Choctaw County Schools
Data Governance Policy

Data Security

The Superintendent is authorized to establish, implement, and maintain data security measures. Procedures to be established include a method of establishing data security classifications, implementing procedural and electronic security controls, and maintaining records regarding security access. The data security measures will apply to Board employees and all Board operations. Any unauthorized access, use, transfer, or distribution of Board data by any employee, student, or any other individual, may result in appropriate disciplinary action, which may include a recommendation for termination and other legal action. All data (electronic, paper or otherwise) used to conduct operations of the System are covered by this policy. This policy does not address public access to data as specified in the Alabama Open Records Act. In all cases, applicable federal and state statutes and regulations that guarantee either protection or accessibility of System records will take precedence over this policy.

Applicable Laws and Standards

FERPA

The Family Educational Rights and Privacy Act, applies to all institutions that are recipients of federal aid administered by the Secretary of Education. This regulation protects student information and provides students specific rights with respect to their data.

ALABAMA RECORDS DISPOSITION AUTHORITY

Alabama Law Section 41-13-23 authorized the Alabama Department of Archives and History to publish rules for Local Government Records Destruction. For more information: http://www.archives.alabama.gov/officials/localrda.html.

RIGHTS OF CITIZENS TO INSPECT AND COPY PUBLIC WRITINGS; EXCEPTIONS

Alabama Law Section 36-12-40 Every citizen has a right to inspect and take a copy of any public writing of this state, except as otherwise expressly provided by statute. Provided however, registration and circulation records and information concerning the use of the public, public school or college and university libraries of this state shall be exempted from this section. Provided further, any parent of a minor child shall have the right to inspect the registration and circulation records of any school or public library that pertain to his or her child. Notwithstanding the foregoing, records concerning security plans, procedures, assessments, measures, or systems, and any other records relating to, or having an impact upon, the security or safety of persons, structures, facilities, or other infrastructures, including without limitation information concerning critical infrastructure (as defined at 42 U.S.C. §5195c(e) as amended) and critical energy infrastructure information (as defined at 18 C.F.R. §388.113(c)(1) as amended), the public disclosure of which could reasonably be expected to be detrimental to the public safety or welfare, and records the disclosure of which would otherwise be detrimental to the best interests of the public shall be exempted from this section. Any public officer who receives a request for records that may appear to relate to critical infrastructure or critical energy infrastructure information, shall notify the owner of such infrastructure in writing of the request and provide the owner an opportunity to comment on the request and on the threats to public safety or welfare that could reasonably be expected from public disclosure on the records.
(Code 1923, §2695; Code 1940, T. 41, §145; Acts 1983, No. 83-565, p. 866, §3; Act 2004-487, p. 906, §1.)

COPPA

The Children's Online Privacy Protection Act, regulates organizations that collect or store information about children under age 13. Parental permission is required to gather certain information; see www.coppa.org for details.

HIPAA

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

ISO Standards (http://www.iso.org/iso/home/standards.htm)

ISO 17799:2000 – Information technology – Code of practice for information security management
ISO 27001:2013 – Information technology – Security techniques – Information security management systems requirements.
ISO 27002L2013 - Information technology – Security techniques – Code of practice for information security controls.

Dissemination of Data Governance Policy

The Choctaw County Board of Education Data Security Policy will be made available to the public and all internal stakeholders via the System's Policy Manual at www.choctawal.org.

Data Governance Committee

Name	Department
Angela Phillips, Federal Programs Director	Federal Programs
Carol Taylor, School Nurse	Health Services
Dawn Dixon, Career Technical Center	Career Tech
Dr. Leo Leddon, Principal	Southern Choctaw High
Dorothy Banks, Superintendent	Superintendent
Kevin Howard, Human Resources	Human Resources
Regina Davis, Technology Coordinator	Technology
Rhonda Johnson, Accountability Specialists	Accountability
Seketha Mitchell, Chief School Financial Officer	Accounting
Grady Johnson, Technician	Technology
Jonathan Johnson, Principal	Southern Choctaw Elementary

Data Security Measures

I. Purpose

(A) Implement standards and procedures to effectively manage and provide necessary access to System Data, while at the same time ensuring the confidentiality, integrity and availability of the information.
(B) Provide a structured and consistent process for employees to obtain necessary data access for conducting Choctaw County School Systems operations.
(C) Define data classification and related safeguards. Applicable federal and state statutes and regulations that guarantee either protection or accessibility of System records will be used in the classification process.
(D) Provide a list of relevant considerations for System personnel responsible for purchasing or subscribing to software that will utilize and/or expose System Data.
(E) Establish the relevant mechanisms for delegating authority to accommodate this process at the school level while adhering to separation of duties and other best practices.

II. Scope

(A) These Security Measures apply to information found in or converted to a digital format. (The same information may exist in paper format for which the same local policies, state laws, statutes, and federal laws would apply, but no electronic control measures are needed.)
(B) Security Measures apply to all employees, contract workers, volunteers, and visitors of the Choctaw County School System and all data used to conduct operations of the System.
(C) Security Measures for public access to data as specified in the Rights of Citizens to Inspect and Copy Public Records.
(D) Security Measures apply to System Data accessed from any location; internal, external, or remote.
(E) Security Measures apply to the transfer of any System Data outside the System for any purpose.

