Gadsden City Schools

DATA GOVERNANCE POLICY

Introduction

Protecting our students' and staffs' privacy is important and the Gadsden City Schools are committed to maintaining strong and meaningful privacy and security protections. The privacy and security of this information is a significant responsibility and we value the trust of our students, parents, and staff.

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

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

The Gadsden City School Data Governance Policy shall be a living document. To make the document flexible details are outlined in the Appendices. With the Board's permission, the Data Governance Committee may quickly modify information in the Appendices in response to changing needs. All modifications shall be posted on the Gadsden City Schools website.

Data Governance Committee

The Gadsden City Schools Data Governance committee consists of all current members of the District Technology Advisory Committee. The Advisory Committee annually consists of staff representatives from each school in the district, students, parents, community members, and district leaders.

Committee Meetings

The Data Governance committee shall meet at least annually. Additional meetings shall be called as needed. Some meetings may be conducted virtually or via e-mail.

Gadsden City Schools Data Governance Policy

I. PURPOSE

A. It is the policy of the Gadsden City Schools that data or information in all its forms--written, electronic, or printed--is protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment, software, and practices used to process, store, and transmit data or information.

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

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

II. SCOPE

The superintendent is authorized to establish, implement, and maintain data and information security measures. The policy, standards, processes, and procedures apply to all students and employees of the district, contractual third parties and agents of the district, and volunteers who have access to district data systems or data.

This policy applies to all forms of Gadsden City Schools' data and information, including but not limited to:

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

B. Hard copy data printed or written,

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

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

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

III. REGULATORY COMPLIANCE

The district will abide by any law, statutory, regulatory, or contractual obligations affecting its data systems. Gadsden City Schools complies with all applicable regulatory acts including but not limited to the following:

(See Appendix A)

A. Children's Internet Protection Act (CIPA)
B. Children's Online Privacy Protection Act (COPPA)
C. Family Educational Rights and Privacy Act (FERPA)
D. Health Insurance Portability and Accountability Act (HIPAA)
E. Protection of Pupil Rights Amendment (PPRA)

IV. SYSTEMS AND INFORMATION CONTROL

Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, AV equipment, server, internal or external storage, communication device or any other current or future electronic or technological device may be referred to as systems. All involved systems and information are assets of Gadsden City Schools shall be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

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

B. Software Installation and Use: All software packages that reside on technological systems within or used by Gadsden City Schools shall comply with applicable licensing agreements and restrictions.

C. Virus, Malware, Spyware, Phishing and SPAM Protection: Virus checking systems approved by the District Technology Department are deployed using a multi-layered approach (computers, servers, gateways, firewalls, filters, etc.) that helps to ensures that all electronic files are appropriately scanned for viruses, malware, spyware, phishing and SPAM. Users shall not turn off or disable Gadsden City Schools' protection systems.

D. Access Controls: Physical and electronic access to information systems that contain Personally Identifiable Information (PII), Confidential information, Internal information and computing resources is controlled. To ensure appropriate levels of access by internal workers, a variety of security measures are instituted as recommended by the data governance committee and approved by Gadsden City Schools. In particular, the data governance committee shall document roles and rights to the student information system and other like systems. Mechanisms to control access to PII, Confidential information, Internal information and computing resources include, but are not limited to, the following methods:

1. **Authorization:** Access shall be granted on a "need to know" basis and shall be authorized by the superintendent, principal, immediate supervisor, or Data Governance Committee with the assistance of the Technology Director. Specifically, on a case-by-case basis, permissions may be added in to those already held by individual users in the student management system, again on a need-to-know basis and only in order to fulfill specific job responsibilities, with approval of the Data Governance Committee.

2. **Identification/Authentication:** Unique user identification (user ID) and authentication are required for all systems that maintain or access PII, Confidential information, and/or Internal Information. Users shall be held accountable for all actions performed on the system with their User ID. User accounts and passwords shall NOT be shared.

3. **Data Integrity:** Gadsden City Schools provide safeguards so that PII, Confidential, and Internal Information is not altered or destroyed in an unauthorized manner. Core data are backed up to a private cloud for disaster recovery. (Note: E-mails are not archived.) In addition, listed below are methods that are used for data integrity in various circumstances:
    - transaction audit
    - disk redundancy (RAID)
    - data encryption

4. **Transmission Security:** Technical security mechanisms are in place to guard against unauthorized access to data that are transmitted over a communications network, including wireless networks. The following features are implemented:

    - integrity controls and
    - encryption, where deemed appropriate

    Note: Only GCS district email accounts shall be used for communications to and from school employees, to and from parents or other community members, to and from other educational agencies, to and from vendors or other associations, and to and from students for school business.

