Clarke County Schools
Data Governance Policy
2015-2016

2015-2016
Committee Members

Superintendent – Larry Bagley
Information Security Officer – Jackie Newsom
Technology Coordinator – Ricky Prine
Federal Programs Director – Gwen Powell
Chief School Financial Officer – Carmen Rotch
CNP Director – Craig Hodge
Principal – Kathy Spidle
Counselor – Kathy Powell
Technology Teacher – Shan Higginbotham

Roles and Responsibilities

I. Job Descriptions

(A) Job descriptions for employees whose responsibilities include entering, maintaining, or deleting data shall contain provisions addressing the need for accuracy, timeliness, confidentiality, and completeness. This includes, but is not limited to: school registrars, counselors, special education staff, and CNP staff handling free and reduced lunch data.

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

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

II. Supervisory Responsibilities

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

(B) Supervisors should immediately report incidents where data quality does not meet standards to the Data Governance Committee.

Data Governance

Information in all its forms--written, recorded electronically or printed--shall be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection shall include an appropriate level of security over the equipment and software used to process, store, and transmit that information.

Clarke County School System will conduct training on its data governance policy and document that training.

The policy, standards, processes, and procedures apply to all students and employees of the system, contractual third parties and agents of the system who have access to district information systems or information.

This policy applies to all forms of information, including but not limited to:

- speech, spoken face to face, or communicated by phone or radio,
- hard copy data printed or written on paper,
- communications sent by post/courier, fax, electronic mail, text, chat or any form of social media, etc.,
- data stored and processed by servers, PC's, laptops, tablets, mobile devices, etc., stored on any type of removable media or cloud based services

The school system will abide by any law or statutory, regulatory, or contractual obligations affecting its information systems. Due consideration is given to, but not limited to, the following acts:

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

- **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.
- **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 it is now used to measure and improve the security of health information as well.
- **Payment Card Industry Data Security Standard (PCI DSS)** 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.pcisecuritystandards.org for more information.

The Superintendent or designee will administer periodic risk assessments to identify, quantify, and prioritize risks. Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities.

Personally Identifiable Information (PII): PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

User: The user is any person who has been authorized to read, enter, or update information. A user of information is expected to:

- Access information only in support of their authorized job responsibilities.
- Comply with Information Security Policies and Standards and with all controls established by the owner and custodian.
- Keep personal authentication devices (e.g. passwords, PINs, etc.) confidential.
- Report promptly the loss or misuse of Clarke County School System information.
- Initiate corrective actions when problems are identified.

Classification is used to promote proper controls for safeguarding the confidentiality of information. Regardless of classification the integrity and accuracy of all classifications of information must be protected. The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, report) must have the same classification regardless of format.

Unauthorized or improper disclosure, modification, or destruction of this information could violate state and federal laws, result in civil and criminal penalties, and cause serious damage to the Clarke County School System.

Confidential Information

- Confidential Information is very important and highly sensitive material that is not classified as PII. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access.

  Examples of Confidential Information may include: personnel information, key financial information, proprietary information of commercial research sponsors, system access passwords and information file encryption keys.

  Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for Clarke County Schools, its customers, or its business partners. Decisions about the provision of access to this information must always be cleared through the information owner.

Public Information

- Public Information has been specifically approved for public release by a designated authority within each entity of the Clarke County School System. Examples of Public Information may include marketing brochures and material posted to the Clarke County School System internet web pages.
- This information may be disclosed outside of the Clarke County School System.

COMPUTER AND INFORMATION CONTROL

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

- **Ownership of Software:** All computer software developed by Clarke County School System employees or contract personnel on behalf of Clarke County School System or licensed for Clarke County School System use is the property of Clarke County School System and must not be copied for use at home or any other location, unless otherwise specified by the license agreement.

- **Installed Software:** All software packages that reside on computers and networks within Clarke County School System must comply with applicable licensing agreements and restrictions and must comply with Clarke County School System acquisition of software policies.

- **Virus Protection:** Virus checking systems approved by the school system must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorized to turn off or disable virus checking systems.