III. Guiding Principles

(A) Inquiry-type access to official System Data will be as open as possible to individuals who require access in the performance of System operations without violating local Board, legal, Federal, or State restrictions.
(B) The Superintendent and/or a designee(s) shall determine appropriate access permissions based on local policies, applicable laws, best practices, and the Rights of Citizens to Inspect and Copy Public Records.
(C) Data Users granted "create" and/or "update" privileges are responsible for their actions while using these privileges. That is, all schools or other facilities are responsible for the System Data they create, update, and/or delete.
(D) Any individual granted access to System Data is responsible for the ethical usage of that data. Access will be used only in accordance with the authority delegated to the individual to conduct Choctaw County School System operations.
(E) It is the express responsibility of authorized users to safeguard the data they are entrusted with, ensuring compliance with all aspects of this policy and related procedures.
(F) These Security Measures apply to System data regardless of location. Users who transfer or transport System data "off-campus" for any reason must ensure they are able to comply with all data security measures prior to transporting or transferring the data.

IV. Access Coordination

(A) Central Office Department heads, supervisors, area specialists, and principals (Authorized Requestors) will assist in classifying data sensitivity levels for their areas of expertise and in identifying which employees require access to which information in order to complete their duties.
(B) The District Technology Coordinator, technician and the Superintendent will designate individuals to implement, monitor, and safeguard access to System Data based on the restrictions and permissions determined by the Authorized Requestors using the technical tools available.
(C) Central Office Department heads, supervisors, area specialists, and principals will be responsible for educating all employees under their supervision of their responsibilities associated with System Data security.

V. Data Classification

(A) Choctaw County School System's Data shall be classified into three major classifications as defined in this section. Requests for changes to the established data sensitivity classification or individual permissions shall come from the identified Authorized Requestors to the Technology Department.
1) Class I – Public Use: This information is targeted for general public use. Examples include Internet website content for general viewing and press releases.
2) Class II – Internal Use: Non-Sensitive (See Class III) information not targeted for general public use.
3) Class III – Sensitive: This information is considered private and must be guarded from unauthorized disclosure; unauthorized exposure of this information could contribute to identity theft, financial fraud, breach of contract and/or legal specification, and/or violate State and/or Federal laws.

(B) **FERPA Directory Information:**

Information disclosed as 'directory information' may fall into either Class I or Class II, depending on the purpose of the disclosure. The following is the District's list of which student information is to be considered 'directory information'.

Choctaw County Schools FERPA Directory Information Disclosure

The Family Educational Rights and Privacy Act (FERPA), a Federal law, requires that the Choctaw County School System with certain exceptions, obtain your written consent prior to the disclosure of personally identifiable information from your child's education records. However, Choctaw County School System may disclose appropriately designated 'directory information' without written consent, unless you have advised the system to the contrary in accordance with System procedures. The primary purpose of directory information is to allow the Choctaw County School System to include this type of information from your child's education records in certain school publications. Publications may be in print or digital format.

Examples include, but are not limited to, the following:

- A playbill, showing your student's role in a drama production;
- The annual yearbook;
- Honor roll or other recognition lists;
- Graduation programs; and
- Sports activity sheets, such as for football, showing weight and height of team members.

Directory information, which is information that is generally not considered harmful or an invasion of privacy if released, can also be disclosed to outside organizations without a parent's prior written consent. Outside organizations include, but are not limited to, companies that manufacture class rings or publish yearbooks, take school pictures, or process data.

In addition, two federal laws require local educational agencies (LEAs) receiving assistance under the *Elementary and Secondary Education Act of 1965* (ESEA) to provide military recruiters, and institutions of higher learning, upon request, three directory information categories – names, addresses and telephone listings – unless parents have advised the LEA that they do not want their student's information disclosed without their prior written consent.
If you do not want Choctaw County School System to disclose 'directory information' from your child's education records without your prior written consent, you must notify the school principal in writing within five (5) school days of the student's first day of attendance.

The System may disclose the following information as directory information:

- Student's name
- Address
- Telephone listing
- Electronic mail address (email)
- Photograph
- Date and place of birth
- Major field of study
- Dates of attendance
- Grade level
- Participation in officially recognized activities and sports
- Weight and height of members of athletic teams
- Degrees, honors, and awards received
- The most recent educational agency or institution attended
- A student number assigned by the System or State (in some cases*)

* In order to make certain software applications available to students and parents, the System may need to upload specific 'directory information' to the software provider in order to create distinct accounts for students and/or parents. Examples of these include, but are not limited to PCS (lunch program), Renaissance Learning (AR and STAR), online textbook vendors (to allow access to online text) and various other educational software applications and assessments. In these cases, the System will provide only the minimum amount of 'directory information' necessary for the student or parent to successfully use the software service.