5. **Remote Access:** Access into Gadsden City Schools' network from outside is allowed using the GCS Portal. All other network access options are strictly prohibited without explicit authorization from the Technology Director or Data Governance Committee. Further, PII, Confidential Information and/or Internal Information that is stored or accessed remotely shall maintain the same level of protections as information stored and accessed within the Gadsden City Schools' network. PII shall only be stored in cloud storage if said storage has been approved by the Data Governance Committee or its designees.

6. **Physical and Electronic Access and Security:** Access to areas in which information processing is carried out shall be restricted to only appropriately authorized individuals. At a minimum, staff and network passwords shall be changed periodically.

    - No PII, Confidential and/or Internal Information shall be stored on a device itself such as a hard drive, mobile device of any kind, or external storage device that is not located within a secure area.
    - No technological systems that may contain information as defined above shall be disposed of or moved without adhering to appropriate Purchasing and Disposal of Electronic Equipment procedures.
    - It is the responsibility of the user to not leave these devices logged in, unattended, and open to unauthorized use.

E. Data Transfer/Exchange/Printing:

1. **Electronic Mass Data Transfers:** Downloading, uploading or transferring PII, Confidential Information, and Internal Information between systems shall be strictly controlled. Requests for mass download of, or individual requests for, information for research or any other purposes that include PII shall be in accordance with this policy and be approved by the data governance committee. All other mass downloads of information shall be approved by the committee and/or ISO and include only the minimum amount of information necessary to fulfill the request. A Memorandum of Agreement (MOA) shall be in place when transferring PII to external entities such as software or application vendors, textbook companies, testing companies, or any other web based application, etc. unless the exception is approved by the data governance committee.

2. **Other Electronic Data Transfers and Printing:** PII, Confidential Information, and Internal Information shall be stored in a manner inaccessible to unauthorized individuals. PII and Confidential Information shall not be downloaded, copied or printed indiscriminately or left unattended and open to compromise. PII that is downloaded for educational purposes where possible

shall be de-identified before use.

F. Oral Communications: Gadsden City Schools' staff shall be aware of their surroundings when discussing PII and Confidential Information. This includes but is not limited to the use of cellular telephones in public areas. Gadsden City Schools' staff shall not discuss PII or Confidential Information in public areas if the information can be overheard. Caution shall be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.

G. Audit Controls: Hardware, software, services and/or procedural mechanisms that record and examine activity in information systems that contain or use PII are reviewed by the Data Governance Committee periodically.

H. IT Disaster Recovery: Controls shall ensure that Gadsden City Schools can recover from damage to critical systems, data, or information within a reasonable period of time. Each school, department, or individual is required to report any instances immediately to the Superintendent and/or Technology Director for response to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages data or systems. The IT Disaster Plan shall include the following:

1. A prioritized list of critical services, data, and contacts.
2. A process enabling Gadsden City Schools to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.
3. A process enabling Gadsden City Schools to continue to operate in the event of fire, vandalism, natural disaster, or system failure.

VII. COMPLIANCE

A. The Data Governance Policy applies to all users of Gadsden City Schools' information including: employees, staff, students, volunteers, and outside affiliates. Failure to comply with this policy by employees, staff, volunteers, and outside affiliates may result in disciplinary action up to and including dismissal in accordance with applicable Gadsden City Schools' procedures, or, in the case of outside affiliates, termination of the affiliation. Failure to comply with this policy by students may constitute grounds for corrective action in accordance with Gadsden City Schools' policies. Further, penalties associated with state and federal laws may apply.

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

1. Unauthorized disclosure of PII or Confidential Information.
2. Unauthorized disclosure of a log-in code (User ID and password).
3. An attempt to obtain a log-in code or password that belongs to another person.
4. An attempt to use another person's log-in code or password.
5. Unauthorized use of an authorized password to invade student or employee privacy by examining records or information for which there has been no request for review.
6. Installation or use of unlicensed software on Gadsden City Schools' technological systems.
7. The intentional unauthorized altering, destruction, or disposal of Gadsden City Schools' information, data and/or systems. This includes the unauthorized removal from GCS of technological systems such as but not limited to laptops, internal or external storage, computers, servers, backups or other media, copiers, etc. that contain PII or confidential information.
8. An attempt to gain access to log-in codes for purposes other than for support by authorized technology staff, including the completion of fraudulent documentation to gain access.

Laws, Statutory, Regulatory, and Contractual Security Requirements

Appendix A

A. CIPA: The **Children's Internet Protection Act** was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program. Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies shall include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they shall provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyber bullying awareness and response.
For more information, see: http://www.fcc.gov/guides/childrens-internet-protection-act

B. COPPA: The **Children's Online Privacy Protection Act**, regulates operators of commercial websites or online services directed to children under 13 that collect or store information about children. Parental permission is required to gather certain information,
See www.coppa.org for details.

