of Software Procedures***

D. Virus, Malware, Spyware, Phishing and SPAM Protection

Virus checking systems approved by the Information Technology Department are deployed using a multi-layered approach (computers, servers, firewalls, filters, Access Control List, etc.) that scans for viruses, malware, spyware, phishing, and SPAM. Users are not authorized to turn off or disable Tuscaloosa County Information Technology Department's protection systems or to install other systems.

E. Access Controls

Physical and electronic access to information systems that contain Personally Identifiable Information (PII), Restricted/Confidential and Internal information, and computing resources is controlled. To ensure appropriate levels of access by users, a variety of security measures are instituted as recommended by the Information Technology Department and approved by the Tuscaloosa County Schools'Data Governance Committee. Mechanisms to control access to PII, Restricted/Confidential information, Internal information and computing resources include, but are not limited to, the following methods:

a. 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 Director of Information Technology and/or Technology Data Manager. Specifically, on a case-by-case basis, additional permissions may be added to those already held by individual users in the student management system, to fulfill specific job responsibilities, with approval of the Data Governance Committee.

*See also *Appendix J: Data Access Roles and Permissions*

b. Identification/Authentication

Unique user identification (user ID) and authentication are required for all systems that are maintained or used to access PII, Confidential information, Internal Information and/or Directory Information. Users will be held accountable for all actions performed on systems accessed with their User ID. Therefore, user IDs must NOT be shared with other individuals or third-party users. In addition, the Information Technology Department provides Self-Registration to allow staff to retrieve and reset/retrieve passwords.

*See also *Appendix H: Password Control Standards*

c. Data Integrity/Data Quality

Tuscaloosa County Schools provide safeguards so that PII, Restricted/Confidential, and Internal Information, and Directory Information is not altered and/or destroyed in an unauthorized manner. Core data are backed up to onsite and offsite storage for disaster recovery. In addition, listed below are methods that are used for data integrity in various circumstances:

i. Transaction audit
ii. Disk redundancy (RAID)
iii. ECC (Error Correcting Memory)
iv. Checksums (file integrity)
v. Data encryption
vi. Data wipes

*See also *Appendix G: Physical and Security Controls Procedures*

d. Transmission Security

Technical security mechanisms are in place to guard against unauthorized access to data that are transmitted over all communications networks, including wireless networks.

The following features are implemented:

i. integrity controls
ii. encryption, where deemed appropriate

*See also *Appendix G: Physical and Security Controls Procedures*

e. Remote Access

Access into the Tuscaloosa County School System network from outside is allowed using the TCSS provided virtual private network (VPN) or approved website links. All other network access options are strictly prohibited without explicit authorization from the Director of Technology, Data Manager, Network Operations Manager or Data Governance Committee. Furthermore, PII, Restricted/Confidential Information and/or Internal Information that is stored or accessed remotely must maintain the same level of protection as information stored and accessed within the Tuscaloosa County Board of Education network.

*See also *Appendix G: Physical and Security Controls Procedures*

f. Physical and Electronic Access and Security

Access to areas in which information processing is carried out must be restricted to only appropriately authorized individuals.

i. No PII, Restricted/Confidential Information, Internal Information and/or Directory Information should be stored on a device such as a hard drive, mobile device of any kind, or external storage device that is not either located within a secure area or secured via password or other like electronic security.
ii. No technological systems that may contain information as defined above should be disposed of or moved without adhering to the appropriate inventory and disposal of electronic equipment procedures.
iii. It is the responsibility of the user to not leave technology devices logged in, unattended, and open to unauthorized use.
iv. At a minimum, staff passwords must be changed annually.
v. All staff are required to complete *Self-Registration* to allow passwords to be changed immediately if an account breach is suspected.

*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: Inventory Procedures*

F. Data Transfer/Exchange/Printing

a. **Electronic Mass Data Transfers**

Downloading, uploading, or transferring PII, Restricted/Confidential Information, and Internal Information between systems must be strictly controlled.

i. Internal Requests

Any internal request from within the school system for a mass download of data that includes PII, 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 Superintendent, Data Manager and/or the Data Governance Committee.

ii. **External Requests**: Any external request from outside the school system for a mass download of the school system's electronic records must be approved by the information owner and include only the minimum amount of information necessary to fulfill the request. A Memorandum of Agreements (MOA) or contract must be in place when transferring PII to external entities such as software or application vendors; textbook, testing, yearbook, and photography companies; or any other web-based application, etc. unless an exception has been approved by the Data Governance Committee. The contents of the MOA or contract may vary depending on the reason for the transfer and how the data will be used.

The school system may also release de-identified records and information for purposes such as research, provided all personally identifiable information is removed and a reasonable determination is made that a student's identity is not personally identifiable, whether through single or multiple releases, and considering other reasonably available information.
Such releases should be approved by the Data Governance Committee.

*See also ***Form a: Tuscaloosa County Schools Sample Memorandum of Agreement***

b. **Other Electronic Data Transfers and Printing:** PII, Restricted/Confidential Information, and Internal Information must be stored in a manner inaccessible to unauthorized individuals. PII and Restricted/Confidential Information must not be downloaded, copied, or printed indiscriminately or left unattended and/or open to compromise. PII that is downloaded for educational purposes where possible should be de-identified before use.

c. **Oral Communications:**
   i. Tuscaloosa County Board of Education employees should be aware of their surroundings when discussing PII and Confidential Information that is protected from disclosure by law. This includes but is not limited to the use of cellular telephones in public areas. Caution should be used in public areas if the information can be overheard, i.e., when conducting conversations on campus and off campus, in public locations or on public transportation.
   ii. When communicating through email only Tuscaloosa County Schools' district-supported email accounts should be used. This includes sharing information 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 educational purposes.

d. **Evaluation:** Tuscaloosa County Schools require 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.

e.

G. IT DISASTER RECOVERY

Controls shall be implemented that are designed to allow the Tuscaloosa County Schools to recover from damage to critical systems, data, or information within a reasonable period of time. Each school, department, or individual is required to report a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages data or systems immediately to the Superintendent, Director of Operations, Director of Technology and/or Data Manager for immediate response.

The IT Disaster Plan should include the following:

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

H. COMPLIANCE

1. The Data Governance and Use Policy and its procedures apply to all users of Tuscaloosa 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 potential sanction and disciplinary action up to and including dismissal in accordance with applicable Tuscaloosa County Board of Education procedures, or, in the case of outside affiliates, termination of the affiliation.

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

    a. Unauthorized disclosure of PII or Restricted/Confidential Information.
    b. Unauthorized disclosure of a login code (User ID and password).
    c. An attempt to obtain a login code or password that belongs to another person.
    d. An attempt to use another person's login code or password.
    e. 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.
    f. Installation or use of unsupported software on Tuscaloosa County Schools' technological systems.
    g. The intentional unauthorized modification, manipulation, destruction, or disposal of Tuscaloosa County Schools' information, data, and/or systems. This includes the unauthorized removal of items from TCSS premises containing PII, restricted/ confidential information and directory information including, but not limited to, the following: technological systems, laptops, desktop computers, tablets, copiers, internal or external storage, servers and server components, backups, or other media, etc.

h. The intentional unauthorized modification, manipulation, destruction, or disposal of Tuscaloosa County Schools' information, data, and/or systems. This includes the unauthorized removal of contents and/or parts of technological systems including, but not limited to, laptops, internal or external storage, computers' and/or servers' components, backups or other media, copiers, etc. that contain PII, restricted/confidential information and/or directory information from Tuscaloosa County Schools' premises.
i. An attempt to gain access to login codes for purposes other than official business, including the completion of fraudulent documentation to gain access.

