Russell County Schools

Data Governance Policy

TABLE OF CONTENTS

Introduction

Protecting our students' and staffs' privacy is an important priority and Russell County Schools is 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 Russell County Schools Data Governance document includes information regarding the Data Governance Committee, the actual Russell County 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 Russell County Schools' 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 Russell County Schools 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 will be posted on the Russell County Schools website.

2016-2017 Data Governance Committee

The Russell County Schools 2016-2017 Data Governance committee consists of Dr. Brenda Coley Superintendent; and Mr. Fabian Bauerschmidt Director of Technology, Mr. Kendrick Britford Security Officer, Debbie Webster Director of Curriculum, Dr. Mesha Patrick Director of Federal Funding, Dr. Vivian Relf Director of Special Education, Cody Patterson Chief Financial Officer. All members of the Russell County Schools Administrative Team will serve in an advisory capacity to the committee and will be called upon to attend meetings when the topic of the meeting requires his or her expertise.

Committee Meetings

The Data Governance committee will meet at a minimum two times per year. Additional meetings will be called as needed.

Russell County Schools Data Governance Policy

I. PURPOSE

A. It is the policy of Russell County 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. Russell County Schools conducts annual training on their data governance policy and documents that training.

D. 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 Russell County 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. Russell County Schools complies with all applicable regulatory acts including but not limited to the following:

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. Payment Card Industry Data Security Standard (PCI DSS)

F. Protection of Pupil Rights Amendment (PPRA)

See also Appendix A (Laws, Statutory, Regulatory, and Contractual Security Requirements.)

IV. RISK MANAGEMENT

A. A thorough risk analysis of all Russell County Schools' data networks, systems, policies, and procedures shall be conducted on an annual basis or as requested by the Superintendent, ISO, or Technology Director. The risk assessment shall be used as a basis for a plan to mitigate identified threats and risk to an acceptable level.
.

B. The Superintendent or designee administers periodic risk assessments to identify, quantify, and prioritize risks. Based on the periodic assessment, measures are implemented that mitigate the threats by reducing the amount and scope of the vulnerabilities.

**** See also Appendix B (Information Risk Management Practices)***
**** See also Appendix C (Definitions and Responsibilities***

V. Data Quality Controls

A. JOB DESCRIPTIONS

(1) 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.

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

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

B. SUPERVISORY RESPONSIBILITIES

(1) 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.

(2) 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.

VI. DATA CLASSIFICATION

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

**** See also Appendix D (Data Classification Levels)***

VII. 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 Russell County 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 Russell County Schools employees or contract personnel on behalf of Russell County Schools, licensed or purchased for Russell County Schools use is the property of Russell County 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 Russell County Schools shall comply with applicable licensing agreements and restrictions and shall comply with Russell County Schools' acquisition of software procedures.

****See also Appendix E (Acquisition of Software Procedures)***

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 ensures all electronic files are appropriately scanned for viruses, malware, spyware, phishing and SPAM. Users shall not to turn off or disable Russell County Schools' protection systems or to install other systems.

****See also Appendix F (Virus, Malware, Spyware, Phishing and SPAM Protection)***

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 Russell County 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 will 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 and/or Information Security Officer (ISO.) 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 will 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:** Russell County Schools provides 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. In addition, listed below are methods that are used for data integrity in various circumstances:

- transaction audit
- disk redundancy (RAID)
- ECC (Error Correcting Memory)
- checksums (file integrity)
- data encryption
- data wipes

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 RCS district-supported 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 Russell County Schools' network from outside is allowed using the RCS Portal. All other network access options are strictly prohibited without explicit authorization from the Technology Director, ISO, 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 Russell County 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.

    - 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 the 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.

See also Appendix G (Physical and Security Controls Procedures.)
See also Appendix I (Purchasing and Disposal Procedures.)
See also Appendix J (Data Access Roles and Permissions.)

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.

See also Appendix K (Russell County Schools Memorandum of Agreement.)

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: Russell County 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. Russell County 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 annually. Further, the committee also regularly reviews records of information system activity, such as audit logs, access reports, and security incident tracking reports. These reviews shall be documented and maintained for six (6) years.

