

Scottsboro City Schools

Data Governance

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

Contents

State Monitoring Checklist Cross-Reference.....	4
Applicable Laws and Standards.....	5
Data Security Policy	6
Dissemination of Data Governance Policy	6
Data Governance Committee.....	7
Data Security Measures	8
I. Purpose	8
II. Scope.....	8
III. Guiding Principals.....	9
IV. Access Coordination	9
V. Data Classification.....	10
Data Classifications for Students	12
Data Classifications for Employees	14
VI. Compliance	15
VII. Implementation of Network/Workstation Controls and Protections and Physical Security.....	16
VIII. Transfer of Data to External Service Provider	18
IX. Reporting Security Breaches.....	22
Data Governance Training.....	23
I. School and Central Office Administrators.....	23

II. School Registrar Data Security Training.....	23
III. Teacher and Staff Training	23
IV. Parent and Booster Training	23
Data Quality Controls	24
I. Job Descriptions	24
II. Supervisory Responsibilities.....	24
Student Information Systems	24
I. Student Information Applications.....	24
II. INOW Access	25
INOW Permission Standards for Scottsboro City Schools.....	29
I. Permission Committee.....	29
II. Allowable INOW Permission Settings	30
I. INOW Substitute Teacher Set Up & Roles.....	33
Email Use and Security Agreement.....	35
I. User Agreement.....	35
II. Scottsboro City Schools Email Disclaimer	35
Banking Security.....	35
I. ACH Transfers.....	35
II. Bank Balance Auditing Recommendations for Preventing Electronic Theft.....	35
Data Backup and Retention Procedures.....	36
I. Purpose of Data Backup and Retention Procedures.....	36
II. Scope	37
III. General System Data Backup Procedures.....	37
IV. E-mail Data Backup Procedures.....	38
V. Time Frames for Data Retention	39
VI. INOW Alabama State Back Up	40
VII. Email Archiving	40
VIII. Data Included / Excluded	41
IX. Responsibility of Data Backup and Data Retention	42

X. Data Restore Procedures	43
XI. Systems Table I.....	43
XII. Systems Table II.....	44
Exhibit A: - Examples of INOW Permissions Memoranda.....	45
Exhibit B: - Identity Theft Training.....	47
Exhibit C: Email User Agreement	51
Exhibit D: Copier Machine Security Recommendations.....	54
Provisions for Consideration – Not Yet Implemented.....	55
Electronic Signature Agreement (Not Implemented).....	55
Restrictions on Parents Posting Images of Students (who are not their own children) to Social Media (Not Implemented)	57

State Monitoring Checklist Cross-Reference

	ON-SITE	INDICATORS	SCS 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 INOW 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 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 (PHI). 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.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 27002:2013 – Information technology – Security techniques – Code of practice for information security controls

Data Security Policy

Policy History:

Current Policy: 6.12	Adopted: July 10, 2014
<p>Educational records as defined by law or Board policy will be available for examination and review by authorized persons in the manner prescribed and to the extent required by law. Except where the context requires otherwise, the term “educational records” has the meaning given in 20 U.S.C. 1232g(a)(4). Copies of such records may likewise be provided to the extent required and under circumstances specified by applicable law or regulation. The Superintendent is authorized to establish administrative standards and procedures respecting access to such records, including a schedule of reasonable changes for the reproduction thereof. Parents will be provided required annual notification regarding educational records through the student handbook or by other appropriate means.</p> <p>[Reference: 20 U.S.C. §1232g(a)(4); 34 CFR 99.3]</p>	

Dissemination of Data Governance Policy

The Scottsboro City Board of Education Data Security Policy, section 6.12, is available to the public and all internal stakeholders via the District Policy Manual at www.scottsboroschools.net.

The detailed policies, provisions, and procedures that serve to implement that Policy 6.12 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 Committee

Name	Department
Tony LaRue	Technology Coordinator
Alan Garner	Testing Coordinator
Tracy Brumley	Technology, iNow
INOW Permission Committee	
Tony LaRue	Technology Coordinator
Alan Garner	Testing Coordinator
Tracy Brumley	Technology, iNow

Data Security Measures

Adopted October, 2014

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 Scottsboro 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 Scottsboro 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 Scottsboro 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 Principals

- (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 Scottsboro 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) Scottsboro 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’.

Scottsboro City Schools FERPA Directory Information Disclosure

Updated to include District student number on May 6, 2014

The Family Educational Rights and Privacy Act (FERPA), a Federal law, requires that the Scottsboro 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, Scottsboro 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 Scottsboro 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 Scottsboro 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	Class III	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, CNP	No

Status*		Coordinator and staff, Immediate teacher, (Point of Sale transactions will be done in such a way as to not identify students who 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, Special Ed. Case Worker, Assigned Teachers and After School Care workers	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	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, Registrar, Student Services Coordinator and staff, Truancy Officers, School Resource Officer, Immediate Teachers, PST Committee	INOW 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,	No

		PST Committee, Student, Parent	
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 II	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 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 Scottsboro City Schools.)*
- 3) 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.
- 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 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 (i.e. read only, read/write, print, etc.)

(C) Location of Data and Physical Security

- 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.
- 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) 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.
- 5) District 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.

(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 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 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.

(F) 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 is encrypted in a Technology Department-approved encryption format.
- 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. 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
- (E) Non-Disclosure Agreement (NDA) Information

The following instructions comply with Scottsboro City Schools Policy 4.10 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 Scottsboro 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 forms relative to these requests prior to transferring data.

(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.
- 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.