Appendices

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

A. The **Alabama Administrative Code** is a compilation of the rules of all state agencies covered by the Alabama Administrative Procedures Act.
**For more information, visit http://www.alabamaadministrativecode.state.al.us/*

B. Alabama Records Disposition Authority
Alabama Law Section 41-13-23 authorized the Alabama Department of Archives and History to publish regulations for Local Government Records Destruction.
**For more information, visit*
http://www.archives.alabama.gov/officials/rdas/local/EdRDA_04_14.pdf

C. 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 cyber bullying awareness and response.
**For more information, visit* http://www.fcc.gov/guides/childrens-internet-protection-act

D. 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, visit* https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

E. FERPA
The **Family Educational Rights and Privacy Act** applies to all institutions that receive 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, visit* http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

F. 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, visit* www.pcisecuritystandards.org

G. HIPPA
The **Health Insurance Portability and Accountability Act,** applies to organizations that transmit or store Protected Health Information. 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, visit https://www.hhs.gov/hipaa/index.html*

H. PPRA

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

1. Consent before students is required to submit 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-
    a. Political affiliations or beliefs of the student or parent
    b. Mental or psychological problems of the student or student's family
    c. Sexual behavior or attitudes
    d. Illegal, antisocial, self-incriminating, or demeaning behavior
    e. Critical appraisals of others with whom respondents have a close family relationship
    f. Legally recognized privileged relationships (lawyers, minister, doctors, etc.)
    g. Religious practices, affiliations, or beliefs of the student or parent
    h. Income, other than as required by law to determine program eligibility
2. Receive notice and an opportunity to opt a student out of-
    a. Any other protected information survey, regardless of funding
    b. 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
    c. 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, visit* http://www2.ed.gov/policy/gen/guid/fpco/ppra/index.html

Appendix B: Information Risk Management Practices

The analysis involved in Tuscaloosa County Schools Risk Management Practices examines the types of threats– internal or external; natural or manmade; electronic and non-electronic – that affect the ability to manage the information resource. The analysis also documents any existing vulnerabilities found within each entity, which potentially exposes the information resource to the threats. Finally, the analysis includes an evaluation of the information assets and the technology associated with its collection, storage, dissemination, and protection.

From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information is determined and addressed based on recommendations by the Information Technology Department. 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.

Appendix C: Definitions and Responsibilities

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 Tuscaloosa County Schools– regardless of their status. This includes nurses, 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 Tuscaloosa County Schools physically or virtually. This includes all platforms, i.e., operating systems; all computer/device sizes, i.e., personal digital assistants, desktop computers, 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, medical, financial, 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 the Tuscaloosa County School System is responsible for working with the Data Manager, Data Governance Committee Chairman, Director of Technology, or another designee assigned by the Superintendent to ensure security policies, procedures, and standards are in place and adhered to by the entity. Other responsibilities include:

1. Reviewing the Data Governance and Use Policy and Procedures annually and communicating changes in procedure to all involved parties.
2. Educating data custodians and information owners and users with comprehensive information about security controls affecting system users and application systems.

B. Information Security Officer (ISO): The ISO is responsible for working with the Superintendent, Data Governance Committee, Webmaster, data owners, and users to develop and implement prudent and effective security policies, procedures, and controls. This includes performing and overseeing security audits, reporting regularly to the Superintendent, Directory of Technology in regard to data and/or information security and/or safety threats.

C. Data Manager: The Data Manager for the Tuscaloosa County School System 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. This title/individual may be the Director of Information Technology, the Data Specialist, the Network Administrator, or another designee assigned by the Superintendent. 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.
3. Guiding users 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 Tuscaloosa County Schools Data Governance Committee on Tuscaloosa County Board of Education status regarding information security.

D. School Technology Team Leader (STTL): The STTL is responsible for the successful and effective technology integration and system technology initiatives at the local school level. Specific responsibilities include:

1. Assist school staff with basic Level one hardware and software trouble shooting and determines if Level Two IT support is needed to resolve technical issues.
2. Places work orders for technical issues at the local school and works with assigned Level Two IT Department Technicians to ensure technology issues are resolved.
3. Ensures that critical systems, e.g., administrators' and bookkeepers' computers, are set to back up daily.
4. Assist with educating staff and students on Internet Safety, as well as awareness training about Malware, Ransomware, and other cyber threats.
5. Assist the administration in the purchase of technology-related resources.
6. Communicates with the school administration on behalf of the teachers their expressed technology needs.
7. Ensures the creation and distribution of school level technology procedures and district level policies and procedures.

E. Property Control Manager: The job of the local school Property Control Manager (PCM) is to maintain asset records in *Destiny Asset Manager*; and ensure the adequate control and accountability of the local school's fixed assets. To maintain accurate asset records, the PCM is responsible for creating records for and tagging new items received and updating records for items transferred and/or disposed of.

F. Administrators: Tuscaloosa County Schools' building-level administrators are responsible for overseeing their staff's use of information and systems with support from the Superintendent, Director of Technology, and the ISO, 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 building access to terminated employees, i.e., confiscating keys, changing combination locks, etc.

5. Providing employees with the opportunity for training needed to properly use the computer systems.
6. Reporting promptly to the Information Technology Department and/or Data Governance Committee the loss or misuse of Tuscaloosa County School System information.
7. Initiating corrective actions when problems are identified.
8. Following the district 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.

G. Information Owner: The Information Owner is usually the individual or person responsible for data retention and ensuring prudent and effective procedures are in effect to protect the integrity, confidentiality, and availability information used or created. In some cases, the owner may be the primary user of that information. In this context, ownership does not signify proprietary interest, and ownership may be shared. The owner of information has the responsibility for:

1. Knowing the information for which they are responsible.
2. Determining a data retention period for the information, relying on Alabama State Department of Education 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 Information Technology Department and/or Data Governance Committee the loss or misuse of Tuscaloosa County School System's data.
7. Initiating corrective actions when problems are identified.
8. Promoting employee education and awareness by utilizing programs approved by the Information Technology Department, where appropriate.
9. Following district approval processes within the respective organizational unit and district for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

H. Data Custodian: The data custodian is assigned by an administrator, information owner, or the Data Manager 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, the Data Manager, 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 Data Manager and/or Data Governance Committee.

6. Promoting employee education and awareness by utilizing programs approved by the Information Technology Department, where appropriate.
7. Reporting promptly to the Information Technology Department and/or Data Governance Committee the loss or misuse of Tuscaloosa County Board of Education data.
8. Identifying and responding to security incidents and initiating appropriate actions when problems are identified.

I. **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 Tuscaloosa County Schools Data Governance and Use Policy and Procedures and all controls established by the information owner and/or data custodian.
3. Keep personal authentication information (e.g., passwords, secure cards, PINs, access codes, etc.) confidential.
4. Report promptly to the Information Technology Department and/or Data Governance Committee the loss or misuse of Tuscaloosa County School System's data and/or information. Follow corrective actions when problems are identified.

