Data Governance

Policy & Procedures

The following documents are affiliated with Chickasaw City Schools Data Governance policy, procedures, training, and guidance.

Contents

State Monitoring Checklist Cross-Reference

	ON-SITE	INDICATORS	ECS Data Governance Plan
1.	Has the 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	See committee files Committee
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	Board Policy
3.	Does the data governance policy address physical security?	Documented physical security measures	Controls and Protections
4.	Does the data governance policy address access controls and possible sanctions?	Current list of controls Employee policy with possible sanctions	General provisions Data transfers Powerschool Permissions Reporting breaches Data Security Agreements Email –Violations and Enforcement
5.	Does the data governance policy address data quality?	Procedures to ensure that data are accurate, complete, timely, and relevant	Quality Controls
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	Data transfers and Non-Disclosure Agreements Disclosure of data via email
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	Dissemination of policy Data Security Training

Applicable Laws and Standards

The District will abide by any law, statutory, regulatory, or contractual obligations affecting its information systems. The District's data governance policy and procedures are informed by the following laws, rules, and standards, among others:

FERPA

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

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.

ALABAMA OPEN RECORDS LAW

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.

Payment Card Industry Data Security Standard (PCI DSS)

This 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. See www.PCI security standards.org for more information.

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

Data Security Policy

Policy History:

Current Policy: 1101 Adopted: February 28, 2019

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.

Dissemination of Data Governance Policy

The Chickasaw City Schools Data Security Policy, section 1100, is available to the public and all internal stakeholders via the District Policy Manual at www.chickasawschools.com

The detailed policies, provisions, and procedures that serve to implement that Policy 4.10 are shown below. As exposing these specific security measures to outside, unknown parties could result in greater risk to the District's data, this document will not be made publicly available. Requests for detailed information about the District's data security procedures shall be brought to the committee or the Superintendent who will determine the legitimacy of the request and respond accordingly.

Data Governance & Powerschool Permissions Committee

Name	Department
Data Governance Committee Only	
Nash Campbell	Legal
Data Governance and Powerschool Permissions Committee	
Juwan Withers	Technology
Mark Isley	Curriculum
Sheila Smith	Special Education
Chris Arras	Finance
Powerschool Permissions Committee Only	

Data Security Measures

Adopted: February 28, 2019

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. Insofar as this policy deals with access to Chickasaw City Schools' computing and network resources, all relevant provisions in the Acceptable Use Policies are applicable.

(B) Provide a structured and consistent process for employees to obtain necessary data access for conducting Chickasaw City Schools 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 Chickasaw City Schools and all data used to conduct operations of the System.

(C) Security Measures do not address public access to data as specified in the Alabama Open Records Act

(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 his designees shall determine appropriate access permissions based on local policies, applicable laws, best practices, and the Alabama Open Records Act.

(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 Chickasaw City Schools 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 that 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 System Technology Coordinator and Technical Services Supervisor will designate individuals within the technology department 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) Chickasaw City Schools System 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 above 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'.

……

Chickasaw City Schools FERPA Directory Information Disclosure

The Family Educational Rights and Privacy Act (FERPA), a Federal law, requires that the Chickasaw City Schools (District), with certain exceptions, obtain your written consent prior to the disclosure of personally identifiable information from your child's education records. However, Chickasaw City Schools may disclose appropriately designated 'directory information' without written consent, unless you have advised the district to the contrary in accordance with District procedures. The primary purpose of directory information is to allow the Chickasaw City Schools 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 wrestling, 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, with 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 Chickasaw City Schools 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 District may disclose the following information as directory information:

- Student's name
- Address
- Telephone listing
- Electronic mail address
- 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 District (in some cases*)

* In order to make certain software applications available to students and parents, the District 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 MyLunchMoney.com, Blackboard Connect, and various education software applications. In these cases, the District 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, Registrar, 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.	No
State Student Number*	Class II	Principal, Asst. Principal, Counselor, Registrar Student, Parent	No
Social Security Number*	Class III	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker	No
Home Phone Number	Class I or II, depending on use	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker, Assigned Teachers and After School Care workers. 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, Registrar, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker, Assigned Teachers and After School Care workers	No
Ethnicity*	Class II	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker, Assigned Teachers and After School Care workers	No
National School Lunch Program Status*	Class III	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, CNP Coordinator and staff, Immediate teacher, (Point of Sale transactions will be done in such a way as to not identify students who	No