(F) Sample Non-Disclosure Agreement

Nondisclosure Agreement

THIS NONDISCLOSURE AGREEMENT (this “Agreement”), by and between SCOTTSBORO CITY SCHOOLS, AL (the “District”), and _____ (the “Service Provider”), relates to the disclosure of valuable confidential information. The “District” refers to all schools, departments, and other entities within Scottsboro City Schools. The Service Provider refers to any free or fee-based company, organization, agency, or individual which is providing services to the District or is conducting District-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 District’s Confidential Information by a Receiving Party may result in loss or damage to the District, its students, parents, employees, or other persons or operations. Accordingly, the Parties agree as follows:

Confidential Information disclosed under this Agreement by the District shall only be transmitted in compliance with the District’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 District 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 District’s prior written consent.

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

The Service Provider will not disclose any aspect or portion of such Confidential Information to any third party, without the District’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 District 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 District promptly if the Service Provider discovers that an employee, consultant, representative or other party, 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 (5) days to the District after receiving written notice to do so, or whenever the contract for services between the District and the Service Provider expires or is terminated. In addition, the Service Provider may be required by the District to destroy any Confidential Information contained on primary or backup media upon written request of the District.

Date	Date
District	Service Provider
Printed Name	Printed Name
Signature	Signature
Title	Title
Phone/Email	Phone/Email
<p>Confidential Information includes:</p> <ul style="list-style-type: none">• 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 District requires the Service Provider to treat as confidential	

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 Technology Coordinator or the Students Services Department 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, such as the information shown in [Exhibit B](#).

II. School Registrar Data Security Training

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

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 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 superior and to any other relevant department, including the State Department of Education, if applicable.

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 are:
 - 1) INOW – General student information system
 - 2) SetsWeb – Special Education information system
 - 3) PCS – 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. 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 its, INOW permissions sub-committee, has implemented the following:

- (A) Strong password requirement for INOW logins
- (B) Data Security Agreements for those with INOW permissions who are not teachers

STI Data Security Agreement Memo

Date: _____

To: Principals

From: Tony LaRue

RE: Data Security and Data Security Agreement

As you know, our student employee data should be carefully protected. Not only is much of this information subject to FERPA and HIPAA, but it is also data which could be used for identity theft. In order to ensure that all staff members who have access to STI Office understand the important responsibilities that come with such access, we have prepared the attached STI Data Security Agreement form.

Please read the document carefully and notice that it warns against removing personal data on students and employees from the workplace. This type of information should not be carried outside of your school on USB drives, disks, or on laptops. If any of these portable devices were to be lost or stolen, it could put the system at great risk.

Please make enough copies of this document for each of your staff who have STI **Office** permissions to sign. Have them sign the form. Make them a copy of the signed form, and then forward the original to the Technology Department. This will include you, your assistant principals, your counselors, the school nurse, and a few others in your school. The registrars have already received and signed a copy at the recent Registrar's meeting.

If you have questions, please feel free to contact me.

Scottsboro 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 Scottsboro 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 Scottsboro 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/Title

Signature

Date

Location

(C) 'Notification of Risks' to school administrators and registrars

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. Remember, INOW permissions are web-based so what volunteers can see from the school, they can also access from anywhere they have Internet access.

Concerns about Parent Volunteers Checking Students Out of School

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.

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. Registrars who are using multiple machines have been instructed to notify Technology of this so that dual logins on specific IP addresses will not be viewed as a potential violation of this rule.

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

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 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.

INOW Permission Standards for Scottsboro City Schools

As of October 2014

I. Permission Committee

- (A) An INOW Permissions committee was formed in October of 2014, members include:
- 1) Technology Coordinator/Data Governance Committee chairperson
 - 2) INOW central support staff and data engineer responsible for INOW
 - 3) Students Service department representatives
 - 4) Principal representatives
 - 5) Testing/Counseling representative
- (B) Requests for changes to the standards set by the INOW 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 INOW Permissions Committee makes the final determination for access settings.

- (E) The INOW 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. (See [Exhibit A.](#))

II. Allowable INOW Permission Settings

As of October 2014

Group: **Find Student Only** (Schedule Lookup)

Staff Affected: All INOW Users. (Parent Volunteers may be granted this permission, but only when the INOW Permissions Committee approves a request submitted by a principal.)

All INOW users can use the Look Up feature to find any student's current location. The staff can also refer to a Student Schedule Matrix pdf file which the school's Registrar will post to the Faculty Share. Registrars will update the file as needed.

Only Technology INOW administrators can add individuals to this permission group.

Group: **Check In/Out**

Staff Affected: Assigned by Technology upon request

This level of permission allows the user to see the Summary, Main, and Contacts tabs. It gives them the ability to check students in and out and to view the following information:

- Name
- Date of Birth
- Age
- Phone (This can be hidden if necessary)
- Gender
- Grade (This can be hidden if necessary)
- Address (This can be hidden if necessary)
- List of Contacts and their relationship and phone numbers

The user will see the special symbols, but not open up these notes to see what instructions they contain.

Only Technology INOW administrators can add individuals to this permission group.

Group: Limited Student View

Staff Affected: Library Media Specialists*

Staff with “Limited Student View” permissions will have Read-Only rights to contact information for all students in the school.

**Library Media Specialist may have additional permissions if they give grades or serve in other roles within the school.*

Only Technology INOW administrators can add individuals to this permission group.

Group: Test Data Entry

Staff Affected: Secretaries in counseling offices (if requested by principal)

These permissions enable staff to enter testing data.

Only Technology INOW administrators can add individuals to this permission group.