- **Access Controls:** Physical and electronic access to information systems that contain PII, Confidential and Internal information and computing resources is controlled. To ensure appropriate levels of access by internal workers, security measures will be instituted by the school system. In particular, the Data Governance Committee shall document roles and rights to the student information system and other like systems.

Compliance

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

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

- Unauthorized disclosure of PII or Confidential Information as specified in Confidentiality Statement.
- Attempting to obtain a sign-on code or password that belongs to another person.
- Using or attempting to use another person's sign-on code or password.
- Unauthorized use of an authorized password to invade patient privacy by examining records or information for which there has been no request for review.
- Installing or using unlicensed software on Clarke County School System computers.
- The intentional unauthorized destruction of Clarke County School System information.
- Attempting to get access to sign-on codes for purposes other than official business, including completing fraudulent documentation to gain access.
- Unauthorized access to the Clarke County School System wireless or wired network.

Data Quality

A proactive approach to data governance requires establishing data quality standards and regularly monitoring and updating the data management strategies to ensure that the data are accurate, relevant, timely, and complete for the purposes they are intended to be used. To ensure high quality data, the following strategies are used to prevent, detect, and correct errors and misuses of data.

1. Data stewards or their designees review student information for accuracy as it is submitted by parents, students, and teachers. This includes grades submitted into the INOW portal.

2. Data stewards or their designees correct data immediately when errors are brought to their attention.

3. Data stewards or their designees allow access to only those individuals with a "need to know" status as determined by data stewards.

APPENDICES

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 Clarke County 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 my password. 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 Clarke County Schools Student Data Confidentiality Agreement.

_____ Date_____

Signature of Employee

Job Title_____ School_____

School Year:_____

NEW EMPLOYEE TECHNOLOGY INFORMATION

Legal Name: _____ Nickname: _____Middle Initial: __

Last Name: _____

Street Address: _____

City: _____ State: _____ Zip: _____

Last Four Digits of SS# _____ Date of Birth: _____

Home Phone: _____ Current Email Address: _____

Emergency Contact Information (Name and Number):_____

Grade/Subject/Position: _____School:_____

Would you like for the Clarke County School System to request a transfer of your STI PD professional development records? __If yes, in which school system were you employed? _____

I have received and am knowledgeable of the content in the revised Technology Usage Policy adopted by the Clarke County Board of Education in May, 2011, and completed the online training for the Data and Information Governance and Use Policy.

Name: _____ Date: _____

**Accounts are disabled on the last day of active employment or when on leave for more than 6 months.*

Temporary Guardianship Agreement

I, _____, of _____
(print your full name) (street)

_____, as the custodial parent of:
(city, state, zip)

List the full names of each child	List each child's birth date

Do hereby grant temporary guardianship of the above listed children to:

List the full names of the individual (s) to whom you are granting temporary custody	List each person's relationship to the child(ren)

Contact information of temporary guardians listed above:

Address: _____

Phone numbers: _____

Statement of Consent: (To be signed in the presence of a legalized notary public.)

I, _____, *hereby grant temporary guardianship of the above children, whom*

I have legal custody of to _____:

☐ From _____ to _____
(mm/dd/yyyy) (mm/dd/yyyy)

☐ For as long as necessary, beginning on _____
(mm/dd/yyyy)

In addition, in the event of an emergency or non-emergency situation requiring medical treatment, I hereby grant permission for any and all medical and/or dental attention to be administered to my child/children, in the event of an accidental injury or illness. This permission includes, but is not limited to, the administration of first aid, and the use of an ambulance, and the administration of anesthesia and/or surgery, under the recommendation of qualified medical personnel. I also grant permission for the guardian(s) named above to make educational decisions for my child/children.

Signature: _____ Date: _____

Signature: _____ Date: _____

Notarization:

On this _____day of _____, _____, _____
(date) *(month)* *(year)* *(name of parent)*
personally appeared before me in _____, _____and, in my presence,
(city) (state)
has/have satisfactorily identified him/her/themselves as the signer(s) of this Temporary Guardianship Form.

Affix Notary Seal Here

Name of Notary Official: _____

Signature: _____Commission Expires: _____