Data Classifications for Students

Student Data	Classification	Authorized Users	Web Access
Student Name*	Class I or II, depending on use	All, as needed	First Name, Last Initial only, except in press release, school newspaper, or C2C
District Student Number	Class II	Principal, Asst. Principal, Counselor, Enrollment Clerk/Secretary, District INOW Designee, Teachers, Student, Parent, CNP, Media Specialist. Also export to approved service providers in order to establish unique identities or accounts – requires Data Governance Committee approval. Appropriate Central Office Administrators, Social Worker, Federal Programs Support Specialist	No
State Student Number*	Class II	Principal, Asst. Principal, Counselor, Enrollment Clerk/Secretary, District INOW Designee, Parent	No
Social Security Number*	Class III	Principal, Asst. Principal, Counselor, Enrollment Clerk/Secretary, District INOW Designee, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker	No
Home Phone Number	Class I or II, depending on use	Principal, Asst. Principal, Counselor, Enrolment Clerk/Secretary, District INOW Designee, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker, Assigned Teachers and After School workers, Federal Program Suppor Specialist, Social Worker, and Appropriate Central Office Administrators. School directories with parental permission being first obtained. Rapid notification system directory.	No
Home Address	Class I, II, III, depending on use	Principal, Asst. Principal, Counselor, Enrollment Clerk/Secretary, District INOW Designee, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker, Assigned Teachers and After School workers and Appropriate Central Office Administrators.	No
Ethnicity*	Class II	Principal, Asst. Principal, Counselor, Enrollment Clerk/Secretary, District INOW Designee, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker, Assigned Teachers and After School workers and Appropriate Central Office Administrators.	No
National School Lunch Program Status*	Class III	Principal, Asst. Principal, Counselor, Enrollment Clerk/Secretary, District INOW Designee, Testing Coordinator, Immediate teacher, Special Education Coordinator, Case Worker, Appropriate Central Office Administrators, CNP Director and staff (Point of Sale transactions will be done in a way as to not identify students who receive free or reduced lunches. Cafeteria managers/CNP employees who process F/R applications or lists of benefit recipients will ensure inform-ation is secure and available only to persons who require it.)	No

ESL Status*	Class II	Principal, Asst. Principal, Counselor, Enrollment Clerk/Secretary, District INOW Designee, Testing Coordinator, Federal Programs Director, Assigned Teachers, After School workers and Appropriate Central Office Administrators	No
Special Ed Status*	Class III	Principal, Asst. Principal, Counselor, Enrollment Clerk/Secretary, District INOW Designee,Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker, Assigned Teachers and Appropriate Central Office Administrators	No
Medical Conditions and/or Care Plans	Class III, except in emergencies	Principal, Asst. Principal, Enrollment Clerk/Secretary, Nurse, Immediate Teacher, Lunch Room personnel (if food allergy), and After School workers, if applicable	No
Grades	Class III, except when used in conjunction with honor rolls/awards	Principal, Asst. Principal, Enrollment Clerk/Secretary, District INOW Designee, Immediate Teachers, Student, Parents or legal guardian, Counselor, Gifted Teacher (only for students assigned), Appropriate Central Office Administrators, Testing Coordinator, Transfer to schools and Scholarship applications, C2C and Athletic Directors and Coordinators	INOW Parent Portal - Access is to be given to parents or legal guardians only. INOW Teacher web access
Attendance*	Class III	Principal, Asst. Principal, Attendance Clerk, Enrollment Clerk/Secretary, District INOW Designee, Immediate Teachers, Social Worker and Appropriate Central Office Administrators	INOW Parent Portal only
Discipline*	Class III	Principal, Asst. Principal, Counselor, Enrollment Clerk/Secretary, District INOW Designee and Appropriate Central Office Administrators	No
Standardized Test Scores*	Class III	Principal, Asst. Principal, Enrollment Clerk/Secretary, District INOW Designee, Immediate Teachers, Testing Coordinator, Appropriate Central Office Administrators, Student, Parent	No
System Benchmark Test Scores	Class III	Principal, Asst. Principal, Enrollment Clerk/Secretary, District INOW Designee, Immediate Teachers, Testing Coordinator, Appropriate Central Office Administrators, Student, Parent	No
*ALSDE may access all such information for State Reporting Collection purposes			

Data Classifications for Employees

Student Data	Classification	Authorized Users	Web Exposure
Employee Name*	Class I or II, depending on use	Human Resource Director, Principal, INOW data manager, District INOW Designee and Appropriate Central Office Administrators	Yes
District Employee Number	Class II	Principal, Payroll, Human Resource Director, as needed and Appropriate Central Office	No

		Administrators	
Social Security Number*	Class III	Human Resource Director, Payroll,	No
Home Phone Number	Class II	Human Resource Director, Principal, INOW data manager, District INOW Designee, Appropriate Central Office Administrators, school directories with employee permission, Rapid notification system directory	No
Home Address	Class III	Human Resource Director, Principal, Appropriate Central Office Administrators	No
Ethnicity*	Class II	Human Resource Director, Principal, Appropriate Central Office Administrators	No
Medical Conditions	Class III	School Nurse	No
Certifications*	Class II	Human Resource Director, Principal, Payroll, Appropriate Central Office Administrators	No
Attendance	Class III	Human Resource Director, Payroll, Principal, Appropriate Central Office Administrators	No
Evaluations*	Class III	Human Resource Director, Principal, Appropriate Central Office Administrators	No
College or school transcripts /grades	Class III	Human Resource Director, Principal	No
HQT Status*	Class II	Human Resource Director, Principal, Asst. Principal, Appropriate Central Office Administrators	Only as needed to comply with any Federal Programs reporting requirements
Prof. Dev. Records*	Class II	Human Resource Director, Principal, Asst. Principal, Appropriate Central Office Administrators	No
Benefits	Class III	Human Resource Director and Payroll	No
Salaries*	Class II	Human Resource Director, Principal, Asst. Principal, Appropriate Central Office Administrators	Schedules, but not individual salaries
*ALSDE may access all such information for State Reporting Collection purposes			

VI. Compliance

(A) Data Users are expected to respect the confidentiality and privacy of individuals whose records they access; to observe any restrictions that apply to Class III (Sensitive) data; and to abide by applicable laws, policies, procedures and guidelines with respect to access, use, or disclosure of information. The unauthorized use, storage, disclosure, or distribution of System Data in any medium is expressly forbidden; as is the access or use of any System Data for one's own personal gain or profit, for the personal gain or profit of others, or to satisfy one's personal curiosity or that of others.