Group: Special Student View

Staff Affected: Individuals serving in the following roles, when endorsed by the principal/supervisor

- Athletic Directors (Can also be added to AD Quick Entry Edit Group, see below)
- Lead Special Ed Teachers
- Lead ESL Teachers
- PST Chairperson

Staff with “Special Student View” permissions will be able to see the following information for ALL students in the school:

- Contacts – full records
- Grades which have been posted by teacher
- Attendance profile
- Schedules

Principals may also want to ask Registrars to set up Non-Reporting Class Rosters (see below) for individuals who have been granted Special Student View permissions. Or, they may want to request that these individuals be set up with Non-Reporting Class Rosters *instead of* being given

the Special Student View. In either case, Non-Reporting Classes can make it easier for individuals to look up information on the students they are responsible for because it will enable them to check each student's information from a 'class' roster (i.e. football, PST, girl athletes, etc.) rather than look up each student by name in INOW. Creating these 'Non-Reporting Class Rosters' will take more work on the Registrar's part. However, it is a good option when principals want to restrict access to only the students served by the individual, rather than all students in the school.

Group: Athletic Directors Quick Entry & Future Year

Staff Affected: Athletic Directors only

Middle and high school athletic directors will be given the ability to use the Quick Entry Edit feature in INOW to edit students' eligibility settings, but only after being trained by the school registrar.

Athletic Directors with this permission must sign the associated [Security Agreement](#).

Group: Non-Reporting Class Rosters

Staff Affected: Various

When teachers have a formal responsibility to support students who they do not have on a class roll, and this responsibility includes viewing the students' grades, then the Registrar may be asked to set up a Non-Reporting Class for that teacher. Examples of these situations/individuals include:

- Special Education teachers with students on their caseload, but who are not in their class
- Academics First Sponsor
- Math or Reading Coaches, where applicable
- Gifted advisors, where applicable
- Anyone who already has or would be eligible for the Special Student View (above)

Once the 'class' is created, the 'teacher' will have the ability to 'print' a comprehensive progress report for the students which will give the 'teacher' access to posted grades from all classes. Keep in mind that this will take some work on the Registrar's part. In the case of the Athletic Director and a separate Academics First teacher, they could both be listed as teachers for the non-reporting class to minimize the work involved.

The Technology Department will provide Registrars with directions for creating these non-reporting classes. These directions must be followed carefully so that the courses do not affect

attendance, LEAPS, or other state reports. These courses will need to be scheduled outside of the school day, must be tagged as a non-reporting course in the Master Schedule, and must use the correct State Course Number.

Group: **Discipline History**

Staff Affected: Administrators Only

Only school administrators will have access to student discipline history. Staff should consult with their school administrators if they need discipline history on a given student.

AHSAA Student in Good Standing Forms –

The AHSAA Student in Good Standing Release Form must be completed and signed by the school Principal. This is only to be completed when the student athletes leaving your school are not in good standing.

I. INOW Substitute Teacher Set Up & Roles

As of October 2014

All Subs and Temporary Employees who are granted INOW access must sign the STI Security Agreement. The school registrar should facilitate this and store the Agreement at the school. If a Long Term Sub works at more than one school, each school should have a signed Agreement on file.

When possible, the teacher going on leave should set up the class grade book before the Long Term Sub takes over. Technology INOW administrators can assist in setting up grade books if the teacher is not able to do so prior to his/her absence.

Group: **Substitute Teacher Access**

Staff Affected: Long Term Subs and Temporary Employees

Scenario 1: **Short Term Sub (under 21 days)**

INOW: No access

- If the teacher does not return after 20 days, then the sub may have INOW access as a Long Term Sub. Select the appropriate Scenario from those listed below.
- If it is known in advance that the teacher will be out for longer than 20 days but less than 1 semester then use either Scenario 2 or 3, whichever applies.

Scenario 2: Sub over 21 days, but less than 1 Semester (aka Long Term Sub)

INOW Role: Long Term Sub
INOW Schedule: Additional Teacher

Scenario 3: Long Term Sub/Temporary Employee* for more than 1 semester, but less than 1 year

INOW Role: Long Term Sub
INOW Schedule: Additional Teacher

EXCEPTION: If the original teacher will not be returning to your school (i.e. transferring, resigning, retiring, etc.) then they should be removed from the master schedule and the teacher replacing them should be shown as:

INOW Role: Long Term Sub
INOW Schedule: Teacher

Scenario 4: Temporary Employee* for one full year

If the ***original teacher has highest degree*** and years of experience, then the Temporary Employee will have:

INOW Role for Temporary Employee: Long Term Sub
INOW Schedule for Temporary Employee: Additional Teacher
INOW Role for Teacher on Leave: First Primary Teacher
INOW Schedule for Teacher on Leave: Teacher

If ***the temporary employee has highest degree*** and years of experience, then the Temporary Employee will have:

INOW Role: First Primary Teacher
INOW Schedule: Teacher
INOW Role for Teacher on Leave: None
INOW Schedule for Teacher on Leave: None

Email Use and Security Agreement

I. User Agreement

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

II. Scottsboro City Schools Email Disclaimer

Adopted August 2012

*****CONFIDENTIAL*****

The information in this e-mail message is legally privileged and confidential information intended only for the use of the addressee(s) named above. If the reader of this message is not the intended recipient or the agent responsible to deliver it to the intended recipient, you are hereby notified that any review, copying, dissemination, distribution, forwarding or the taking of any action in reliance on the contents of this communication is prohibited. If you have received this e-mail in error, please notify the sender as soon as possible. In addition, please delete the erroneously received message from any device/media where the message is stored.