C. FERPA: The **Family Educational Rights and Privacy Act**, applies to all institutions that are recipients of federal aid administered by the Secretary of Education. This regulation protects student information and accords students specific rights with respect to their data.
For more information, see: http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

D. HIPAA: The **Health Insurance Portability and Accountability Act**, applies to organizations that transmit or store Protected Health Information (PII). It is a broad standard that was originally intended to combat waste, fraud, and abuse in health care delivery and health insurance, but is now used to measure and improve the security of health information as well.
For more information, see: http://www.hhs.gov/ocr/privacy/hipaa/understanding/
In general, schools are not bound by HIPAA guidelines

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

These include the right to the following:

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

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

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

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

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

Gadsden City Schools Technological Services and Systems

Memorandum of Agreement (MOA)
Appendix B

THIS MEMORANDUM OF AGREEMENT, executed and effective as of the ___ day of _____, 20__, by and between _____, a corporation organized and existing under the laws of _____ (the "Company"), and **GADSDEN CITY SCHOOLS (GCS)**, a public school system organized and existing under the laws of the state of Alabama (the "School Board"), recites and provides as follows.

Recitals

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

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

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

Agreement

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

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

The Company shall cause each officer, director, employee and other representative who shall have access to GCS Student Records during the term of the Agreement (collectively, the "Authorized Representatives") to maintain in strict confidence and trust all GCS Student Information. The Company shall take all reasonable steps to insure that no GCS Student information is disclosed to any person or entity except those who (a) are Authorized Representatives of the Company performing functions for GCS under the Agreement and have agreed to be bound by the terms of this Agreement; (b) are authorized representatives of GCS, or (c) are entitled to such GCS student information from the Company pursuant to federal and/or Alabama law. The Company shall use GCS student information, and shall take all reasonable steps necessary to ensure that its Authorized Representatives shall use such information, solely for purposes related to and in fulfillment of the performance by the Company of its obligations pursuant to the Agreement.

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

Other Security Requirements. The Company shall maintain all technologies, policies, procedures and practices necessary to secure and protect the confidentiality and integrity of GCS student information, including procedures to (a) establish user IDs and passwords as necessary to protect such information; (b) protect all such user passwords from detection and unauthorized use; (c) prevent hostile or unauthorized intrusion that could result in data corruption, or deny service; (d) prevent and detect computer viruses from spreading to disks, attachments to e-mail, downloaded files, and

documents generated by word processing and spreadsheet programs; (e) minimize system downtime; (f) notify GCS of planned system changes that may impact the security of GCS data; (g) return or destroy GCS data that exceed specified retention schedules; (h) notify GCS of any data storage outside the US; (i) in the event of system failure, enable immediate recovery of GCS information to the previous business day. The Company should guarantee that GCS data shall not be sold to, accessed by, or moved by third parties.

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

Disposition of GCS Data Upon Termination of Agreement

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

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

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

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

[COMPANY NAME]

By:_____
[Name]
[Title]

GADSDEN CITY SCHOOLS

By:_____
Ed Miller
Superintendent
Gadsden City Schools

Gadsden City Schools

STUDENT DATA CONFIDENTIALITY AGREEMENT

I acknowledge my responsibility to respect the confidentiality of student records and to act in a professional manner in the handling of student performance data. I will ensure that confidential data, including data on individual students, is not created, collected, stored, maintained, or disseminated in violation of state and federal laws.

Furthermore, I agree to the following guidelines regarding the appropriate use of student data collected by myself or made available to me from other school/system employees, iNow, SETS or any other file or application I have access to:

- I will comply with school district, state and federal confidentiality laws, including the state Data and Information Governance and Use Policy, the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g and 34 CFR Part 99; and, and the Gadsden City Schools Student Data Confidentiality Agreement.
- Student data shall only be accessed for students for whom I have a legitimate educational interest and shall be used for the sole purpose of improving student achievement.
- I understand that student specific data is never to be transmitted via e-mail or as an e-mail attachment unless the file is encrypted and/or password protected.
- I understand that it is illegal for a student to have access to another student's data. I shall not share any student's information from any source with another student.
- I shall securely log in and out of the programs that store student specific data. I shall not share any passwords. Any documents I create containing student specific data shall be stored securely within the District network or within a password protected environment. I shall not store student specific data on any personal computer and/or external devices that are not password protected. (external devices include but are not limited to USB/Thumb drives and external hard drives)
- Regardless of its format, I shall treat all information with respect for student privacy. I shall not leave student data in any form accessible or unattended, including information on a computer display.

By signing below, I acknowledge, understand and agree to accept all terms and conditions of the Gadsden City Schools Student Data Confidentiality Agreement.

_____
Employee Name (Printed)

_____ Date_____
Signature of Employee

Job Title_____ School_____

Resource 1: ALSDE State Monitoring Checklist

Data Governance

A. Data Governance and Use Policy

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