Appendix D: Data Classification Levels

A. Personally Identifiable Information (PII)

PII is information about an individual maintained by an agency, including:

1. Any information that can be used to distinguish or trace an individual ‘s identity directly or indirectly through linkage with other information, such as name, social security number, date and place of birth, mother’s maiden name, medical, financial, or biometric records.
2. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

PII will only be accessed by individuals with permission. Unauthorized disclosure, modification, or disposal of PII may violate Alabama state laws, federal laws, result in criminal or civil penalties, or incur legal implications.

Note: <u>Any disclosure of these records</u> must be in accordance with applicable law.

B. Restricted/Confidential Information

1. Confidential Information is very important and highly sensitive information 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 or in accordance with applicable law. 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, modification, or disposal of Restricted/Confidential Information may violate Alabama state laws, federal laws, result in criminal or civil penalties, or incur legal implications.
3. 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 Tuscaloosa County School System, and in some cases within affiliated organizations such as Tuscaloosa County Schools’ business or community partners. This type of information is already widely distributed within Tuscaloosa 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, and system wide communications such as newsletters and announcements.
2. Any information not explicitly classified as PII, Restricted/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 (PI)

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

E. Directory Information

Tuscaloosa County Schools may disclose appropriately designated "directory information" without written consent. Directory Information, which is information generally not considered harmful or an invasion of privacy if released, can also be disclosed to an outside organization without prior written consent. Organization may include but are not limited to: Companies that manufacture class rings, companies that publish yearbooks or military recruiters upon request. If you do not want Tuscaloosa County Schools to disclose directory information from your child's education records without your prior written consent, you must notify the district in writing.

The following information had been designated as student Directory Information:

1. First and last name
2. Gender
3. Home address
4. Home telephone number
5. School assigned monitored and filtered email address
6. Photograph
7. Place and date of birth
8. Dates of attendance (years)
9. Grade level
10. Diplomas, honors, awards received
11. Participation in school activities or school sports
12. Weight and height for members of school athletic teams
13. Most recent institution/school attended
14. ID number

F. De-identified Information

The primary reason for "de-identifying" data is to protect the privacy or identify of the individuals associated with the data. De-identified data generally refers to data from which all personally identifiable information has been removed, i.e., data about individual students, teachers, or administrators that has been rendered anonymous by stripping out any information that would allow people to determine an individual's identity. Common forms of personally identifiable information include first and last names, home addresses, social security numbers, and other types of information that may reveal – advertently or inadvertently – an individual's identity in each set of data.

Appendix E: Acquisition of Software Procedures

These procedures are intended to provide the proper procedures for purchasing and/or licensing subscriptions for software and/or websites. A subscription software or website is a site that collects a recurring payment from customers in exchange for recurring product replenishment or on-going service. For further classification of the term "subscription software or subscription websites," contact the Tuscaloosa County School System (TCSS) Information Technology Department.

All software and website subscriptions licensed or purchased for use in any/all Tuscaloosa County Schools is the property of Tuscaloosa County Schools and must not be copied for use at home or any other location, unless otherwise specified by the license agreement. All information and data collected by software and website subscriptions and/or purchases is the property of the Tuscaloosa County Schools and must be compliant with all privacy laws and regulations.

The purpose of the Acquisition of Software Procedures is to:

1. Ensure proper management of the legality of information systems;
2. Allow all academic disciplines, administrative functions, and athletic activities the ability to utilize proper software tools;
3. Minimize licensing costs;
4. Increase data integration capability and efficiency of Tuscaloosa County Schools (TCSS) as a whole; and
5. Minimize malicious code that can be inadvertently downloaded.

The Information Technology Department and Software Selection 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, these procedures help ensure that all software is legally licensed and compliant with all privacy laws and regulations as well as the Tuscaloosa County Schools' Data Governance Policy.

A. Software Licensing

1. All district software licenses owned by Tuscaloosa County Schools will be:
   a. kept on file by the Information Technology Department;
   b. accurate, up-to-date, and adequate; and
   c. in compliance with all copyright laws and regulations.
2. All other software licenses owned by Central Office departments will be:
   a. kept on file with the Information Technology Department;
   b. accurate, up-to-date, and adequate; and
   c. in compliance with all copyright laws and regulations.
3. All other software licenses owned by the local schools will be:
   a. kept on file with the local school administrator and local school Library Media Specialist;
   b. accurate, up-to-date, and adequate; and
   c. in compliance with all copyright laws and regulation.
4. Software installed on Tuscaloosa County Schools' technological systems and other electronic devices will:
   a. have proper licensing on record,
   b. be properly licensed, and

c. be the responsibility of each employee purchasing and installing software to ensure proper licensing is obtained.

5. Purchased software accessed from and storing data in a cloud environment will have a Memorandum of Agreement (MOA) or contract on file that states and confirms at a minimum that:
   a. Student and/or staff data and PII will not be shared, sold, or mined with or by a third party unless approved in the signed MOA or contract;
   b. Student and/or staff data will not be stored on servers outside the United States unless otherwise approved by Tuscaloosa County Schools' Data Governance Committee;
   c. the company will comply with the Tuscaloosa County Schools' guidelines for data transfer or destruction when contractual agreement is terminated; and
   d. No application programming interface (API) will be implemented without full consent of the Tuscaloosa County Schools' and the ALSDE.
6. Software with or without physical media (e.g., downloaded from the Internet, apps, or online) must be properly evaluate, and licensed if necessary and applicable to the *Acquisition of Software* procedures.
7. 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 installation and/or using said electronic resources.
8. 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 when such permission is required by law.

B. Supported Software

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 Information Technology Department.

1. A list of supported software will be maintained on the Tuscaloosa County Schools' Information Technology Department's site.
2. It is the responsibility of the Tuscaloosa County Schools' Information Technology Department to keep the list current.
3. It is the responsibility of the Software Review Committee to submit any newly approved software to the Information Technology Department so the supported software on their website will be up-to-date.
4. Any software not listed as supported software on the Information Technology Department website, is considered unsupported software and must be approved by the Software Review Committee. If approval from the Software Review Committee is not received prior to purchasing, it will not be allowed on any Tuscaloosa County Schools' owned devices.
5. When staff recommends programs or apps for software 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.
6. Software that accompanies adopted instructional materials will be vetted by the Coordinators of Curriculum and Instruction and the Director of Information Technology or their designee and is therefore supported.

7.

C. Unsupported / New Software:

In the Evaluate and Test Software Packages phase, the Software Review Committee and Information Technology Department will evaluate unsupported software against current standards and viability of implementation into the Tuscaloosa County Schools' 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:
    a. Determining how the software will impact the Tuscaloosa County Schools' technology environment such as storage, bandwidth, etc.
    b. Determining hardware requirements.
    c. Determining what additional hardware is required to support a particular software package.
    d. Outlining the license requirements/structure, number of licenses needed, and renewals.
2. Determining any Maintenance Agreements including cost.
    a. Determining how the software is updated and maintained by the vendor.
    b. Determining funding for the initial purchase and the sustainability of continued licenses and maintenance.
3. When staff makes a recommendation of software programs or apps for purchase and/or testing, it is the responsibility of the Software Review Committee to properly vet the app or software to ensure that is instructionally sound, is in line with curriculum and/or behavioral standards and is age appropriate.