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 Technology Department highly recommends that the District 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 (not completely implemented)

The following standards may be updated, amended, or changed as needed. Any changes will be clearly marked and prior versions will be kept available for review.

Backup and Retention Change Log		
Date	Description	Person
3/16/2007	Original Created	
10/2/2008	Email Backup portion amended	Susan Poling
1/5/2009	Corrected numbering of section 4	Susan Poling
10/13/2011	Updated tape/disk procedures, Exchange information, iNOW & added Sept. 5 th Email Archive outage.	Walter Alexander
12/04/2013	Update INow, Google Apps, Email servers and other minor edits	Susan Poling w/ staff input

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

(B) This Policy applies to all servers and systems installed and controlled exclusively by the Scottsboro City Schools Technology Department. (Systems Table I) and excludes servers and systems controlled by specific departments within Scottsboro 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.

(D) This Policy includes a special section for the e-mail system, as its backup and retention system is separate from other systems.

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 servers 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 DataBackup Network Attached Storage (NAS) devices.
 - 2) Incremental Backups occur automatically once per day, 7 days a week.
 - 3) DataBackup NAS devices are housed at the Network Operation Center (NOC), a facility designed for increased security and protection.
- (C) Exports
- 1) System Data residing on the DataBackup NAS devices is copied to removable drives.
 - 2) Exports are manually run by a Network Administrator, or their designee, once a day, Monday thru Friday, during normal working hours.
 - 3) If school is closed, missed exports are run the next working day to "catch up" to the current day.
 - 4) Includes any data not already on the Export Drive.
 - 5) Export Drives are initially stored in protective cabinets at the NOC.
 - 6) Export Drives are rotated to a second SCBOE facility on a weekly basis to provide greater physical protection in the event of a disaster.
- (D) Bi-Annual Comprehensive Data Storage
- 1) Twice a year, just before Christmas break and just before the start of school in August, a complete copy of all data housed on the centralized DataBackup NAS devices is initiated to external hard drives.
 - 2) Includes all data residing on the DataBackup NAS devices.
 - 3) Drives are stored in the second SCBOE facility once the backup jobs are complete.
 - 4) Bi-annual backup drives will be stored indefinitely.

IV. E-mail Data Backup Procedures

- (A) The e-mail system is comprised of multiple servers, including three "Mailbox" servers.
- (B) Two Mailbox servers are duplicated to a mailbox server at the Central Office for Disaster-Recovery with a 24-hour lag-time. This lag-time provides a window to detect data

corruption and prevent that corruption from spreading from the active systems to the backup systems.

- (C) The backup procedure is designed for a full-system restore, as opposed to the ability to restore individual messages.
- (D) Backup processes are automatic.

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. Time frame changes will be noted in a log kept by the System Technical Services Supervisor noting the reason for any time frame change and approval from the Deputy Superintendent.
- (C) Data Retention timeframe 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 within the last 30 days provided off-site locations have not been similarly destroyed.
- (E) Retention of General System Data.
 - 1) Retained for normal restores for a period of two weeks.
 - 2) Rotated off-site on a weekly basis.
 - 3) 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 for a period of two weeks.
 - 1) Rotated off-site on a weekly basis.
- (G) Retention of Web Traffic and Browsing Data.
 - 1) 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.

- (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. INOW Alabama State Back Up

- (A) Student Information System - Offsite Remote Backup
 - 1) Currently an offsite backup provided by Software Technology Incorporated (STI) 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.

VII. Email Archiving

- (A) In September, 2008, a Barracuda Email Archive appliance was added to the network. The device is set to retain all internal and external mail for long-term retrieval purposes. The size of the hard drive space allotted for this may need to be expanded over time to accommodate a full 2 years of data. Expansion of disk space will be based on available funding at the time. Prior to the addition of the Email Archive appliance, the back-up/retention for email was two (2) weeks.
- (B) The Barracuda Email Archive appliance is not backed up. Losses from catastrophic events damaging equipment or data may be irrevocable.
- (C) Event Log for Email Archiving

- (D) On September 5, 2011, there was a hardware failure of the Barracuda Email Archive appliance following a power outage. Although we cannot confirm any data loss, the appliance was offline, or operating in a degraded state, from September 5, 2011 until October 10, 2011. The accuracy and recoverability of e-mail data from this time period is questionable.
- (E) Google Apps for Education was implemented for students in grades K-12 in August 2014, the staff has been using Google Apps since August 2012. Email, using the domain address @scottsboroschools.org, will be part of this implementation. This is an auxiliary email account and is intended to be used between students and teachers for instructional use only. This email system is hosted by Google. It will not be backed-up by the District. Mailbox contents can be downloaded on an as-needed basis by the District's Google Apps administrators to recover deleted items or conduct investigations. The search capabilities of this system are limited and the length of time these mailboxes are kept available is not within our control. In addition, if the District exits the Google Apps for Education program, this data will become unavailable to the District.