(B) Each employee in the System will be responsible for being familiar with the System's Network Security and Internent Acceptable Use Policy and these Security Measures as they relate to his or her position and job duties. It is the express responsibility of Authorized Users and their respective supervisors to safeguard the data they are entrusted with, ensuring compliance with all aspects of this policy and related procedures.

(C) Employees, whether or not they are Authorized Users, are expressly prohibited from installing any program or granting any access within any program to Class III without notifying the Technology Department to determine whether or not adequate controls are available within the application to protect that data. *(The exception to this would be any software program purchased or utilized by the Alabama State Department of Education. In this case, the Alabama State Department of Education shall take all security responsibility for data it accesses or receives from Chocaw County School System.)*

(D) Violations of these Data Security Measures may result in loss of data access privileges, administrative actions, and/or personal civil and/or criminal liability.

VII. Implementation of Network/Workstation Controls and Protections and Physical Security

(A) **Shared Responsibilities**

1) The Technology Department shall implement, maintain, and monitor technical access controls and protections for the data stored on the System's network.
2) The Technology Department staff and/or the Authorized Requestor will provide professional development and instructions for Authorized Users on how to properly access data to which they have rights, when necessary. However, ensuring that all employees have these instructions will be the shared responsibility of the supervisor(s) of the Authorized User(s) and the Technology Department.
3) Technical controls and monitoring cannot ensure with 100% certainty that no unauthorized access occurs. For instance, a properly Authorized User leaves their workstation while logged in, and an unauthorized person views the data in their absence. Therefore, it is the shared responsibility of all employees to cooperatively support the effectiveness of the established technical controls through their actions.

(B) **Authorized Requestors**

1) Authorized Requestors are responsible for being knowledgeable in all policies, laws, rules, and best practices relative to the data for which they are granting access; including, but not limited to FERPA, HIPAA, etc.
2) Authorized Requestors shall be responsible for informing appropriate Technology Department personnel about data classifications in order that the Technology Department can determine the best physical and/or logical controls available to protect the data. This shall include:
   a. Which data should be classified as Class III
   b. Where that data resides (which software program(s) and servers)
   c. Who should have access to that data (Authorized Users)
   d. What level of control the Authorized User should have to that data (read only, read/write, print, etc.)

(C) **Location of Data, Physical Security and Application of Network and Computer Access Permissions**

1) Class III data shall be stored on servers/computers which are subject to network/workstation controls and permissions. It shall not be stored on portable media that cannot be subjected to password, encryption, or other protections.

2) Serving devices (servers) storing sensitive information shall be operated by professional network system administrators, in compliance with all Technology Department security and administration standards and policies, and shall remain under the oversight of Technology Department supervisors. All servers containing system data will be located in secured areas with limited access. At the school or other local building level, the principal or other location supervisor will ensure limited, appropriate access to these physically secured areas.

3) Persons who must take data out of the protected network environment (transport data on a laptop, etc.) must have the permission of their supervisor prior to doing so. Permission to do so will be granted only when absolutely necessary, and the person transporting the data will be responsible for the security of that data, including theft or accidental loss.

4) System staff who must print reports that contain Class II or III data shall take responsibility for keeping this material in a secure location – vault, locked file cabinet, etc. In addition, all printed material containing Class III documentation shall be shredded when no longer in use.

5) The Technology Department staff shall be responsible for implementing network protection measures that prevent unauthorized intrusions, damage, and access to all storage and transport mediums; including, but not limited to:
    a. Maintaining firewall protection access to the network and/or workstations.
    b. Protecting the network from unauthorized access through wireless devices or tapping of wired media, including establishing 'guest' wireless networks with limited network permissions.
    c. Implementing virus and malware security measures throughout the network and on all portable computers.
    d. Applying all appropriate security patches.
    e. Establishing and maintaining password policies and controls on access to the network, workstations, and other data depositories.

6) Technology Department staff will apply protection measures based on the Data Classifications (see sections IV and V), including:
    a. Categorizing and/or re-classifying data elements and views.
    b. Granting selective access to System Data.
    c. Documenting any deviation from mandatory requirements and implementing adequate compensating control(s).
    d. Conducting periodic access control assessments of any sensitive information devices or services.

(D) **Disposal of Hardware containing System Data**

1) Prior to disposal of any computer, the user will notify the Technology Department. A technician will remove the hard drive from the device and destroy it prior to the device being disposed of or auctioned off.

2) All schools and departments which purchase or lease copy machines or multifunction printers will be expected to include provisions for the destruction of data on the device's hard drive or the destruction of the hard drive itself prior to disposing of the copier or multifunction printer or its return to the leasing agency.

(E) **Sensitive Data as it pertains to Desktops/Laptops/Workstations/Mobile Devices**

1) Firewalls and anti-virus software must be installed on all desktops, laptops and workstations that access or store sensitive information, and a procedure must be implemented to ensure that critical operating system security patches are applied in a timely manner.

2) Storage of sensitive information on laptops, mobile devices, and devices that are not used or configured to operate as servers is prohibited, unless such information follows data security protocols (see sections V and VI, pages 6-8).

3) The user responsible for the device shall take proper care to isolate and protect files containing sensitive information from inadvertent or unauthorized access.

4) Assistance with securing sensitive information may be obtained from school-level Technology Coordinators with input from the Technology Department, as necessary.