D. Software Purchasing Procedures

1. Staff should send <u>all</u> software subscription requests to the local school administrator and the local school STTL via electronic mail.
2. The local school STTL will verify the software requested is supported by the Information Technology Department by submitting a work order.
3. The work order response will determine the next steps of actions:
    a. If the software is supported, the staff may proceed with the purchasing process and request a purchase order.
    b. If the software is not currently supported by the Information Technology Department, the staff must submit a *software review request* via electronic mail to the the Director of Information Technology, local school administrator, and the local school STTL. The request must contain the following information:
        i. Name of software
        ii. Cost
        iii. Supplier/vendor
        iv. Funding source for the purchase
        v. How the software is different from other software currently provided by the district
        vi. How the staff will be able to track and show student progress/usage.
4. The Director of Information Technology will present all *Software Review Requests* to the Software Review Committee for review and determination.
5. The Director of Information Technology or their designee will notify the requesting staff member, local school administrator, and local school STTL of the Software Review Committee's determination.

6. The next actions will be determined by Software Review Committee's decision:
    a. If the software is denied as a *supported software*, no further action is needed.
    b. If the software is approved as a Tuscaloosa County School *supported software*, the requesting staff may proceed with the purchasing process by requesting a purchase order.
        i. When the approved purchase order is issued, the bookkeeper must provide the requesting staff, local school STTL, and local school Property Control Manager with a copy of the approved purchase order.

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

A. Virus, Malware, and Spyware Protection

Tuscaloosa County School System desktops, laptops, and fileservers run the Cylance Protection software. Virus definitions are updated multiple times per day and implemented as quickly as possible to protect against Zero-Day threats and all known malicious code.

B. Internet Filtering

Student learning using online content and social collaboration continues to increase. Tuscaloosa 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 Barracuda filter using the user's network credentials. For companion devices and guest devices, users see a "pop-up screen" that requires them to login to the Barracuda Internet 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, etc. are blocked.

C. Phishing and SPAM Protection

In addition to Microsoft's Exchange Online Protection (EOP) the built-in spam filtering for Office 365, the Barracuda Essentials, Barracuda Sentinel and Manage Methods network monitoring tools is used to protect TCSS resources.

D. Security Patches

Patches are scheduled to auto-download and install as appropriate. Fileservers are scheduled to auto-download and are installed as appropriate. Machines are re-booted as necessary.

E. Operating Systems Updates and Upgrades

Windows computers, Macintosh computers and iOS device updates occur throughout the year. These updates and upgrades are issued to improve performance, maintain proper functionality, and increase security of the technology resources.

Note: The Information Technology Department recommends that users back up their computer data and iOS device data before installing system updates and upgrades.

Appendix G: Physical and Security Controls

The following physical and security controls must be adhered to:

1. Data centers must be installed in an access-controlled area. The area in and around the computer facility must afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations.

2. Monitor and maintain data centers' temperature levels according to industry standard temperature levels and requirements.

3. 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.

4. 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.

5. Ensure network systems (i.e., data closets) and network equipment are properly secured to prevent unauthorized physical access and data is properly safeguarded to protect from loss.

6. Local school administrators should ensure data closets are vacuumed monthly as preventive maintenance to reduce dust, prevent overheating and fire hazards, as well as prolong the life of the network systems and network equipment.

Appendix H: Password Control Standards

The Tuscaloosa County Schools Data Governance and Use Procedures 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 organizational groups that are managed through Microsoft Active Directory.

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 a designated data manager.
2. Every password must, where possible, be changed yearly if not more frequently for staff and on an age-appropriate schedule for students. Guest passwords are changed every 30 days.
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. Some suggested criteria for passwords are listed below.
5. Passwords should:
    a. NOT contain the user's account name or parts of the user's full name that exceed two consecutive characters
    b. Contain characters from three of the following four categories:
        i. English uppercase characters (A through Z)
        ii. English lowercase characters (a through z)
        iii. Base 10 digits (0 through 9)
        iv. Non-alphabetic characters (for example, !, $, #, %)
6. It is recommended that passwords should never be saved when prompted by any application.
7. It is recommended that passwords must not be recorded anywhere that someone may find and use them.
8. 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.…). Instead, consider using a combination of alpha and numeric characters that is more difficult to guess.
9. All staff are required to complete *Self-Registration* to allow passwords to be changed immediately if an account breach is suspected. To complete *Self-Registration*, reset or change password, visit https://reset.tcss.net/

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. System software must disable the user password when more than eight consecutive invalid passwords are given. Lockout time must be set at a minimum of 15 minutes.
5. System software should maintain a history of previous passwords and prevent them being easily guessed due to their association with the user. A combination of alpha and numeric characters is more difficult to guess.

Appendix I: Purchasing and Disposal Procedures

These procedures are 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, audio visual 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 Tuscaloosa County Schools' Information Technology Department.

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

A. Purchasing

Prior to purchasing any systems that will be used in conjunction with the Tuscaloosa County Schools' technology resources, staff must:

1. submit an *Intent to Purchase* form via electronic mail to the local school administrator and local STTL and receive approval to proceed with the purchasing process. The *Intent to Purchase* should include at minimum the following:
    a. name and model of the system
    b. description/purpose of the system
    c. cost
    d. vendor
    e. anticipated delivery
    f. quote with shipping
2. purchase systems from an approved vendor, contract, consortium, or the Alabama Joint Purchasing (ALJP) regardless of funding source; and
3. purchase systems with a district and/or local school approved purchase order approved by a school administrator, the Director of Information Technology or their designee, or appropriate department.
    * See Resource 4: Competitive Bid Law

To ensure accurate asset inventory records and appropriate network support, the bookkeeper must provide the local school Property Control Manager and the local school STTL with a copy of the purchase order and quote once it has been approved and signed.

Failure to have the purchase approved by the Director of Information Technology or designee may result in a lack of technical support, removal of the item(s) from Tuscaloosa County Schools' premises, or access denied for the item(s) to other technology resources.

B. Inventory

All systems over $500 are inventoried in accordance with the Tuscaloosa County Board of Education Finance Department using the *Destiny Asset Manager*. There are some exceptions under $500 that must be inventoried, such as but not limited to Apple TVs, iPads, Apple Magic Trackpads, Apple Pencils, Apple Magic Mouses, Apple Magic Keyboards (any model), and other companion devices or peripherals as determined by the Director of Information Technology. The *Inventory Procedures* provides the steps for purchased, transferred/redistributed, discarded, and donated technological systems to ensure inventory records are standardized to contain accurate information about all systems that allows proper identification and home locations for all items.

* **See also *Appendix J: Inventory Procedures***

C. Disposal of Items

Equipment should be considered for disposal for the following reasons:

a. End of useful life,
a. Lack of continued need,
b. Obsolescence,
c. Wear, damage, or deterioration,
d. Excessive cost of maintenance or repair.

D. Methods of Disposal

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

1. Transfer/Redistribution of items

a. 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.
b. An IT work order request must be submitted to have the equipment transferred, moved, reinstalled and, in the case of computers, laptops, or companion devices, wiped and reimaged or configured for another location.

2. Discarding/Recycling of items

a. All electronic equipment in the Tuscaloosa 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), Restricted/Confidential, or Internal Information. A process of wiping the data is performed.
b. 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.
c. Under no circumstances should any technological systems/equipment be placed in the trash. Doing so may make the Tuscaloosa County School System, the local school, and/or

employee who disposed of the equipment liable for violating environmental regulations or laws.