		receive free or reduced lunches. Cafeteria managers and CNP employees who process F/R applications or lists of benefit recipients will ensure the information is secure and made available only those persons who require it.)	
ESL Status*	Class II	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, ESL Supervisor, ESL Dept. employees, Assigned Teachers and After School Care workers	No
Special Ed Status*	Class III	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, Special Ed Coordinator, and Special Ed. Case Worker	No
Medical Conditions	Class III, except in emergencies	Principal, Asst. Principal, Registrar, Nurse, Immediate Teacher, Lunch Room personnel (if food allergy), and After School Care workers, if applicable	No
Grades	Class III, except when used in conjunction with honor rolls/awards	Principal, Asst. Principal, Registrar Immediate Teachers, Student, Parents or legal guardian, School Counselor, Gifted Teacher (only for students assigned), PST Committees, Appropriate Central Office Administrators, Testing Coordinator, Transfer to schools and Scholarship applications, C2C	Powerschool 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, Registrar, Student Services Coordinator and staff, Truancy Officers, School Resource Officer, Immediate Teachers, PST Committee	Powerschool Parent Portal only
Discipline*	Class III	Principal, Asst. Principal, Counselor, SRO, Registrar, Student Services	No
Standardized Test Scores*	Class III	Principal, Asst. Principal, Registrar, Immediate Teachers, Testing Coordinator, Appropriate Central Office Administrators, PST Committee, Student, Parent	No
System Benchmark Test Scores	Class III	Principal, Asst. Principal, Registrar, Immediate Teachers, Testing Coordinator, Appropriate Central Office Administrators, PST Committee, 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 Resources, Principal, INOW data manager	Yes
District Employee Number	Class II	Principal, Payroll, Human Resources, and Maintenance staff, as needed	No
Social Security Number*	Class III	Human Resources, Payroll, Principal, INOW data manager	No
Home Phone Number	Class II	Human Resources, Principal, INOW data manager, school directories with employee permission, Rapid notification system directory	No
Home Address	Class III	Human Resources, Principal, INOW data manager	No
Ethnicity*	Class II	Human Resources, Principal	No
Medical Conditions	Class III	Human Resources, Principal	No
Certifications*	Class II	Human Resources, Principal, Payroll	No
Attendance	Class III	Human Resources, Payroll, Principal	No
Evaluations*	Class III	Human Resources, Principal	No
College or school transcripts or grades	Class III	Human Resources, Principal	No
HQT Status*	Class I	Human Resources, Principal, Asst. Principal, Registrar, Appropriate Central Office Administrators	Only as needed to comply with any Federal Programs reporting requirements
Prof. Dev. Records*	Class II	Human Resources, Principal, Asst. Principal, Registrar, PD Supervisor, Appropriate Central Office Administrators	No
Benefits	Class III	Human Resources and Payroll Staff	No
Salaries*	Class II	Human Resources, Principal, Asst. Principal, Registrar, 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 at the System will be responsible for being familiar with the System's Data Security 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.

(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) System employees, including Authorized Requestors, shall not select or purchase software programs that will utilize or expose Class III data without first consulting the Data Governance Committee 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 Chickasaw City Schools.)*

3) The Data Governance Committee 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 Data Governance Committee.

4) 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 (Section IV. A) 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 Data Governance Committee personnel about data classifications in order that the Data Governance Committee 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 (i.e. read only, read/write, print, etc.)

(C) **Location of Data and Physical Security**

1) 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.
2) District staff who must print reports that contain Class II or III data shall take responsibility for keeping this 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.

3) 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.

4) 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.
5) Printed 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.

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

1) Prior to disposal of any computer, the user will notify the Technology Department.

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 MFP or its return the leasing agency. (See Exhibit D.)

(E) **Application of Network and Computer Access Permissions**

1) 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.

2) Technology Department staff or District System Administrator 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.

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

3) Assistance with securing sensitive information may be obtained 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. Provide 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 Code of Conduct/AUP.

   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 first consulting and receiving approval from the Data Governance committee.

(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 Understanding
   4) Memorandum of Agreement
   5) Non-Disclosure Agreement

……

The following instructions comply with Chickasaw City Schools Policy 1101 Data Security

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 the Student Services, Special Education, 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 Instruction Department and the Technology Department for their 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 (see below). 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 individual whose records will be transferred.

3. Directory Information. Although Chickasaw City Schools has 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 notification relative to these requests prior to transferring data.

……

(E) Non-Disclosure Agreement Processing

1) All NDAs will be kept on file at the Brewton Central Office. This will eliminate the need for each school to solicit an NDA from companies which already have NDAs on file. The system will also ensure that the NDA is renewed annually where necessary.
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 for referral to the Data Governance Committee.
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 securing uploading the necessary data to the service provider.
4) Note that all confidential data that will be transferred by email, whether in the body of the email or as an attached file, should be encrypted. The Technology Department can help you with transporting this data.