VIII. Transfer of Data to External Service Provider

(A) Student Class I data, directory information, and, in some cases Class II data, may be transferred to an external service provider, such as an online website that teachers wish students to use for educational purposes. Provided that:

1) The teacher follows the protocols for getting approval for the site to be used.
2) The District notifies parents about their right to restrict their child's data from being shared with such sites annually via the Student Handbook and the Network Security and Internent Acceptable Use Policy.
3) The transfer of data is handled in a manner approved by the Technology Department, or is performed by the Technology Department.

(B) No Class III data, or FERPA protected educational records, will be transferred to an external service provider without prior approval of the Data Governance committee. Exception: Alabama State Department of Education.

(C) No school or department should enter into a contract for the use of any program that requires the import of District data without following established procedures when entering contracts for any programs/services that require data.

(D) The Data Governance committee will determine which of the following should be required of the service provider and assist in ensuring these requirements are met prior to any data transfer:
1) Contract
2) Designating the service provider as an "Official" as defined in FERPA
3) Memorandum of Agreement
4) Non-Disclosure Agreement

(E) Non-Disclosure Agreement (NDA) Information

When to Use a Non-Disclosure Agreement

1. Private Information. Confidential information, as defined by FERPA and other regulations and policies, is to be protected and disclosed only to those employees who have a direct legitimate reason for access to the data in order to provide educational services to the student.

2. You must seek guidance from relevant departments, and/or the Technology Department prior to transferring confidential information to any outside company, online service (free websites), or to any outside individual, organization, or agency without the explicit written permission of the parent of a minor student or an adult-aged student. This information includes:
    1) Social Security number
    2) Grades and test scores (local and standardized)
    3) Special education information
    4) Health information and 504 information
    5) Attendance information (not enrollment, but specific attendance dates)
    6) Family/homeless/or other similar status
    7) Child Nutrition Program status (free or reduced meals)

    This includes providing confidential information to individuals, including System employees, for use in dissertations or other studies for college courses or doctoral studies. Refer all such requests, including those for federal, state, or other studies to the Superintendent for approval before releasing any such individualized information. Approved recipients may be required to complete an NDA so that they fully understand their responsibilities with regard to safeguarding and later destroying this private information. This restriction does not apply to publicly available aggregated data such as dropout rates, attendance rates, percentage of free and reduced lunch program students.

    Exceptions. Other Public K-12 Schools - Private information may be transferred upon request to the State Department of Education or other public school systems with a legitimate need for the data; however, the transfer process should comply with data security protocols. In addition, personnel must research all recipients to ensure that the school is legitimately a public school rather than a private school.

    Colleges – Confidential information may be transferred to institutions of higher education, when the adult student or the parent of a minor student requests that transcripts or other private information be released to specific institutions. Such information should not be transferred to colleges based on a request from the college directly, unless approved by the adult student or the parent of a minor student whose records will be transferred. If the student is off-site, an electronic form may be obtained from the district/school website or by request from the school/system. The completed form must be signed and submitted to the school for approval prior to transfer of confidential information.

3. Directory Information. Although Choctaw County Schools have identified the following as "Directory Information," schools should still carefully consider the transfer or publication of this information. Seek guidance when in doubt. Much of this information, combined with data collected elsewhere can be used for identity theft purposes, stalking, and other unlawful or unethical purposes.
    1) Home address
    2) Home or cell phone numbers of students or their parents
    3) Email addresses of students or their parents
    4) Date and place of birth

    Exception: U.S. Military and institutions of higher learning for recruiting purposes. However, school must first determine which parents have submitted Opt Out forms relative to these requests prior to transferring data. (Refer to the Student's Network Security and Acceptable Use Consent Form)

4. Non-Disclosure Statement requirement for Contracted Services
    All contracts involving access to confidential/private information must include a non-disclosure statement in adherence with the Data Governance Policy.

(E) Non-Disclosure Agreement Processing

1) The Technology Department will keep all NDAs on file. This will eliminate the need for each school to solicit an NDA from companies which already have NDAs on file. Technology will also ensure that the NDA is renewed annually where necessary. The Data Governance Committee will ensure NDAs are revised annually.

2) What the school should do:

    a. Get the following specific information from the "entity" to which you want to transfer the information: company name, web address, phone number, fax number, and email address, name of individual you are working with.

    b. List the information you wish to transfer to the 'entity'

    c. Send this information to the Technology Department.

3) Upon approval by the Data Governance Committee, the Technology Department will determine if there is a current NDA already on file with the entity. If not, one will be prepared and sent to them. Once the agreement has been signed, the Technology Department will notify the school and oversee the process of securely uploading the necessary data to the service provider.

Nondisclosure Agreement

THIS NONDISCLOSURE AGREEMENT (this "Agreement"), by and between CHOCTAW COUNTY SCHOOLS, AL (the "System"), and _____ (the "Service Provider"), relates to the disclosure of valuable confidential information. The "System" refers to all schools, departments, and other entities within the Choctaw County School System. The Service Provider refers to any free or fee-based company, organization, agency, or individual which is providing services to the System or is conducting System-approved academic research. The Disclosing Party and the Receiving Party are sometimes referred to herein, individually as a "Party" and collectively, as the "Parties."

To further the goals of this Agreement, the Parties may disclose to each other, information that the Disclosing Party considers proprietary or confidential.
The disclosure of the System's Confidential Information by a Receiving Party may result in loss or damage to the System, its students, parents, employees, or other persons or operations. Accordingly, the Parties agree as follows:

Confidential Information disclosed under this Agreement by the System shall only be transmitted in compliance with the System's approved security protocols. The Receiving Party must accept the data transmitted in these formats.