H. Evaluation: Russell County Schools requires that periodic technical and non-technical evaluations of access controls, storage, and other systems be performed in response to environmental or operational changes affecting the security of electronic PII to ensure its continued protection.

I. IT Disaster Recovery: Controls shall ensure that Russell County Schools can recover from any 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, Risk Management Officer, Technology Director and/or ISO 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 Russell County Schools to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.
3. A process enabling Russell County Schools to continue to operate in the event of fire, vandalism, natural disaster, or system failure.
4. Procedures for periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary.

VII. COMPLIANCE

A. The Data Governance Policy applies to all users of Russell County 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 Russell County 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 Russell County 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 Russell County School technological systems.
7. The intentional unauthorized altering, destruction, or disposal of Russell County Schools' information, data and/or systems. This includes the unauthorized removal from RCS 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. PCI DSS: The **Payment Card Industry Data Security 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. For more information, see: www.pcisecuritystandards.org

F. 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.

Information Risk Management Practices

Appendix B

The analysis involved in Russell County Schools Risk Management Practices examines the types of threats – internal or external, natural or manmade, electronic and non-electronic – that affect the ability to manage and protect the information resource. The analysis also documents any existing vulnerabilities found within each entity, which potentially exposes the information resource to the threats. Finally, the analysis includes an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection.

From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information is determined and addressed based on recommendations by the Data Governance Committee. The frequency of the risk analysis is determined at the district level. It is the option of the superintendent or designee to conduct the analysis internally or externally.

Definitions and Responsibilities

Appendix C

Definitions

A. Availability: Data or information is accessible and usable upon demand by an authorized person.
B. Confidentiality: Data or information is not made available or disclosed to unauthorized persons or processes.
C. Data: Facts or information
D. Entity: Organization such as school system, school, department or in some cases business
E. Information: Knowledge that you get about something or someone; facts or details.
F. Data Integrity: Data or information has not been altered or destroyed in an unauthorized manner.
G. Involved Persons: Every user of Involved Systems (see below) at Russell County Schools – no matter what their status. This includes nurses, residents, students, employees, contractors, consultants, temporaries, volunteers, substitutes, student teachers, interns, etc.
H. Systems: All data-involved computer equipment/devices and network systems that are operated within or by the Russell County Schools physically or virtually. This includes all platforms (operating systems), all computer/device sizes (personal digital assistants, desktops, mainframes, telephones, laptops, tablets, game consoles, etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.
I. 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.
J. Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.

Responsibilities

A. Data Governance Committee: The Data Governance Committee for Russell County Schools is responsible for working with the Information Security Officer (ISO) to ensure security policies, procedures, and standards are in place and adhered to by the entity. Other responsibilities include:

1. Reviewing the Data Governance Policy annually and communicating changes in policy to all involved parties.
2. Educating data custodians and manage owners and users with comprehensive information about security controls affecting system users and application systems.

B. Information Security Officer: The Information Security Officer (ISO) for Russell County Schools is responsible for working with the superintendent, Data Governance Committee, user management, owners, data custodians, and users to develop and implement prudent security policies, procedures, and controls. Specific responsibilities include:

1. Providing basic security support for all systems and users.
2. Advising owners in the identification and classification of technology and data related resources. ***See also Appendix D (Data Classification Levels.)***
3. Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation.
4. Performing or overseeing security audits.
5. Reporting regularly to the superintendent and Russell County Schools Data Governance Committee on Russell County Schools’ status with regard to information security.

C. User Management: Russell County Schools' administrators are responsible for overseeing their staff use of information and systems, including:

1. Reviewing and approving all requests for their employees' access authorizations.
2. Initiating security change requests to keep employees' secure access current with their positions and job functions.
3. Promptly informing appropriate parties of employee terminations and transfers, in accordance with local entity termination procedures.
4. Revoking physical access to terminated employees, i.e., confiscating keys, changing combination locks, etc.
5. Providing employees with the opportunity for training needed to properly use the computer systems.
6. Reporting promptly to the ISO and the Data Governance Committee the loss or misuse of Russell County Schools' information.
7. Initiating corrective actions when problems are identified.
8. Following existing approval processes within their respective organization for the selection, budgeting, purchase, and implementation of any technology or data system/software to manage information.
9. Following all privacy and security policies and procedures.