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 annually at principals meetings

(B) Principals and Central Office Administrators shall contact the Data Governance Committee when in doubt about how to handle Class II and III information

(C) Principals and Central Office Administrators will be kept aware of emerging issues pertaining to data security.

II. School Registrar Data Security Training

(A) School registrars will be trained and refreshed on FERPA and other data security procedures annually.

(B) School registrars' 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 District technology policies, including how their use of technology is governed by FERPA and other data security procedures established by the District.

(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 and Booster 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 Data Governance Committee 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.

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: school registrars, counselors, special education staff, 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 monitor 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 the Data Governance Committee.

Student Information Systems

I. Student Information Applications

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

1) Powerschool – General student information system
2) Powerschool Special Programs – Special Education information system
3) Heartland/Mosaic – Child nutrition information system

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

II. Powerschool Access

The Data Governance Committee, has implemented the following:

(A) Strong password requirement for Powerschool logins

(B) Data Security Agreements for those with Powerschool permissions who are not teachers

……

Chickasaw City 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 Chickasaw City 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 policies, 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 district 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.

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

.....

Printed Name	Signature
Date	Location

Data Security Agreement: Athletic – Quick Entry Edit Provision

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 Chickasaw City 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 policies, 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 district 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

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 registrars

Notice of Risks Related to Power School Usage

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

A user's Power school 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 Power school and allow others to use their access. Participating in this practice violates our Acceptable Use policies and Data Security Procedures.

Plan for when your Registrar is Out for an Extended Period

You should have a plan for occasions when your registrar is out sick or on vacation. Anyone filling in for the registrar 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

Power school 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 Student Services 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 that you are now unaware of, so the safe action to take is to refer such requests to the Student Services Department.

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 Student Services for guidance.

……

Powerschool Permission Standards for Chickasaw City Schools As of February 28, 2019

I. Permission Committee

(A) An Powerschool Permissions committee was formed in June of 2014, members include:

1) Data Governance Committee
2) Powerschool central support staff and data engineer responsible for Powerschool
3) Principal representatives

4) Testing/Counseling representative

(B) Requests for changes to the standards set by the Powerschool Permissions committee can be made at any time by a school or District-level administrator. School administrators will be notified prior to the annual committee meeting so that they can submit requests in writing prior to that date for consideration.

(C) Changes to settings may also be made by the committee decision as a result of software changes, new job roles, other local factors, directives from the State, or as determined by the Superintendent.

(D) The permissions are granted to individuals officially serving in the roles shown below. However, these permissions will not be granted automatically. The individual's principal/supervisor must endorse them by submitting their name to the Technology Department. Principals and supervisors will be asked to renew their endorsements annually. In addition, these endorsements may be revoked if the principal, supervisor, or the committee determines that the access is no longer necessary or has other reasonable concerns. The Powerschool Permissions Committee makes the final determination for access settings.

(E) The Powerschool Permissions committee will meet annually in order to review permissions and to consider new requests. Requests that are made between annual meetings will be presented to the members via email or in-person, as appropriate. Changes will be conveyed to affected personnel via memos and updates to the manual.

II. Powerschool Permission Settings

Powerschool user permissions will be determined by the Powerschool permissions committee.

Email Use and Security Agreement

I. User Agreement

All individuals issued an email account by Chickasaw City Schools are expected to follow the District's Email Use and Security Agreement. This agreement is provided all new staff. (See Exhibit)

Banking Security

I. ACH Transfers

The CFO should notify the Technology Coordinator of any plans to change its electronic banking processes. The Technology Department will assist in evaluating whether or not any such practices would pose an unacceptable risk to the District's network.

II. Bank Balance Auditing Recommendations for Preventing Electronic Theft

The Data Governance Committee highly recommends that the District and school bank balances which employ electronic payment measures be checked within the time frame 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 onsite and offsite locations of backup media.

(E) Establish the procedural guidelines used to initiate a data restore.

II. Scope

(B) This Policy applies to all servers and systems installed and controlled exclusively by the Chickasaw City Schools Technology Department. (Systems Table I) and excludes servers and systems controlled by specific departments within Chickasaw City Schools (Systems Table II). 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 trained and urged to store data onto their server workspace, but they are permitted to store files on local machines. Individuals users may delete their data from either network servers or local machines at will. If data stored on a server is deleted by the end user and falls outside of the backup period, the System has no method of recovering such files.

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.

III. General System Data Backup Procedures

(A) Source Server Shadow Copy

1) As data is changed, replaced or deleted on school and district servers, older versions of that data are preserved.
2) Shadow Copy occurs automatically once per day, Monday thru Friday.
3) Includes any data that has been added or modified in the last 24 hours.
4) Shadow Copy versions are housed on the same storage which originally contained the data.
5) Servers are physically isolated from students and most faculty members to protect from tampering and disturbance.