3. **Donation of item by the Tuscaloosa County Schools**
   On occasion, Tuscaloosa County Schools may donate technological equipment to other school systems. Technological equipment donations may occur if the technological equipment is in good working order but no longer meets the requirements and/or needs of the local school/site where it is located, and it cannot be put into use in another part of the local school or in another Tuscaloosa County school. Technological equipment may be donated upon the written request of the receiving public school system's superintendent or non-profit organization's director. Donations may be allowed to individuals outside of the school system of Tuscaloosa County Schools as approved by the Superintendent and Tuscaloosa County Board of Education.

   To protect the integrity of the Tuscaloosa County School System, the following guidelines should be followed when donating technological equipment:
   a. It should be made clear to any school or organization receiving donated equipment that Tuscaloosa County Schools is not agreeing to and is not required to support or repair any donated equipment. It is donated AS IS.
   b. Tuscaloosa County Schools' staff should, before offering donated equipment, make every effort to ensure that it is in good condition and can be re-used. Microsoft licenses or any other software licenses shall non-transferrable outside the Tuscaloosa County School System.
   c. Once the items are approved for donation, an IT work order request must be submitted to wipe the equipment of any PII, Restricted/Confidential and/or internal information, and allow inventory records to be updated in *Destiny Asset Manager.*

Appendix J: Inventory Procedures

These procedures are intended to provide for the proper inventory of technological devices only. Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, audio visual 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 Tuscaloosa County School System Information Technology Department. All involved systems and information are assets of Tuscaloosa County Schools are expected to be inventoried to protect against misuse, unauthorized removal from school premises, and/or theft.

I. Acquisition of Technological Assets

A. Technology Asset Classification

All technological devices or systems over $500 are inventoried in accordance with the Tuscaloosa County Board of Education Finance Department using the *Destiny Asset Manager*. There are some exceptions under $500 that must be inventoried, such as but not limited to Apple TVs, iPads, Apple Magic Trackpads, Apple Pencils, Apple Magic Mouses, Apple Magic Keyboards (any model), and other companion devices or peripherals as determined by the Director of Information Technology.

B. Asset Purchases

1. Once a purchase order has been approved to purchase any technological devices or systems, the bookkeeper should provide the local school Property Control Manager with a copy of the approved purchase order.
2. Upon receipt of the technological devices or systems, it is the responsibility of the local school Property Control Manager to submit an IT work order to request an asset tag for the newly acquired devices and/or systems. The work order should include the following information:
    a. name of the item (display name)
    b. serial number
    c. quantity of items
    d. purchase order number
    e. date of receipt of item(s)
    f. MAC Wi-Fi address (all lowercase, if applicable)
3. Upon receipt of the asset tag(s), it is the responsibility of the local school Property Control Manager to catalog the item in *Destiny Asset Manager*.
    a. If no other items match the model of the item acquired, the item will be added by creating a new resource source. When adding a new resource source, the following items must be included in the record:
        i. Manufacturer
        ii. Model
        iii. Instructional Classification
        iv. Replacement Price

b. If there are other technological devices or systems in the district that match the model, the item will be added using the "add item" in *Destiny Asset Manager*. The item's record must include the following information:

a. name of the item
b. home location
c. department
d. funding source
e. district identifier, i.e. active directory name
f. purchase price
g. date acquired – date received
h. purchase order
i. serial number
j. general ledger number – purchasing code from purchase order
k. vendor

C. Assets Donated to Tuscaloosa County Schools

1. Items donated by individuals and/or businesses are the property of the Tuscaloosa County Schools.
2. Items must be inspected by the Information Technology Department to determine if the technological device(s) is in usable condition.
3. All donated devices should be reset to factory settings and erased to remove any potential security threats before being placed on the Tuscaloosa County Schools' network.

D. Asset Transfer & Redistribution

Once the Information Technology Department has completed their portion of the transfer/redistribution work order, the work order will be forwarded to the local school Property Control Manager of the item's new school/location to complete the final step of the transfer and redistribution process. It will be necessary for the local school Property Control Manager to update transferred and redistributed items' "home location" in *Destiny Asset Manager*.

a. Transfer & Redistribution within a local school: It is the responsibility of the local school Property Control Manager to update the "home location" of the item.
b. Transfer & Redistribution to another school or location in the district: It is the responsibility of the **receiving** school's Property Control Manager to transfer the item to their *Destiny Asset Manager* inventory and to update the item's "home location" in the inventory record.

E. Warranty Claims on Technological Devices

1. For technological devices under warranty, the local school STTL should place a work order for the IT Technicians to determine repair costs with vendor.

Discarding Assets

1. When an item is to be discarded, the local school Property Control Manager will update the item's asset record in *Destiny Asset Manager* by changing the condition to "unusable" and the status to "ready for disposal."
2. The local school Property Control Manager will submit via email the "Ready for Disposal" report from *Destiny Asset Manager* to the local school administrator, Director of Information Technology, and the Chief School Finance Officer. The "Ready for Disposal" report includes but is not limited to the following information and must be provided to the Finance Department no later than one week prior to the next Board of Education meeting:
    a. TCSS asset tag number (barcode),
    b. Displayable Name,
    c. Model,
    d. Home Location,
    e. Serial number,
    f. Purchase Order
    g. Funding source,
    h. Resource Type, and
    i. District ID
3. Once the items have been approved by the TCSS Board of Education for disposal, the Information Technology Department is responsible for updating the items' inventory record status to "approved for disposal" in *Destiny Asset Manager*.

Assets Donated by TCSS

On occasion, TCSS may donate technological equipment to other school systems. Technological equipment donations may occur, if the technological equipment is in good working order, but no longer meets the requirements and/or needs of the local school/site where it is located, and it cannot be put into use in another part of the local school or in another Tuscaloosa County school.

Technological equipment may be donated upon the written request of the receiving public school system's superintendent or non-profit organization's director.

Donations may be allowed to individuals outside of the school system of Tuscaloosa County Schools as approved by the Superintendent and Tuscaloosa County Board of Education.

1. Once the items are approved for donation, an IT work order request must be submitted to wipe the equipment of any PII and allow inventory records to be updated in *Destiny Asset Manager.*
2. *Local school items donated:* It is the responsibility of the local school Property Control Manager to update the status of donated items to "Approved for Disposal."
3. *Central office items donated:* It is the responsibility of the Information Technology Department staff to update the status of donated items to "Approved for Disposal."
4.

Annual Inventory

It is the expectation of the district that an annual inventory of local school technological systems be performed at least once per fiscal year using *Destiny Library & Asset Manager.* The Director of Information Technology, TCSS Finance Department, and/or Superintendent shall set the dates on which the inventory shall be reconciled for the local schools. The local school inventory is the responsibility of the local school Property Control Manager and school administrator. Local school staff shall be responsible for assisting with locating items in their buildings.