D. Information Owner: The owner of a collection of information is usually the administrator or supervisor responsible for the creation of that information. In some cases, the owner may be the primary user of that information. In this context, ownership does not signify proprietary interest, and ownership may be shared. The owner may delegate ownership responsibilities to another individual by completing the Russell County Schools Information Owner Delegation/Transfer Request Form and submitting the form to the Data Governance Committee for approval. The owner of information has the responsibility for:

1. Knowing the information for which she/he is responsible.
2. Determining a data retention period for the information, relying on ALSDE guidelines, industry standards, Data Governance Committee guidelines, or advice from the school system attorney.
3. Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created.
4. Authorizing access and assigning data custodianship if applicable.
5. Specifying controls and communicating the control requirements to the data custodian and users of the information.
6. Reporting promptly to the ISO the loss or misuse of Russell County Schools' data.
7. Initiating corrective actions when problems are identified.
8. Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
9. Following existing approval processes within the respective organizational unit and district for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

E. Data Custodian: The data custodian is assigned by an administrator, data owner, or the ISO based his/her role and is generally responsible for the processing and storage of the information. The data custodian is responsible for the administration of controls as specified by the owner. Responsibilities may include:

1. Providing and/or recommending physical safeguards.
2. Providing and/or recommending procedural safeguards.
3. Administering access to information.

4. Releasing information as authorized by the Information Owner and/or the ISO and/or Data Governance Committee for use and disclosure using procedures that protect the privacy of the information.
5. Maintaining information security policies, procedures and standards as appropriate and in consultation with the ISO and/or Data Governance Committee.
6. Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
7. Reporting promptly to the ISO and/or Data Governance Committee the loss or misuse of Russell County Schools data.
8. Identifying and responding to security incidents and initiating appropriate actions when problems are identified.

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

1. Access information only in support of their authorized job responsibilities.
2. Comply with all data security procedures and guidelines in the Russell County Schools Data Governance Policy and all controls established by the data owner and/or data custodian.
3. Keep personal authentication devices (e.g. passwords, secure cards, PINs, access codes, etc.) confidential.
4. Report promptly to the ISO and/or Data Governance Committee the loss or misuse of Russell County Schools' information.
5. Follow corrective actions when problems are identified.

Data Classification Levels

Appendix D

A. Personally Identifiable Information (PII)

1. PII is information about an individual maintained by an agency, including:
   a. 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.
   b. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
2. 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 legal implications for Russell County Schools.

B. Confidential Information

1. 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 shall 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.
2. Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for Russell County Schools, its staff, parents, students including contract employees, or its business partners. Decisions about the provision of access to this information shall always be cleared through the information owner and/or Data Governance Committee.

C. Internal Information

1. Internal Information is intended for unrestricted use within Russell County Schools, and in some cases within affiliated organizations such as Russell County Schools’ business or community partners. This type of information is already widely-distributed within Russell County Schools, or it could be so distributed within the organization without advance permission from the information owner.
   Examples of Internal Information may include: personnel directories, internal policies and procedures, most internal electronic mail messages.
2. Any information not explicitly classified as PII, Confidential or Public will, by default, be classified as Internal Information.
3. Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.

D. Public Information

1. Public Information has been specifically approved for public release by a designated authority within each entity of Russell County Schools. Examples of Public Information may include marketing brochures and material posted to Russell County Schools’ web pages.
2. This information may be disclosed outside of Russell County Schools.