VIII. Data Included / Excluded

- (A) Data is generally included by default when a new server or system is configured to be backed up by the DataBackup System.
- (B) Configuration of the DataBackup System is reviewed twice per calendar year by the Network Administration Team (Network Engineers, Network Administrators and the Technical Services Supervisor) to ensure that systems are being adequately protected.
- (C) All data included or excluded for the DataBackup System is included in (or excluded from) all the routines of the system, including:
 - 1) Server Shadows
 - 2) Incremental Backups
 - 3) Exports
 - 4) Bi-Annual Tape Jobs
- (D) Data specifically included in the DataBackup System:
 - 1) ~~STI (Legacy) application share at schools~~ (moved to VMs at NOC)
 - 2) General application drive (Q :) at schools
 - 3) Faculty home directories
 - 4) Faculty shared data areas
 - 5) Student home directories
 - 6) Student shared data areas
 - 7) Backups repository on all servers, encompassing:

- 7.1) SQL database backups
- 7.2) SQL applications (such as ACT)
- 7.3) 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 DataBackup 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 (i.e. Lee Vs. Macon)
- e) Any directory that's name begins with an exclamation point (!)
- f) STI Legacy Data - final copy of legacy data is on external USB hard drive in vault in TNOC. Local schools have lookup availability through virtual servers.

IX. Responsibility of Data Backup and Data Retention

- (A) The Technology Department assumes responsibility of facilitating, operating, maintaining, checking and testing the DataBackup System.
- (B) For schools leaving SCS, a backup copy of the INOW database will be turned over to STI after all state report have been submitted and approved by ALSDE at the end of the school year. It should be understood that the original data will remain with SCS.
- (C) The chief architect and operator of the DataBackup System is Walter Alexander.
- (D) Walter Alexander is responsible to provide documentation, and to instruct the members of the Network Administration and Network Engineering groups, in the proper maintenance and operation of the DataBackup system.
- (E) The ultimate responsibility of the DataBackup system, it's maintenance, operation and procedures falls to (in order):
 - 1) Walter Alexander
 - 2) Network Engineers
 - 3) Network Administrators

X. 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 the Technology Help Desk
 - 2) Contact their School Technology Coordinator (TC)
 - 3) Contact Walter Alexander, Technical Services Supervisor
- (B) A Restore Request Form shall be completed for every requested restore, regardless of the outcome.
- (C) Restores shall be given High Priority treatment and initiated in an expedited manner.
- (D) The requestor shall be notified when the restore operations are complete, to ensure that data is accessible and meets the user's needs.
-

XI. Systems Table I

Systems under the Control of the Technology Department

System	Location	Special Conditions	Date Changes/Notes
Web Server(s)	dNOC	Annual website backup made only	
iNOW Servers	dNOC	Data replicated from dNOC to OMHS	
School Domain Controller Servers	School NOC	Yes	
School Application Server	dNOC	Yes	
School Course Servers (i.e. graphics, etc)	dNOC	No	

XII. Systems Table II

Systems NOT Under the Control of the Technology Department

System	Location	Special Conditions	Date Changes/Notes
McAleer			
NextGen			

End of Document Backup and Retention Procedures

Exhibit A: - Examples of INOW Permissions Memoranda

Home Access and Passwords Memo from 2008

(Originally this memo pertained to Outside Access to STI Legacy grade book)

We are happy to announce that we are nearly ready to enable STI Classroom access from home for your teachers. If you have been one of the pilot sites for this, please note that the pilot phase is now at an end and that access will be temporarily disabled until the following steps have been taken.

It is extremely important that teachers use a strong password for STI. Your school has already received instructions from Lisa Kirkpatrick to put this in motion. In the past, teachers have used weaker passwords but have generally been able to spot any student who appears to be “tampering” with their computer. Once we enable access to STI Classroom from the Internet, any student who knew or could guess a teacher’s password – could go online from anywhere and get into the teacher’s gradebook. Therefore, we are requiring principals at all schools to assure us that they have had teachers change their STI password to one that will provide more security.

Even if a teacher does not plan to use STI from home, they must still change their password.

You are already prepared to have teachers change their network password to a strong password on Sept. 6th. Please note that the network password and the STI password should be different from one another. So teachers need to think of one password with a minimum of 8 characters for the network and another for STI.

Attached please find a Certification sheet. Once we receive your assurance that your teachers have changed their STI passwords, we will open up access to STI Remote Classroom on a school by school basis. We are hoping to have every school make this change by Friday so that teachers can test out the home access over the weekend if they choose.

In addition, please DO NOT keep a list of teachers’ STI passwords in your office or use some type of uniform naming convention for STI passwords. Both of these pose additional security risks. Since teachers do attendance everyday it is highly unlikely that they will forget their STI password. If this should happen, the Technology office can reset the password for them.

I am sure you are aware that other school systems have been having grade changing concerns. This plan of the teacher being the only one with the password to STI Classroom and the school administrators and registrar only having the STI Office passwords is aimed at ensuring that access is clearly defined. It is the teacher’s responsibility to keep his/her password secure just as it is your responsibility to keep the STI Office password secure. Principals can still review student grades and teacher lesson plans from the Principal’s module so this should not hinder you in any way.

We have posted a podcast that will tell teachers about STI from home and will be sending that link to your TCs so that they can pass it on to your teachers.

If you have questions, please give me a call.

What is a “strong password?”

- Between **8** and **15** characters long
- Includes at least 1 **number**
- Includes at least 1 **special character** (\$,%*,!,?, a **space**, etc.)
- Does **not** contain your personal information (dog or child’s name, social security number, birthday, etc.)
- Is not written down anywhere near the computer or where it could be easily found. (Especially a sticky note on the monitor or in the top desk drawer!!!)

Note: Passwords in INOW are *not* case-sensitive, so it doesn’t matter if letters are entered as lower case or upper case.

DATE: October 2014

TO: School and District Administrators

RE: INOW Permissions

FROM: INOW Permissions Committee

The INow Permissions Committee met on September 4th to review our standards and discuss possible

changes. The committee determined that our current standards remain effective in terms of balancing various employees' need for access with our responsibility to keep student and employee information confidential.

The following information is important, please read this entire memo.