Appendix K: Data Access Roles and Permission Groups

Tuscaloosa County Schools maintain the following permission groups in PowerSchool:

1. District Admins
2. District CNP Reports
3. Staff Maintenance
4. Advanced Registrar
5. District Office Staff
6. ESL Teachers
7. InFocus Users
8. Scheduling
9. Scheduling Course Requests
10. School Enroll Withdraw
11. School Enrolment Clerk
12. School Office Staff
13. School Programs
14. Bookkeeper
15. District View Only
16. Learning Earnings
17. School Assistant Principal
18. School Athletic Checkbox
19. School Attendance Clerk
20. School Counselor
21. School Principal
22. School View Only
23. TMS Basic Attendance Clerk
24. Assistant Coaches
25. Chalkable Pilot Group
26. Checkout Authorization
27. Day Program
28. Graduation Coach
29. Instructional Assistant
30. JPO
31. School Elementary Teacher
32. SETS Staff
33. School Physical Fitness Testing
34. School Nurse
35. School Secondary Teacher
36. State Reports
37. TIS Office Staff

Resources

Alabama State Department of Education State Monitoring Checklist

Resource 1

Data Governance

ON-SITE	YES	NO N/A	Indicators	Notes
1. Has a data governance committee been established and roles and responsibilities at various levels specified?			• Dated minutes of meetings and agendas • Current list of roles and responsibilities	
2. Has the local school board adopted a data governance and use policy?			• Copy of the adopted data governance and use policy • Dated minutes of meetings and agenda	
3. Does the data governance policy address physical security?			• Documented physical security measures	
4. Does the data governance policy address access controls and possible sanctions?			• Current list of controls • Employee policy with possible sanctions	
5. Does the data governance policy address data quality?			• Procedures to ensure that data are accurate, complete, timely, and relevant	
6. Does the data governance policy address data exchange and reporting?			• Policies and procedures to guide decisions about data exchange and reporting • Contracts or MOAs involving data exchange	
7. Has the data governance policy been documented and communicated in an open and accessible way to all stakeholders?			• Documented methods of distribution to include who was contacted and how • Professional development for all who have access to PII	

Alabama Record Disposition Authority

Resource 2

The information below is from the Local Boards of Education Records Disposition Authority approved by the Local Government Records Commission, April 2021. The complete document can be found at: http://www.archives.alabama.gov/officials/localrda.html.

The following sections are of special interests in Local Boards of Education Records Disposition: https://archives.alabama.gov/officials/rdas/local/education_rda.pdf

A.	1.02	Improvement Plans
B.	1.03	Local Boards of Education Meeting Records (includes school all committee meetings)
C.	1.04	Administrative Correspondence
D.	2.01	Child Nutrition Program Operational Records
E.	3.01	School Bus Monthly Route Reports
F.	4.02	20-Day Average Daily Membership Reports (ADM)
G.	4.03	Adequate Yearly Progress (AYP) Reports
H.	4.04	Principal's Attendance Reports
I.	4.05	Student Dropout Records
J.	5.03	Student Discipline Files
K.	5.07	Truancy Case Files
L.	5.12	Student Health Records
M.	6.01	Student Handbooks
N.	6.03	Daily/Weekly Teacher Lesson Plans
O.	6.10	School Library/Media Center Records
P.	7.01	Student Records
Q.	8.01	Athletic Program Records
R.	9.01	Local Board of Education Internal Policies and Procedures
S.	9.14	Records Management Documentation
T.	9.16	Websites and Social Media
U.	10.04	Purchasing Records
V.	10.05	Records of Formal Bids
W.	10.06	Contracts, Leases, Franchises, and Agreements
X.	10.08	Grant Project Files
Y.	12.01	Annual Inventory Records
Z.	12.07	Facilities/Buildings Security Record

Agreements for Contract Employees Including Long Term Substitutes

Resource 3

Procedure:

All contract employees including long term substitutes should complete the following prior to gaining access to the Tuscaloosa County School System Network, PowerSchool SIS, PowerTeacher Pro, PowerSchool Special Programs (if applicable):

1. **Complete the** Request for Email Account and Other Resources for Contract Employees Form.
2. **Read the** Board Policy on Technology and Telecommunications.
    - Form available on www.tcss.net – Under (About, Board Policy, Section 5.90)
3. Make appointment with Local School Administrator to review Data Usage and Classroom Tools
4. Read and sign the **Tuscaloosa County Schools Student Data Confidentiality Agreement** in the Data Governance and Use Procedures.

Once the above has been completed and forms reviewed, if all requirements are met, the new email account will be enabled.

*Account will be created as soon as Information Technology Department receives the **Request for Email Account and Other Resources for Contract Employees Form** for the contracted employee. The account will be disabled until the contracted employee meets with the school administrator and/or local STTL.

Disabling of employee accounts

1. on the last day of active employment;
2. when on leave for more than 6 months; or
3. if directed by the Superintendent.

If approved by the Superintendent, accounts may be allowed to remain open for a time determined by the Superintendent or his designee.

Competitive Bid Laws & Purchasing Cooperatives

Resource 4

The State of Alabama Bid Law requires that all purchases and/or contracts for labor, services, materials, equipment, and supplies for such amounts as set by the State of Alabama, shall, except as otherwise provided in the law, be let by free and open competitive bidding, on sealed bids, to the lowest responsible bidder.

Purchasing Cooperatives

A cooperative contract is one that has been competitively bid by any group or consortium of governmental entities or a group purchasing organization with the goal of complying with standard procurement practices and state bid laws. Cooperative contracts leverage the purchasing power of large volume commitments by allowing multiple entities to purchase from a single contract.

For a list of the purchasing cooperatives that have been approved for use by the Alabama State Examiner's office, visit https://examiners.alabama.gov/purchase-coop.aspx

Competitive Bid Laws

1. All electronic equipment is subject to Alabama competitive bid laws.

2. Generally, for technological devices and services, Tuscaloosa County Schools purchase from the Alabama Joint Purchasing Agreement (ALJP). To access the ALJP, visit https://aim.alsde.edu/index.aspx
3. In the event that a desired product is not included in one of cooperative purchasing agreements, Tuscaloosa County Schools will bid the item or items using the district's competitive bid process.
4. Most technological systems, services, etc. over $15,000 purchased with public funds are subject to Alabama's competitive bid laws.

Forms

Tuscaloosa County Schools Technological Services and Systems Memorandum of Agreement (MOA)

THIS MEMORANDUM OF AGREEMENT, executed and effective as of the_____day of_____, 20_, by and between_____, a corporation organized and existing under the laws of_____(the "Company"), and **TUSCALOOSA COUNTY SCHOOLS(TCSS)**, a public school system organized and existing under the laws of the state of Alabama (the "School Board"), recites and provides as follows.

Recitals

The Company and the School Board are parties to a certain agreement entitled "_____" hereafter referred to as (the "Agreement"). In connection with the execution and delivery of the Agreement, the parties wish to make this Memorandum of Agreement (also referred to as MOA or Addendum) a part of the original Agreement in order to clarify and/or make certain modifications to the terms and conditions set forth in the original Agreement.

The Company and the School Board agree that the purpose of such terms and conditions is to ensure compliance with the Family Educational Rights and Privacy Act (FERPA) and the overall privacy and security of student Personally Identifiable Information (PII) hereafter referred to as student information and/or data, including but not limited to (a) the identification of the Company as an entity acting for the School Board in its performance of functions that a School Board employee otherwise would perform; and (b) the establishment of procedures for the protection of PII, including procedures regarding security and security breaches.

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is acknowledged hereby, the parties agree as follows.

Agreement

The following provisions shall be deemed to be included in the Agreement:

Confidentiality Obligations Applicable to Certain TCSS Student Records. The Company hereby agrees that it shall maintain, in strict confidence and trust, all TCSS student records containing personally identifiable information (PII) hereafter referred to as "Student Information". Student information will not be shared with any other resource or entity that is outside the intended purpose of the Agreement.