E. Directory Information

1. Russell County Schools defines Directory information as follows:
2. Student first and last name
3. Student gender
4. Student home address
5. Student home telephone number
6. Student school-assigned monitored and filtered email address

7. Student photograph
8. Student place and date of birth
9. Student dates of attendance (years)
10. Student grade level
11. Student diplomas, honors, awards received
12. Student participation in school activities or school sports
13. Student weight and height for members of school athletic teams
14. Student most recent institution/school attended
15. Student ID number
16. Student Home Room number

Acquisition of Software Procedures

Appendix E

The purpose of the Acquisition of Software Procedures is to:

- Ensure proper management of the legality of information systems,
- Allow all academic disciplines, administrative functions, and athletic activities the ability to utilize proper software tools,
- Minimize licensing costs,
- Increase data integration capability and efficiency of Russell County Schools (RCS) as a whole, and
- Minimize the malicious code that can be inadvertently downloaded.

A. Software Licensing:

1. All district software licenses owned by RCS will be:
   - kept on file at the central office,
   - accurate, up to date, and adequate, and
   - in compliance with all copyright laws and regulations
2. All other software licenses owned by departments or local schools will be:
   - kept on file with the department or local school technology office,
   - accurate, up to date, and adequate, and
   - in compliance with all copyright laws and regulations
3. Software installed on RCS technological systems and other electronic devices:
   - will have proper licensing on record,
   - will be properly licensed or removed from the system or device, and
   - will be the responsibility of each RCS employee purchasing and installing to ensure proper licensing
4. Purchased software accessed from and storing data in a cloud environment will have a Memorandum of Agreement (MOA) on file that states or confirms at a minimum that:
   - RCS student and/or staff data will not be shared, sold, or mined with or by a third party,
   - RCS student and/or staff data will not be stored on servers outside the US unless otherwise approved by Russell County Schools' Data Governance Committee,
   - the company will comply with RCS guidelines for data transfer or destruction when contractual agreement is terminated, and
   - No API will be implemented without full consent of RCS and the ALSDE.
5. Software with or without physical media (e.g. downloaded from the Internet, apps, or online) shall still be properly evaluated and licensed if necessary and is applicable to this procedure. It is the responsibility of staff to ensure that all electronic resources are age appropriate, FERPA compliant, and are in compliance with software agreements before requesting use. Staff members are responsible for ensuring that parents have given permission for staff to act as their agent when creating student accounts for online resources.

B. Supported Software:

In an attempt to prevent software containing malware, viruses, or other security risk, software is categorized as Supported and Not Supported Software. For software to be classified as Supported Software downloads and/or purchases shall be approved by the district technology director or designee such as a local school technology coordinator or member of the technical staff.

1. A list of supported software will be maintained on the RCS District Technology site.
2. It is the responsibility of the RCS Technology Team members to keep the list current and for staff to submit apps or other software to the Technology Team.
3. Unsupported software is considered New Software and shall be approved or it will not be allowed on RCS owned devices.

4. When staff recommends apps for the RCS Mobile Device Management Apps Catalog or software for installation, it is assumed that the staff has properly vetted the app or software and that it is instructional sound, is in line with curriculum or behavioral standards, and is age appropriate.
5. Software that accompanies adopted instructional materials will be vetted by the Curriculum and Instruction Director and the Technology Director and is therefore supported.

C. New Software:

In the Evaluate and Test Software Packages phase, the software will be evaluated against current standards and viability of implementation into the RCS technology environment and the functionality of the software for the specific discipline or service it will perform.

1. Evaluation may include but is not limited to the following:
   - Conducting beta testing.
   - Determining how the software will impact the RCS technology environment such as storage, bandwidth, etc.
   - Determining hardware requirements.
   - Determining what additional hardware is required to support a particular software package.
   - Outlining the license requirements/structure, number of licenses needed, and renewals.
2. Determining any Maintenance Agreements including cost.
   - Determining how the software is updated and maintained by the vendor.
   - Determining funding for the initial purchase and continued licenses and maintenance.
3. When staff recommends apps for the RCS Mobile Device Management Apps Catalog or software for purchase and/or testing, it is the responsibility of the appropriate staff to properly vet the app or software to ensure that is instructional sound, is in line with curriculum or behavioral standards, and is age appropriate.

Virus, Malware, Spyware, Phishing and SPAM Protection
Appendix F

Virus, Malware, and Spyware Protection
Russell County desktops, laptops, and fileservers run the Sophos Security Suite software. Virus definitions are updated every Day and an on access scan is performed on all "read" files continuously. A full scheduled scan runs every day at 7:00 p.m. or at the next time the computer/laptop is turned on. A full scheduled scan is performed on all fileservers daily at 7:00 p.m.