Summary of New Permissions & Standards

Athletic Directors

Middle and high school athletic directors will be given the ability to use the Quick Entry Edit feature in INOW to edit students' eligibility settings, but only after being trained by the school registrar.

Check In/Check Out Permission Group

A new level of permissions for staff checking students in and out has been established. This permission level has slightly more access than Schedule Lookup, which is typically used by parent volunteers. (See permissions descriptions that follow.) Only Technology INOW administrators can add individuals to this permission group.

Long Term Subs & INOW Permissions

See the INOW Permission Handbook section of this memo for details.

All Subs and Temporary Employees who are granted INOW access must sign the STI Security Agreement. The school registrar should facilitate this and store the Agreement at the school. If a Long Term Sub works at more than one school, each school should have a signed Agreement on file.

When possible, the teacher going on leave should set up the class grade book before the Long Term Sub takes over. Technology INOW administrators can assist in setting up grade books if the teacher is not able to do so prior to his/her absence.

Exhibit B: - Identity Theft Training

Data Security Education for Registrars

February 22, 2007

Operating a school and school system means handling personal data for thousands of students and employees. It is our responsibility to take security measures to ensure that our data does not end up in the hands of identity thieves. According to the Federal Trade Commission's 2005 report:

- Alabama ranked 31st in reports of identity theft
- Birmingham, AL ranked highest in the number of victims
- The highest number of victims were in the 18-29 year old group

What is identity theft?

Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.

Young people, 18-29 years of age, are the number one target for identity thieves, according to Quest, a communications company that is working to raise awareness of the issue.

Teenagers and young people are more vulnerable to identity theft than adults because most have not established credit records that can be monitored.

Teens also are more susceptible to identity theft because they are less likely to check their credit card records and may not even be aware of their credit record and its importance. Most teens have little or no knowledge of financial transactions and credit reports.

Most teens discover they have fallen victim to identity theft when they apply for a driver's license and are denied because one has already been issued under their Social Security number.

Source: http://www.pbs.org/newshour/extra/features/july-dec05/idtheft_8-29.html

How do identity thieves get your personal information?

- They get information from businesses or other institutions by:
 - stealing records or information while they're on the job

- bribing an employee who has access to these records
- hacking these records
- conning information out of employees
- They may steal your mail, including bank and credit card statements, credit card offers, new checks, and tax information.
- They may rummage through your trash, the trash of businesses, or public trash dumps in a practice known as "dumpster diving."
- They may get your credit reports by abusing their employer's authorized access to them, or by posing as a landlord, employer, or someone else who may have a legal right to access your report.
- They may steal your credit or debit card numbers by capturing the information in a data storage device in a practice known as "skimming." They may swipe your card for an actual purchase, or attach the device to an ATM machine where you may enter or swipe your card.
- They may steal your wallet or purse.
- They may complete a "change of address form" to divert your mail to another location.
- They may steal personal information they find in your home.
- They may steal personal information from you through email or phone by posing as legitimate companies and claiming that you have a problem with your account. This practice is known as "phishing" online, or pretexting by phone.

What is "pretexting" and what does it have to do with identity theft?

Pretexting is the practice of getting your personal information under false pretenses. Pretexters sell your information to people who may use it to get credit in your name, steal your assets, or to investigate or sue you. Pretexting is against the law.

Pretexters use a variety of tactics to get your personal information. For example, a pretexter may call, claim he's from a research firm, and ask you for your name, address, birth date, and social security number. When the pretexter has the information he wants, he uses it to call your financial institution. He pretends to be you or someone with authorized access to your account. He might claim that he's forgotten his checkbook and needs information about his account. In this way, the pretexter may be able to obtain other personal information about you such as your bank and credit card account numbers, information in your credit report, and the existence and size of your savings and investment portfolios.

Keep in mind that some information about you may be a matter of public record, such as whether you own a home, pay your real estate taxes, or have ever filed for bankruptcy. It is not pretexting for another person to collect this kind of information.

What do thieves do with a stolen identity?

Once they have your personal information, identity thieves use it in a variety of ways.

Credit card fraud:

1. They may open new credit card accounts in your name. When they use the cards and don't pay the bills, the delinquent accounts appear on your credit report.

2. They may change the billing address on your credit card so that you no longer receive bills, and then run up charges on your account. Because your bills are now sent to a different address, it may be some time before you realize there's a problem.

Phone or utilities fraud:

- They may open a phone or wireless account, or run up charges on your existing account.
- They may use your name to get utility services like electricity, heating, or cable TV.

Bank/finance fraud:

- They may create counterfeit checks using your name of account number.
- They may open a bank account in your name and write bad checks.
- They may clone your ATM or debit card and make electronic transfers in your name, draining your accounts.
- They may take out a loan in your name.

Government documents fraud:

- They may get a driver's license or official ID card issued in your name but with their picture.
- They may use your name to get government benefits.
- They may file a fraudulent tax return using your information.

Other fraud:

- They may get a job using your Social Security number.
- They may rent a house or get medical services using your name.
- They may give your personal information to police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.

What do you do if you believe personal data has been exposed or stolen at your school site?

Notify both the Technology Coordinator and the Deputy Superintendent immediately. These individuals will take the appropriate next steps of investigating and notifying law enforcement.

Preventative Measures to be take at all Scottsboro City School locations:

- Ensure only authorized personnel have access to INOW and other applications that contain personal information.
- Use good password protection and do not give others access to your password or computer if you have access to software containing personal information.
- Do not use social security numbers on printed documents unless absolutely necessary.