The Service Provider will request or receive Confidential Information from the System solely for the purpose of entering into or fulfilling its contractual obligations or pre-approved academic research.

The Service Provider agrees not to use, or assist anyone else to use, any portion or aspect of such Confidential Information for any other purpose, without the System's prior written consent.

The Service Provider will carefully safeguard the System's Confidential Information and may be required to describe such safety measures to the System upon request.

The Service Provider will not disclose any aspect or portion of such Confidential Information to any third party, without the System's prior written consent.

Confidential Information disclosed under this Agreement shall not be installed, accessed or used on any computer, network, server or other electronic medium that is not the property of the System or the Service Provider, or to which third-parties have access, unless otherwise provided in a separate contract or agreement between the Parties hereto.

The Service Provider shall inform the System promptly if the Service Provider discovers that an employee, consultant, representative or any outside party has made, or is making or threatening to make, unauthorized use of Confidential Information.

The Service Provider shall immediately cease all use of any Confidential Information and return all media and documents containing or incorporating any such Confidential Information within five days to the System after receiving written notice to do so, or whenever the contract for services between the System and the Service Provider expires or is terminated. In addition, the Service Provider may be required by the System to destroy any Confidential Information contained on primary or backup media upon written request of the System.

Date	Date
System	Service Provider
Printed Name	Printed Name
Signature	Signature
Title	Title
Phone/Email	Phone/Email

Confidential Information includes:

- *any written, electronic or tangible information provided by a Disclosing Party*
- *any information disclosed orally by a Disclosing Party that is treated as confidential when disclosed*
- *all information covered by FERPA or other local, state, or federal regulation applying to educational agencies*
- *any other information not covered by FERPA, HIPAA, or other local, state, or federal regulation which the System requires the Service Provider to treat as confidential.*

TRANSCRIPT REQUEST FORM (for official high school transcript or GED scores)

Instructions to student: 1. **Complete this Transcript Request Form and send it to your high school.**
2. **Photo ID Required (Drivers License or State Issued ID)**
NOTE: Some schools charge a fee for official transcripts.

Social Security Number _____ Date of Birth _____

Last Name _____ First _____ Middle/Maiden _____

Other name(s) under which your records may be listed _____

_____ _____
Street Address City State Zip Phone Number

Transcript requested from (name of your high school):

_____

Enrollment dates: From _____ to _____

Graduation date: _____

Signature of Student _____ Date _____

SCHOOL official: Please send an official transcript to: (include complete mailing address)

_____

_____

_____

_____

IX. Reporting Security Breaches

All employees shall be responsible for reporting suspected or actual breaches of data security whether due to inappropriate actions, carelessness, loss/theft of devices, or failures of technical security measures.

Data Governance Training

I. School and Central Office Administrators

(A) School and Central Office Administrators will receive refresher training on FERPA and other data security procedures and emerging issues pertaining to data security annually at administrator's meetings

(B) Principals and Central Office Administrators shall contact the Technology Coordinator or the Superintendent when in doubt about how to handle Class II and III information

II. Data Security Training

(A) Enrollment clerks, secretaries and counselors will be trained and refreshed on FERPA and other data security procedures twice annually.

(B) Adherence to the data security procedures will be monitored by the Technology Department through random audits.

III. Teacher and Staff Training

(A) All new teachers will complete training on all System technology policies, including how their use of technology is governed by FERPA and other data security procedures established by the System.

(B) All department heads will be expected to educate their support staff on data governance as it applies to their department's work.

(C) All users will receive reminders throughout the year via email regarding malware threats and phishing scams and how to report suspected threats.

IV. Parent, Booster and Volunteer Training

(A) School administrators shall educate PTOs, boosters, and other parent groups about FERPA and student confidentiality. For instance, organizations who intend to post information about the school's students or activities should not compromise the privacy of students in protective custody. Because the school cannot tell these groups which students may be in such situations, the organization should be cautioned about exposing any information or photos that could cause harm to students or their families.

(B) The Technology Department shall have procedures that include educational materials for booster organizations who wish to post their own websites. This shall include both FERPA and COPPA information.

(C) The Technology Department shall educate volunteers and substitutes about FERPA, student confidentiality and INOW usage.

Data Quality Controls

I. Job Descriptions

(A) Job descriptions for employees whose responsibilities include entering, maintaining, or deleting data shall contain provisions addressing the need for accuracy, timeliness, confidentiality, and completeness. This includes, but is not limited to: enrollment clerks/school secretaries, human resource, accounting, data managers, counselors, special education staff, health services staff, social worker, federal programs support specialists, and CNP staff handling free and reduced lunch data.

(B) Teachers shall have the responsibility to enter grades accurately and in a timely manner.

(C) School administrators shall have the responsibility to enter discipline information accurately and in a timely manner.

II. Supervisory Responsibilities

(A) It is the responsibility of all Supervisors to set expectations for data quality and to evaluate their staff's performance relative to these expectations annually.

(B) Supervisors should immediately report incidents where data quality does not meet standards to their supervisors and to any other relevant department, including the State Department of Education, if applicable.

III. Software Systems/Applications

(A) Any software system owned or managed by the System which is used to store, process, or analyze student 'educational records' as defined by FERPA shall be subject to strict security measures. These systems are:

1) INOW – General student information system
2) SetsWeb – Special Education information system
3) PCS – Child nutrition information system
4) McAleer – Accounting System

(B) Administrators with supervisory responsibilities over the System's Student Information Systems shall determine the appropriate access rights to the data and enforce compliance with these roles and permissions.