Internet Filtering
Student learning using online content and social collaboration continues to increase. Russell County Schools views Internet filtering as a way to balance safety with learning—letting good content, resources, and connections in while blocking the bad. To balance educational Internet resource and app use with student safety and network security, the Internet traffic from all devices that authenticate to the network is routed through the iBoss filter.

Phishing and SPAM Protection
In addition to the built in spam filtering for Google Gmail, email is filtered for viruses, phishing, spam, and spoofing using our Sophos Email Security appliance.

Security Patches
Windows security patches and other Windows patches are scheduled to "auto-download" and "Install."

Physical and Security Controls
Appendix G

The following physical and security controls shall be adhered to:

1. Network systems shall be installed in an access-controlled area. The area in and around the computer facility shall afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations.
2. Monitor and maintain data centers' temperature and humidity levels. The American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) recommends an inlet temperature range of 68 to 77 degrees and relative humidity of 40% to 55%.
3. File servers and/or storage containing PII, Confidential and/or Internal Information shall be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.
4. Computers and other systems shall be secured against use by unauthorized individuals. It is the responsibility of the user to not leave these devices logged in, unattended, and open to unauthorized use.
5. Ensure network systems and network equipment are properly secured to prevent unauthorized physical access and data is properly safeguarded to protect from loss. A record shall be maintained of all personnel who have authorized access.
6. Maintain a log of all visitors granted entry into secured areas or areas containing sensitive or confidential data (e.g., data storage facilities). Record the visitor's name, organization, and the name of the person granting access. Retain visitor logs for no less than 6 months. Ensure visitors are escorted by a person with authorized access to the secured area.
7. Monitor and control the delivery and removal of all asset-tagged and/or data-storing technological equipment or systems. Maintain a record of all such items entering or exiting their assigned location using the district approved technology inventory program. No technology equipment regardless of how purchased or funded shall be moved without the explicit approval of the technology department.
8. Ensure that technological equipment or systems being removed for transfer to another organization or being designated as surplus property is appropriately sanitized in accordance with applicable policies and procedures.

Purchasing and Disposal Procedures

Appendix I

This procedure is intended to provide for the proper purchasing and disposal of technological devices only. 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 in this document. For further clarification of the term technological systems contact the Russell County Schools' (RCS) district Technology Director.

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

A. Purchasing Guidelines

All systems that will be used in conjunction with Russell County Schools' technology resources or purchased, regardless of funding, shall be purchased from an approved list or be approved by a local school Technology Coordinator and/or the district Technology Director. Failure to have the purchase approved may result in lack of technical support, request for removal from premises, or denied access to other technology resources.

B. Alabama Competitive Bid Laws

All electronic equipment is subject to Alabama competitive bid laws. There are several purchasing coops that have been approved for use by the Alabama State Examiners office: http://www.examiners.state.al.us/purchcoop.aspx. Generally for technological devices and services, Russell County Schools purchase from the Alabama Joint Purchasing Agreement (ALJP): https://connect.alsde.edu/sites/eia/aljp/SitePages/ALJP%20(Alabama%20K-12%20(IT)%20Joint%20Purchasing)Home.aspx. In the event that a desired product is not included in one of these agreements, Russell County Schools bids the item or items using the district's competitive bid process. All technological systems, services, etc. over $15,000 purchased with public funds are subject to Alabama's competitive bid laws.

C. Disposal Guidelines

Equipment shall be considered for disposal for the following reasons:

1. End of useful life,
2. Lack of continued need,
3. Obsolescence,
4. Wear, damage, or deterioration,
5. Excessive cost of maintenance or repair.

D. Methods of Disposal

1. Discard Procedure

The Superintendent shall advise the board in the event that certain property is no longer needed for school purpose.

The Board upon receipt of such report may at its discretion declare that such property is no longer needed for school purpose.

3. Donation

All donations and/or sales shall be approved by the Finance Director and Technology Director.