It is understood and agreed upon, between the Tuscaloosa County School System and Vendor that these aforementioned software products offered by Vendor do contain student level data and therefore the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99), along with the Alabama Data Breach Notification Act of 2018 (S.B. 318) does apply to this MOA

The Company shall cause each officer, director, employee and other representative who shall have access to TCSS Student Records during the term of the Agreement (collectively, the "Authorized Representatives") to maintain in strict confidence and trust all TCSS Student Information. The Company shall take all reasonable steps to ensure that no TCSS Student information is disclosed to any person or entity except those who (a) are Authorized Representatives of the Company performing functions for TCSS under the Agreement and have agreed to be bound by the terms of this Agreement; (b) are

authorized representatives of TCSS, or (c) are entitled to such TCSS student information from the Company pursuant to federal and/or Alabama law. The Company shall use TCSS student information, and shall take all reasonable steps necessary to ensure that its Authorized Representatives shall use such information, solely for purposes related to and in fulfillment of the performance by the Company of its obligations pursuant to the Agreement.

The Company shall: (a) designate one of its Authorized Representatives to be responsible for ensuring that the Company and its Authorized Representatives maintain the TCSS student information as confidential; (b) train the other Authorized Representatives with regard to their confidentiality responsibilities hereunder and pursuant to federal and Alabama law; (c) maintain at all times a list of Authorized Representatives with access to TCSS student information.

Other Security Requirements. The Company shall maintain all technologies, policies, procedures and practices necessary to secure and protect the confidentiality and integrity of TCSS student information, including procedures to (a) establish user IDs and passwords as necessary to protect such information; (b) protect all such user passwords from detection and unauthorized use; (c) prevent hostile or unauthorized intrusion that could result in data corruption, or deny service; (d) prevent and detect computer viruses from spreading to disks, attachments to e- mail, downloaded files, and documents generated by word processing and spreadsheet programs; (e) minimize system downtime; (f) notify TCSS of planned system changes that may impact the security of TCSS data; (g) return or destroy TCSS data that exceed specified retention schedules; (h) notify TCSS of any data storage outside the US; (i) in the event of system failure, enable immediate recovery of TCSS information to the previous business day. The Company should guarantee that TCSS data will not be sold to, accessed by, or moved by third parties.

In the event of a security breach, the Company shall (a) immediately take action to close the breach; (b) notify TCSS within 24 hours of Company's first knowledge of the breach, the reasons for or cause of the breach, actions taken to close the breach, and identify the TCSS student information compromised by the breach; (c) return compromised TCSS data for review; (d) provide communications on the breach to be shared with affected parties and cooperate with TCSS efforts to communicate to affected parties by providing TCSS with prior review of press releases and any communications to be sent to affected parties; (e) take all legally required, reasonable, and customary measures in working with TCSS to remediate the breach which may include toll free telephone support with informed customer services staff to address questions by affected parties and/or provide monitoring services if necessary given the nature and scope of the disclosure; (f) cooperate with TCSS by providing information, records and witnesses needed to respond to any government investigation into the disclosure of such records or litigation concerning the breach; and (g) provide TCSS with notice within 24 hours of notice or service on Company, whichever occurs first, of any lawsuits resulting from, or government investigations of, the Company's handling of TCSS data of any kind, failure to follow security requirements and/or failure to safeguard TCSS data. The Company’s compliance with the standards of this provision is subject to verification by TCSS personnel or its agent at any time during the term of the Agreement. Said information should only be used for the purposes intended and should not be shared, sold, or moved to other companies or organizations nor should other companies or organization be allowed access to said information.

Disposition of TCSS Data Upon Termination of Agreement

Upon expiration of the term of the Agreement, or upon the earlier termination of the Agreement for any reason, the Company agrees that it promptly shall deliver to the School Board, and shall take all reasonable steps necessary to cause each of its Authorized Representatives promptly to deliver to the School Board, all required TCSS student data and/or staff data. The Company hereby acknowledges and agrees that, solely for purposes of receiving access to TCSS data and of fulfilling its obligations pursuant to this provision and for no other purpose (including without limitation, entitlement to compensation and other employee benefits), the Company and its Authorized Representatives shall be deemed to be school officials of the School Board, and shall maintain TCSS data in accordance with all federal state and local laws, rules and regulations regarding the confidentiality of such records. The non-disclosure obligations of the Company and its Authorized Representatives regarding the information contained in TCSS data shall survive termination of the Agreement. The Company shall indemnify and hold harmless the School Board from and against any loss, claim, cost (including attorneys' fees) or damage of any nature arising from or in connection with the breach by the Company or any of its officers, directors, employees, agents or representatives of the obligations of the Company or its Authorized Representatives under this provision.

Certain Representations and Warranties. The Company hereby represents and warrants as follows: (a) the Company has full power and authority to execute the Agreement and this MOA and to perform its obligations hereunder and thereunder; (b) the Agreement and this MOA constitute the valid and binding obligations of the Company, enforceable in accordance with their respective terms, except as such enforceability may be limited by bankruptcy or similar laws affecting the rights of creditors and general principles of equity; and (c) the Company's execution and delivery of the Agreement and this Addendum and compliance with their respective terms will not violate or constitute a default under, or require the consent of any third party to, any agreement or court order to which the Company is a party or by which it may be bound.

Governing Law: Venue. Notwithstanding any provision contained in the Agreement to the contrary, (a) the Agreement shall be governed by and construed in accordance with the laws of the State of Alabama, without reference to conflict of laws principles; and (b) any dispute hereunder which is not otherwise resolved by the parties hereto shall be decided by a court of competent jurisdiction located in the State of Alabama.

IN WITNESS WHEREOF, the parties hereto have caused this Addendum to be executed by their duly authorized officers effective as of the date first written above.

[COMPANY NAME]

By:_____

[Name] [Title]

TUSCALOOSA COUNTY BOARD OF EDUCATION

By:_____

Dr. Keri Johnson, Superintendent
Tuscaloosa County Board of Education

Tuscaloosa County Schools Student Confidentiality Agreement

In general, student educational records include records, files, documents, and other materials that are directly related to a student and are maintained by the school system. As an employee of Tuscaloosa County Board of Education, you may have access to student education records while on or off campus in order to perform your duties for the school system.

By signing this agreement, you agree to abide by the following guidelines regarding the appropriate use of student educational records:

- I will comply with school district, state and federal confidentiality laws, including the school system's Data Governance and Use Policy and Procedures, the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g and 34 CFR Part 99; and, and this Agreement.
- I will not disclose the contents of student educational records to persons who do not have the right to access the records pursuant to FERPA or other applicable requirements.
- I will review and familiarize myself with the school system's FERPA notifications to parents/guardians contained in the Student Code of Conduct.
- I will only access student records for students for whom I have a legitimate educational interest.
- I understand that a student should not have access to another student's confidential educational records.
- If I become aware of a breach of confidentiality of student records, I will report it to my immediate supervisor.
- I will securely log in and out of the programs that store student educational records. I will not share my password. Any documents that I create containing student educational records will be stored securely within the TCSS district network or within a password protected environment. I will not store student educational records on any personal computer and/or external devices that are not password protected. (External devices include but are not limited to USB/Thumb drives and external hard drives.)
- I will handle and store student educational records in a manner designed to prevent unauthorized persons from accessing those records regardless of its format, including information on a computer display.
- Regardless of its format, I will treat all information with respect for student privacy. I will not leave student educational records in any form accessible or unattended, including information on a computer display.