- Shred any printed documents with personal information that was printed and is no longer needed.
- BE SURE ALL EMPLOYEES “Lock” or Log Off their workstations when away from their desks. (See instructions below).
- Educate your staff about identify theft.
- Ensure your employees are not giving out phone numbers or other personal information about employees or students to anyone who is not requesting it for an official business purpose. (Do not allow employees to give out the home phone numbers of parents or employees as a courtesy to someone who asks for it.)

Locking a computer workstation:

Press Control – Alt – Delete

Click “Lock Workstation”

When you return you will press any key and then use your password to log back into the computer.

Exhibit C: Email User Agreement

Electronic communications, in its many forms, can be a very efficient and effective method of communicating with others; however, it has many inherent risks. Once sent or posted, the author no longer has control over the information contained in the message or posting. The purpose of this Acknowledgement is to make Scottsboro City Board of Education employees and others granted network accounts aware of certain risks and responsibilities that accompany using electronic communications provided by Scottsboro City Schools.

This Acknowledgement provides guidance on the professional, ethical, legal, and responsible use of System electronic communications (E-mail, list serve, web site, etc.). This document does not constitute all rules concerning electronic communications. Refer to Scottsboro City Schools' [Policy website](#) for a complete list of policies.

This Acknowledgement applies to all full-time employees, part-time employees, contracted employees, temporary employees, and other agents operating on behalf of Scottsboro City Schools. It applies to any person or group of persons who have E-mail accounts, and also to those who request that an account holder send a message on their behalf. It is applicable to all electronic communications regardless of the physical location (school, office, home, or any other offsite location) of the user.

Prohibited Use

The Scottsboro City Schools' electronic communications programs shall not be used for the creation or distribution of any content that:

- Discloses unauthorized or restricted information to inside or outside parties via electronic communications, including restricted or confidential information that would violate the privacy of individuals or violate any other local, state, or federal laws including, but not limited to [FERPA](#) and [HIPAA](#).
- Contains private information such as student grades, discipline incidents, suspensions, social security numbers, special education status, or Individualized Education Plans in cases where it would violate FERPA.
- Discloses personal information regarding students, faculty, staff, or parents to third parties.
- Contains information that pertains to someone other than the addressee (For instance, do not address E-mails to numerous individuals that contains private information that does not apply to all of the recipients).
- Defames, slanders, or libels another person or organization.
- Contains or links to pornography or other content inappropriate for K-12.
- Contains content that may be considered offensive or discriminatory, including, race, gender, hair color, disabilities, age, sexual orientation, religious beliefs and practice, political beliefs, or national origin.
- Contains content or files that violate any copyright or trademark law. Users should be aware that passing on E-mails that contain copyrighted or trademarked material may make them liable in copyright or trademark infringement cases even though they were not the original sender.
- Intentionally contains malicious or harmful software such as computer viruses and spyware.
- Contains fraudulent, harassing, or intimidating content.
- Violates any license governing use of software.

- Is intended for personal or private financial gain.

In addition, should employees receive electronic communications that contain such information, they should not forward such messages on to others whether inside or outside the System.

Personal Use

Occasional use of the E-mail system for personal use is permitted with certain limitations. Personal E-mails should be kept in a separate folder with the user's Gmail account and stored for no longer than 1 week. Except in cases of emergency, users should refrain from sending and reviewing personal E-mails during work hours. The content of personal E-mails, whether being received or sent, must also conform to the standards listed above as prohibited, and other restrictions that may be found in the Scottsboro City Board of Education Employee Acceptable Use Policies. Users should immediately delete inappropriate E-mails and inform the sender about the restrictions on acceptable content.

Scottsboro City Schools E-mail addresses shall not be used for non-work related shopping, subscriptions, memberships. In addition, Scottsboro City Schools E-mail addresses should not be used on personal websites, blogs, social networking accounts, online forums, or any other electronic medium.

E-mail Filtering

Scottsboro City Schools attempts to block offensive messages and spam from entering our System; however, this process is not 100% effective. Employees should report offensive and spam messages by forwarding them to help@scottsboroschools.net or by contacting the Technology Department. Such messages should never be intentionally forwarded on to others whether inside or outside the Scottsboro City Schools E-mail directory.

Mass E-mails

E-mails intended for all employees in the Scottsboro City System must be approved by the Superintendent, his designee, or the Technology Coordinator prior to being sent.

Monitoring and Waiver of Privacy

Scottsboro City Schools is not obligated to monitor E-mail messages; however, authorized administrators of the Scottsboro City Schools may monitor messages without prior notice. Furthermore, electronic messages and files stored on Scottsboro City Schools computers or stored elsewhere using a Scottsboro City Schools E-mail or internet account are deemed to be the property of Scottsboro City Board of Education. Therefore, Scottsboro City Board of Education employees and others to which this Acknowledgement applies shall have no expectation of privacy in anything they store, send, or receive on the System's electronic communications systems such as the E-mail system. Employees and others to which this Acknowledgement applies waive any right of privacy they might have in anything they create, store, or receive on the System's computers or electronic communications systems.

Reporting of Violations and Enforcement

Scottsboro City Schools cannot guarantee that users will not occasionally receive offensive or inappropriate E-mails from outside the System or from fellow employees. Employees may report the matter to an immediate supervisor, the Technology Department, or to System administrators should they feel an incident warrants further investigation.

Any employee found to have willfully misused any form of electronic communications as outlined in this Acknowledgement and in the Employee Handbook may be subject to disciplinary action. These actions may include the suspension or loss of E-mail, web, blog, or other electronic communication privileges; or a verbal or written reprimand. A second violation of an employee may result in an adverse personnel action such as suspension or termination.