INOW Access

INOW, unlike its predecessor STI Office, enables authorized users to access the application from anywhere they may have Internet access. In response to this anywhere/anytime access, as well as the fact that INOW provides less-granular permission settings than its predecessor, the Data Governance Committee and the Leadership Team has implemented the following:

(A) Strong password requirement for INOW logins

(B) Data Security Agreements for those with INOW permissions.

Medical Information

Choctaw County School System will allow medical information in INOW regarding medical conditions to be available to medication assistance. Medical assistance are employees required to complete 12 hours of medical assistance program training.

Choctaw County Schools Data Security Agreement

Electronic data is very portable and can be vulnerable to theft and unintended disclosure. Therefore, having access to personal and private information as part of one's job duties also carries with it important responsibilities to protect the security and privacy of that data.

As an employee who has access to Choctaw County Schools' student and employee data, I understand that I have the responsibility to handle, maintain, and disseminate information contained in these records in a secure manner.

I understand that my access to and dissemination of student and/or employee data is subject to local polices, as well as state and federal laws and statutes. This includes, but is not limited to the Federal Educational Rights and Privacy Act (FERPA) and HIPAA.

I understand that transferring personal information to a third party outside of the school system in any electronic format may only be done after approval by an appropriate Coordinator and the Technology Department.

Except when explicitly instructed to do so by school or system administrators, I understand that copies of student and employee data should never be kept on a temporary storage device such as USB drive or CD; and that student and employee data should not be removed from the school premises on a laptop.

I will keep my computer workstation secure by locking or logging off when the machine is unattended. I will not share network or program passwords with others. I will not allow personal data that has been printed into the view or hands of unintended parties. I will not use my software rights to grant others permission to data to which they are not entitled.

Athletic – Quick Entry Edit Provision (Applies to Athletic Staff only)

I understand that access to the Quick Entry Edit utility is being added to my permission so that I may rapidly identify student athletes per the directions provided by the AHSAA. I agree not to delegate this responsibility to others. I will be careful in selecting the Athletic field and the correct students so that school does not incur unintended insurance costs.

Please sign below to indicate you understand and agree to the above statements.

Printed Name	Signature
Date	Location

(C) 'Notification of Risks' to school administrators and enrollment clerks/secretaries

Notice of Risks Related to INOW Usage

INOW Access for Parent Volunteers

Some schools rely on parent volunteers to help greet visitors and locate students. Due to FERPA and other confidentiality expectations volunteers should only be granted very limited INOW rights. In most cases this should be the 'Schedule Lookup' level of access which enables the volunteer to see a list of all students and their schedules.

Concerns about Parent Volunteers Checking Students Out of School (Parent volunteers will not check out student's)????

Releasing a child from school into the care of someone else is a serious responsibility. Schools should carefully assess whether or not the information in INOW for this purpose is always up to date. In the past registrars have raised concerns that parents often change their minds about who can and cannot check out their children, but they don't necessarily notify the school in a timely manner. This makes the prospect of allowing parent volunteers who are unfamiliar with the current circumstances of various family situations to check out students an area of concern. Student Services will be providing recommendations regarding this important function.

Allowing Others to Use Another User's INOW Account to 'Give' them Greater Access is Prohibited

A user's INOW permission level is based on their job responsibilities. Violating FERPA can have serious consequences, including the loss of Federal Funding and other legal liabilities. Since we have a responsibility to protect our student and employee data from identity theft or other misuse, no one may log into INOW and allow others to use their access. Participating in this practice violates our Acceptable Use policies and Data Security Procedures and could result in disciplinary actions.

The Technology Department will perform random scans to determine if the same INOW user id is in use concurrently on two separate computers and investigate these occurrences as warranted.

Plan for when your Enrollment Clerk/Secretary is Out for an Extended Period

You should have a plan for occasions when your enrollment clerk/secretary is out sick or on vacation. Anyone filling in should be a bona fide employee, not a volunteer. Technology will attempt to help in extreme situations, but our ability to do so is limited.

Providing Information to Others on Students NOT Enrolled at Your School

INOW rights intentionally prevent the staff at one school from seeing information on students at another school, which complies with FERPA guidelines. The only exception is for district level personnel who have specific needs to see all school data and teachers or others who serve specific students in multiple schools.

It is important that staff members at one school do not attempt to give information about students enrolled in another school to individuals who ask for such information. Instead they should expect the person asking for the information to contact that school themselves. If the person asking for information does not know what school to contact, then they should be referred to the Technology Department.

DO NOT tell an individual who has no official right to know where else the student is enrolled. Even if the person asking is a parent, there may be a dangerous situation of which you are unaware, so the safe action to take is to refer such requests to the School Administrator.

The danger in telling someone, employee or not, what other school the child is enrolled in lies in the fact that you have no access to that student's record and will not know if the child is in protective custody or is involved in some other situation such as custody dispute, etc. This could result in a safety issue.

This rule applies even when the person asking for the information is one of our own employees. Unless the person requesting the information is currently providing educational services to that student, they should not be given any information about them, including where the student is enrolled. And, if they are providing educational services to a student at another school, but claim not to know where the child is enrolled, then this should raise some flags. In this case, contact the School Administrator for guidance.

INOW Permission Standards for Choctaw County Schools

Access and permissions will be determined by the Superintendent of Education with guidance from the Leadership Team.

Email Use and Security Agreement

I. User Agreement

All individuals issued an email account by Choctaw County Schools are expected to follow the System's Network Security and Internet Acceptable Use Policy.