By signing below, I acknowledge, understand, and agree to accept all terms and conditions of the Tuscaloosa County Schools Confidentiality Agreement.

_____ Date_____
Print Name of Employee

_____ School_____
Signature of Employee

Request for Email Account and Other Resources for Contract Employees

For contract employees to qualify for a district Office 365 account in the TCSS domain, they must have a contract on file with Human Resources and perform work for Tuscaloosa County Schools on a regular basis. If Tuscaloosa County Schools has a contract with an agency to provide services to Tuscaloosa County Schools on an as needed basis, they generally do not qualify and should use the email account provided to them by the agency. However, we will review all requests and may provide access to e-mail if it is necessary for the agency to perform its contractual duties.

Contract Employee legal Name: _____ _____ _____
(First Name) (Middle Name) (Last Name)

Requester:_____Department/School:_____

Start Date:_____ End Date: _____

Work to be Performed or Position: _____

Is contract employed through Kelly Services? Yes/No _____ Other _

Has contract employee had background check? _____ Yes/No

Contract employee been E-Verified?

Network/Wi-Fi Account? **Yes/No NA _____**
Yes/No NA

Other Access Requested:_____

PowerSchool with permissions equal to : Teacher Office Other

If other, please specify: _____

PowerSchool Special Programs permissions equal to: Teacher Office

Other

Name of other software and reason for access: _____

_____

Signature of Requester:_____ Date: _____

****

Central Office Use Only

_____ Denied_____Approved _____Initials Date: _____

Student Technology Equipment Checkout Form

Employee Name: _____ _____
(First Name) (Last Name)

School/Department:_____Grade: _____

Equipment Checkout (Check All Requested)

Laptop/MacBook: ____iPad: __Projector: _____ Screen: ___

Other (please explain): _____

Serial Number_____Asset Tag _____

Equipment Needed From Start Date:_____ End Date: _____

Reason for Equipment Checkout: _____

_____

_____

If More Space Needed: Attach Additional Sheets with the Reason, Serial Number and Asset Tag

Signature of Requester:_____ Date: _____

Parent Signature (for Student)_____Date: _____

Principal or Superintendent Use Only: _____Denied _____Approved

Equipment Checkout Date: _____

Principal or Superintendent Signature: _____

Equipment Returned Date to Principal/Superintendent/Designee: _____

Principal/Superintendent/Designee Signature: _____

Request for Access in Student Management System
PowerSchool

For employees to have access right to PowerSchool:

Employee legal Name:

_____

(First Name)

_____

(Middle Name)

_____

(Last Name)

Employee ID: _____

Requester:_____

Department/School:_____

Start Date:_____

End Date: _____

Position of Employee: _____

PowerSchool with permissions equal to _____Teacher _____Office _____Other

If other, please specify: _____

Reason for access:

_____

_____

PowerSchool Special Programs with permissions equal to ____Teacher _____Office ___Other

Signature of Requester:_____ Date: _____

****

Central Office Use Only

_____ Denied_____Approved _____Initials Date: _____

***** Please note this is an example form ******
The Permission form will be In Harris Forms online to fill out

These are guidelines that have been put in place by The Tuscaloosa County School System (TCSS) and are in effect for use of Portable Technology Devices, such as iPhones, iPads, MacBooks, Laptops, Digital Cameras, etc., owned by TCSS, issued to employees of TCSS. As with any other technology device, this is subject to the rules and conditions contained within the Tuscaloosa County School System's Acceptable Use Policy (AUP) and Technology Policy.

Individuals who have been assigned Portable Technology Devices must regard them as property of the Tuscaloosa County School System and assume the security and care of the device, all components, and accessories.

Portable Technology Devices must not be left in vehicles due to temperature extremes that have been proven to cause damage to the systems and due to the potential for theft. Portable Technology Devices must not be left in an unsecured location.

Devices that are lost, stolen or damaged will result in financial loss to the School System. If it is determined that the loss of a device, or damage to a device, is the result of the individual's failure to comply with School System policies and procedures, neglect or because of the individual's intentional act, the individual will be required to reimburse the School System for the cost of replacement or repair of the device. Do not deface or permanently mark on the device.

Problems with the functionality of the device must be reported by a staff member through the county's on-line help-desk system. No home support will be available to end-users. If units need to be sent out for repair, loaner units will NOT be available.

All Portable Devices have to be recorded in the Tuscaloosa County School System technology inventory. The Tuscaloosa County School System Technology Services Department reserves the right to perform a physical inventory of the hardware at any point.

Individuals **must** report lost, damaged or stolen equipment immediately –no later than 24 hours - to their supervisor. Property loss damage reports must be completed on the appropriate forms and will be closely monitored. Stolen equipment must be reported to the TCSS Resource Manager to ensure thorough investigations, pursuit of criminal prosecution and full restitution, when possible, to the fullest extent of the law. Any person who knowingly files an application for insurance, statement of claim or police report containing any materially false information or attempts to conceal information concerning any fact material thereto, is violating the law and may be punished by criminal and/or civil penalties.

End-users are responsible for the backup of all data on their systems. Technology Services assumes no liability for the loss of data.

If accessories, upgrades or components are purchased by individual schools for these Portable Devices, those items are regarded as local school purchases of the schools and remain with the school.

It is recommended that individuals who are assigned Portable Devices have homeowners, renters and/or automobile insurance coverage in case of theft or loss.

Any data corruption or configuration errors caused by the installation of unauthorized or illegal software may result in a loss of all data on your system due to the need for a complete reload of your Portable Device.

In cases of obvious neglect, abuse or violations, the Portable Device will be taken from the individual and reassigned

Portable Devices with ***ALL*** accessories in working order, (including but not limited to: charger, cord, cases, earphones) must be immediately returned upon request to your supervisor. Failure to do so will result in appropriate action.

Office of Information Technology

PORTABLE TECHNOLOGY EMPLOYEE

Name _____ **School/Location:** _____

Grade/Dept: _____ **Room #/Location of the equipment:**_____

Home Address: _____**City:** _____ **State:** ____ **Zip:** _____

Personal Phone: _____ **School Phone:** _____

Equipment: □Laptop □iPad □iPhone □MacBook □Other (specify) _____

1)Model _____ **Service Tag/Serial Number** _____

Bar Code_____

2) Model _____ **Service Tag/Serial Number** _____

Bar Code_____

3) Model _____ **Service Tag/Serial Number** _____

Bar Code_____

4) Model _____ **Service Tag/Serial Number** _____

Bar Code_____

5) Model _____ **Service Tag/Serial Number** _____

Bar Code_____

Carrying Case _____Power Cord _____AC Adapter _CD/DVD Drive/Cable _____
Spare Battery _____Manuals _Cover _____Other _____

My signature below indicates I have thoroughly read the above information. I understand the School System will seek to recover the cost of repair or replacement of a device that is damaged or lost as a result of an intentional act, or because of my failure to follow the School System policies and procedures. I agree to the above terms and conditions as such, agree to fully cooperate with property loss reporting requirements and with property loss incident investigations. These guidelines can also be found online under Technology forms. I also agree to follow all TCSS Technology Acceptable Use Policies when operating the above listed equipment while on or off school property. I also agree to provide TCSS with the device password.

_____

Employee's Signature
Date

I authorize the release of this equipment to this employee.

_____

Principal/Supervisor's Signature Date