(B) Incremental Backups

1) System Data that has been added or modified since the last backup operation is backed up to centralized Data Backup Network Attached Storage (NAS) devices.
2) Incremental Backups occur automatically once per day, 7 days a week.
3) Data Backup NAS devices are housed at the Network Operation Center (NOC), a facility designed for increased security and protection.

IV. Email Data Backup Procedures

Gmail is currently archived through google Vault. If the District exits the Google Apps for Education program, this data will become unavailable to the District.

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.

(B) The time frames listed below are based on what time frames are currently possible and affordable with current staff and funds for backup servers and media. Time frames may change depending on the amount of data the System generates and the budget provided to manage these services.

(C) Data Retention time frame is expressed as a minimal amount of time for which any protected data should be recoverable, utilizing the multiple protection mechanisms available under normal circumstances.

(D) 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.

(E) Retention of General System Data.

1) Retained for normal restores for a period of two weeks.
2) Preserved on external hard drives twice a year for extended restore ability

(F) E-Mail Data is retained for a Disaster-Recovery full-system restore by service providers. Chickasaw City Schools does not archive email conversations for litigation purposes.

1) See email backup procedures above.

(G) Retention of Web Traffic and Browsing Data.

1) There is currently no system in place to retain Web Traffic and Web Browsing Data.

(H) Backup logs will be maintained by Technology Personnel

(I) Litigation Holds

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 become part of eDiscovery requests.
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 above.

VI. Email Archiving

(A) Google Apps for Education was implemented in 2016 Email, using the domain address @chickasawschools.com, will be part of this implementation. This email system is hosted by Google. Mailbox contents can be downloaded on an as-needed basis by the District's Google Apps administrators to recover deleted items or conduct investigations. If the District exits the Google Apps for Education program, this data will become unavailable to the District.

VII. Data Included / Excluded

(A) Data is generally included by default when a new server or system is configured to be backed up by the Data Backup System.

(B) Configuration of the Data Backup System is reviewed twice per calendar year by the Technology Department to ensure that systems are being adequately protected.

(C) All data included or excluded for the Data Backup System is included in (or excluded from) all the routines of the system, including:

1) Server Shadows
2) Incremental Backups

Data specifically included in the Data Backup System:

1) General application drive (Q :) at schools
2) Backups repository on all servers, encompassing:
3) SQL database backups
4) SQL applications
5) Server System State

(E) Excluded data is generally excluded because it is especially large AND appears in the same format and version on multiple servers throughout the school system.

1) Data specifically excluded from the Data Backup System:

a) Server Operating System, swap files, temp files & lock files.
b) Ghost files and ISO image files.
c) Uncompressed backup or transaction files
d) Static data that is replicated on multiple servers
e) Any directory that's name begins with an exclamation point (!)

IX. Responsibility of Data Backup and Data Retention

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

X. Systems Table I

Systems under the Control of the Technology Department

System	Location in Chickasaw, AL
Domain Controllers & File Servers	201 N. Craft Hwy 80 Grant St. 50 Chieftain Way

XI. Systems Table II

Systems NOT Under the Control of the Technology Department

System	Location

References:

Section 8-1A-13 - Admissibility in evidence.

(a) In any proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form.

(b) In determining the attribution and authenticity or evidentiary weight of an electronic record or signature, the trier of fact may consider, along with any other relevant and probative evidence, proof of the efficacy of any security procedure applied. This may include a showing that the procedure: (1) uniquely identifies the signer or creator of the record; (2) prevents others from using the same identifier; and/or (3) provides a mechanism for determining whether the data contained in the record was changed after it was created or signed. Evidence bearing on the means and the reliability with which the procedure performs these functions may also be considered.

Section 8-1A-5 - Use of electronic records and electronic signatures; variation by agreement.

(a) This chapter does not require a record or signature to be created, generated, sent, communicated, received, stored, or otherwise processed or used by electronic means or in electronic form.

(b) This chapter applies only to transactions between parties each of which has agreed to conduct transactions by electronic means. Whether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the parties' conduct.

(c) A party that agrees to conduct a transaction by electronic means may refuse to conduct other transactions by electronic means. The right granted by this subsection may not be waived by agreement.

(d) Except as otherwise provided in this chapter, the effect of any of its provisions may be varied by agreement. The presence in certain provisions of this chapter of the words "unless otherwise agreed," or words of similar import, does not imply that the effect of other provisions may not be varied by agreement.

(e) Whether an electronic record or electronic signature has legal consequences is determined by this chapter and other applicable law.