Disclaimers

In order to protect the System and the individual, all account holders shall use the disclaimer provided by the System on every E-mail sent. Individuals should be aware, however, that disclaimers do not offer any legal protection in the cases of defamation and libel. In addition, the presence of disclaimers may not entirely protect the sender from civil litigation or criminal prosecution.

Legal Actions

Should any legal actions, civil or criminal, take place which require the production of Scottsboro City Schools' employees E-mails or electronic files, the System may comply with properly executed legal requests to the extent possible. All legal consequences and associated penalties for civil or criminal violations, shall be the sole responsibility of the account holder and not that of the Scottsboro City Schools, unless otherwise found by a court of law.

Indemnification

Employees and others to which the Acknowledgement applies agree to indemnify Scottsboro City Schools for any losses, costs, or damages, including reasonable attorney fees, incurred by Scottsboro City Schools relating to, or arising out of, their violation of this Acknowledgement.

Modifications

Scottsboro City Schools may change the provisions of this Acknowledgement. Posting such modifications on the System's electronic communications system or sending such modifications by e-mail, fax, or U. S. Mail shall constitute proper notice of such modifications. However, no one, including principals or supervisors, may modify this policy in writing or verbally without the consent of the Superintendent.

Acknowledgement

I acknowledge that I have read and understand these risks and conditions, and in consideration of my use of the Scottsboro City Board of Education computers and/or electronic communications systems. I agree to comply with the terms stated herein. I understand that I can seek further training or explanation regarding the content of this document by contacting my Principal, Supervisor, or the Technology Department.

Exhibit D: Copier Machine Security Recommendations

July 2011

Many modern copy machines and multifunction printers record images of all information being copied, faxed, or scanned onto their hard drives. In the case of the Sharp multifunction machines, an image of every print job, fax, and copy ever made on the machine is retained on its hard drive. In our environment, these images could include FERPA- protected educational records, Social Security numbers, I.E.P.s, and other confidential information. Schools need to be aware that there have been instances where criminals have data-mining copy machine hard drives either disposed of in landfills or taken from previously leased machines.

School administrators should take measures to ensure that the hard drives on any copier or multifunction machine their school uses is properly erased or disposed of when the use of the machine is terminated.

Leases –

Ask the vendor what data protection options are available prior to signing a contract. Add an appropriate option to the contract and be sure to require a Letter of Certification once the machine is returned to the dealer.

Purchases -

Find out if the machine is equipped with data security technology already embedded into it and what this entails.

Enter a ticket for the Technology Department to remove and dispose of the copy machine hard drive prior to sending it to the local landfill or putting it out for auction.

Provisions for Consideration – Not Yet Implemented

Electronic Signature Agreement (Not Implemented)

[The following proposed agreement does not directly impact data security. But it could impact the outcome of challenges in cases where staff were asked to sign user agreements containing rules regarding data security electronically, but later protest that their digital signature was not valid.]

Scottsboro City Schools uses many types of electronic communications in order to conduct business. These include electronic mail, documents, applications, and forms. Digital formats enable the district to transmit information rapidly and to and retain records efficiently. Throughout your employment with Scottsboro City Schools you will have occasion to use these various methods to make and respond to requests, convey and receive information, and electronically ‘sign’ forms and agreements.

The Uniform Electronic Transactions Act (UETA) provides a legal framework for the use of electronic signatures and records in government or business transactions. UETA makes electronic records and signatures as legal as paper and manually signed signatures. This Act was adopted by Alabama in 2001 ([Ala. Code §8-1A-1 et seq.](#)) It defines an electronic signature as “an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.”

Scottsboro City Schools may use a variety of methods to verify your electronic ‘signature’ or identity. These include: 1) submitting a form while logged into the network or software application under a password protected account and 2) submitting your employee id or social security number within a form along with other personal information that uniquely identifies you. Therefore, you must keep your network and software login ids and passwords secure at all times.

Agreement

I agree to maintain the security of the UserID and password assigned to me by Scottsboro City Schools in order to prevent disclosure of this information to anyone.

I agree that, if I have any reason to believe that the security of my UserID and password has been compromised, I will immediately inform the _____.

I agree that I will be held legally bound, obligated, and responsible for any submission I make in electronic format to Scottsboro City Schools as I would be by making such submission in hardcopy form with my handwritten signature as certification.

I understand that if I decline to use an electronic ‘signature’ for any particular communication or form, that I may be required to submit that form in a hardcopy form with a handwritten signature; and that it is my responsibility to inform the appropriate person that I am taking this action.

I understand that if there is a hardcopy versions and an electronic version of the same exact document, that the one that is most recent will be considered the binding document and that the handwritten document alone may not override the electronic version.

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.

Restrictions on Parents Posting Images of Students (who are not their own children) to Social Media (Not Implemented)

From correspondence with a school in response to their question about a parent who wanted to post school pictures to Shutterfly.

With respect to pictures of students being posted online on sites that are not on our servers, we are trying to prohibit this for our staff and discouraging it for parents. The number of complaints we have been getting because a parent will take pictures of children who are not theirs and post them online has risen sharply in the last two years. For this reason we have tried to support our schools in discouraging parents from posting pictures of other children on the web. Coming to school is different than joining a little league team or some other voluntary activity. I don't think the classroom teacher or the school could give an individual the right to post pictures of his/her class online without having control of the site and ensuring that every other parent has agreed to this and has access. From our department's standpoint, we think all material posted online about school should be on our servers or a server such as Edmodo which we have control over and administrative access to.