II. Email Disclaimer

This message, and any files transmitted with it, may contain confidential information and is intended only for the individual addressee(s). If you are not the named addressee or if you have received this email by mistake, you should not disseminate, print, distribute or copy this e-mail. If you have received this email by mistake, please notify the sender immediately and delete this e-mail from your system. Employees of the Choctaw County Board of Education are expressly required not to make defamatory statements and not to infringe or authorize any infringement of copyright or any other legal right by email communications. Any such communication is contrary to Board policy and outside the scope of the employment of the individual concerned and result in disciplinary actions.

Banking Security

I. ACH Transfers

The Technology Department will assist in evaluating whether or not any practices would pose an unacceptable risk to the System's network.

II. Bank Balance Auditing Recommendations for Preventing Electronic Theft

The Technology Department highly recommends that the System and school bank balances which employ electronic payment measures, be checked daily, or within the timeframe given by the bank, in order to report fraudulent withdrawals in order to recover stolen funds.

Data Backup and Retention Procedures

I. Purpose of Data Backup and Retention Procedures

(A) Ensure that procedures for comprehensive data backup are in place and that system data is restorable in the event of data corruption, software or hardware failures, data damage or deletion (either accidental or deliberate), and properly executed requests from the office of the Superintendent, or forensic purposes.
(B) Provide a documented policy of how long data is retained, and therefore restorable.
(C) Provide documentation of what systems and data are specifically included in, and excluded from, backup and retention.
(D) Establish the groups or individuals responsible for data backup and retention procedures, including the on-site and offsite locations of backup media.
(E) Establish the procedural guidelines used to initiate a data restore.

II. Scope

(A) This Policy applies to all servers and systems installed and controlled exclusively by the Choctaw County Schools Technology Department. In cases where other Departments are responsible for their backup systems, the Technology Department will provide technical and professional guidance for backup routines and procedures, as requested.

(B) This Policy applies to all user data in the following manner:
All users with network permissions are permitted to store files on local machines. Individual users may delete their data from local machines at will. Files stored by users on individual hard drives or other individual storage devices are not backed up and may become unrecoverable in the case of hard drive failure or accidental deletion. Although technicians may be able to locate or recover locally stored files, these files are not part of the data backup or recovery plan.

(C) This Policy does not apply to connected systems which are the property, and therefore the responsibility, of outside entities such as the Alabama State Department of Education.

(D) This Policy excludes the e-mail system, as its backup and retention system is separate from other systems.

III. General System Data Backup Procedures

(A) Student Information System (Chalkable-INOW)

1) Offsite Remote Backup
Currently an offsite backup provided by Chalkable in conjunction with Enveloc Inc. is in place. From the Student Information Systems source database, a nightly scheduled process occurs to compress, encrypt, and transmit one copy of the InformationNow database backup to the Enveloc storage cloud. This file is accessible for remote access provided that the user account, encryption key, and password are all provided and active.
2) Access to prior years student data may be limited/unavailable due to the changeover from the STI Legacy program to the new web based INOW program. Structural changes to the table design in some cases may prevent access to certain areas of the data as well as the discontinuation of support for the Legacy program.
3) Veeam Ware Server Backup.
The Application and Database server is scheduled to backup every week night at midnight. Backup files are stored onsite on the server. Restore will be done with Veeam Backup and Recovery. Restore time is approximately 8 hours.

(B) PCS – Backups are scheduled daily, onsite. Backups are stored weekly and overwritten.

(C) McAleer – Local backup procedures are performed by accounting staff and overwritten each day. Offsite backups are also scheduled and performed by the company.

V. Time Frames for Data Retention

(A) All statements of data retention, and the subsequent ability to restore that retained data, are subject to hardware and software components functioning properly. Time frames may change depending on the amount of data the System generates and the budget provided to manage these services. In the event of a catastrophic event, such as the destruction of the Network Operations Center, some levels of data recovery will be affected, but recovery will still be possible to some point within the last 30 days provided off-site locations have not been similarly destroyed

(B) Retention of Web Traffic and Browsing Data.
There is currently no system in place to retain Web Traffic and Web Browsing Data. Older data is cleared from system within hours of its recording, due to the high rate of new incoming data.

(C) Litigation

(1) It shall be the responsibility of the Central Office administrators to promptly inform the Technology Department of any pending litigation where user files or emails may be requested.

(2) Once notified, the Technology Department will take all available actions to retain all affected files and emails, such that they are not deleted according to the retention schedules.

VI. Email Archiving

(A) Google Apps for Education was implemented for the system email. Email, using the domain address @choctawal.org, will be part of this implementation. This is an auxiliary email account and is intended to be used for administrative staff and other designated employees and between students and teachers for instructional use only. This email system is hosted by Google. It will not be backed-up by the System. If the System exits the Google Apps for Education program, this data will become unavailable to the System.

VII. Responsibility of Data Backup and Data Retention

(A) The Technology Department assumes responsibility of facilitating, operating, maintaining, checking and testing the DataBackup System.

(B) Contracted service providers which currently include: Chalkable(formerly STI), Harris Computers, PCS and ClearWinds Technologies, Scantron, Renaissance Learning, SchoolMessenger, and SchoolDesk.

VIII. Data Restore Procedures

(A) In the event that a network user requires that data be restored from the DataBackup System, they shall do one of the following:

1) Contact their School Technology Coordinator
2) Contact the System Technician
3) Contact the System Technology Coordinator