Data Access Roles and Permissions

Appendix J

Russell County Schools maintain the following permission groups in INow:

1. Administrators
2. Adviser
3. Attendance Clerk
4. Census Clerk
5. Counselors
6. Data Entry
7. Discipline Clerk
8. District Personnel Admin
9. District Tech
10. Enrollment Clerk
11. Media Specialist
12. Nurse
13. RCHS Request manager
14. Register
15. Scheduling clerk
16. School personal Administrator
17. School Tech
18. SETS Staff
19. Teacher
20. Transcripts Clerk
21. Lead Teacher
22. Volunteer
23. Athletic Coach
24. PE Teachers
25. Section 504
26. Reports

***Complete list of Permissions available upon requests.**

Russell County Schools Technological Services and Systems
Memorandum of Agreement (MOA)
Appendix K

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 **RUSSELL COUNTY SCHOOLS (RCS)**, 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 RCS Student Records. The Company hereby agrees that it shall maintain, in strict confidence and trust, all RCS student records containing personally identifiable information (PII) hereafter referred to as "Student Information". Student information will 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 RCS Student Records during the term of the Agreement (collectively, the "Authorized Representatives") to maintain in strict confidence and trust all RCS Student Information. The Company shall take all reasonable steps to insure that no RCS Student information is disclosed to any person or entity except those who (a) are Authorized Representatives of the Company performing functions for RCS under the Agreement and have agreed to be bound by the terms of this Agreement; (b) are authorized representatives of RCS, or (c) are entitled to such RCS student information from the Company pursuant to federal and/or Alabama law. The Company shall use RCS 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 RCS 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 RCS 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 RCS 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 RCS of planned system changes that may impact the security of RCS data; (g) return or destroy RCS data that exceed specified

retention schedules; (h) notify RCS of any data storage outside the US; (i) in the event of system failure, enable immediate recovery of RCS information to the previous business day. The Company should guarantee that RCS data will 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 RCS 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 RCS student information compromised by the breach; (c) return compromised RCS data for review; (d) provide communications on the breach to be shared with affected parties and cooperate with RCS efforts to communicate to affected parties by providing RCS 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 RCS 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 RCS 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 RCS 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 RCS data of any kind, failure to follow security requirements and/or failure to safeguard RCS data. The Company's compliance with the standards of this provision is subject to verification by RCS 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 RCS 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 RCS student data and/or staff data. The Company hereby acknowledges and agrees that, solely for purposes of receiving access to RCS 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 RCS 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 RCS 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]

RUSSELL COUNTY SCHOOLS

By:_____

Superintendent
Russell County Schools

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	

Technology Responsible Use Employee Contract
Russell County Schools

All technology resource use will be governed by the requirement that it must add to the standards-based educational experience and growth of the user and not disrupt the educational process in any way.

The Responsible Use Policy outlines the guidelines and behaviors that users are expected to follow when using school technologies or when using personally-owned devices on the school campus.

- The RCSD's network is intended for educational purposes only.
- All activity over the network or using district technologies may be monitored and retained.
- Access to online content via the network may be restricted in accordance with our policies and federal regulations, such as the Children's Internet Protection Act (CIPA).
- Employees are expected to follow the same rules for good behavior and respectful conduct online and offline.
- Misuse of school resources can result in disciplinary action.
- Users of the district network or other technologies are expected to alert supervisors immediately of any concerns for safety or security.

Employees should keep personally-owned devices (including laptops, tablets, smartphones, and cell phones) turned off and put away during instructional hours—unless they are being used for educational purposes. Electronic communication devices and other digital devices are not allowed to be present in standardized testing situations based on State Department of Education Policy.

All employees shall maintain a professional relationship with students at all times, both inside and outside of school. No employee shall engage in inappropriate or unprofessional conduct, including specifically conduct of a sexual nature, with a student at any time. This includes a prohibition on any inappropriate communication, conduct or action performed in person, in writing, or conveyed electronically by telephone, cell phone, computer, or other communication device, including text messaging, instant messaging, and social networking. Employees should not "friend" or follow students on social media.

Although social media sites such as Facebook are generally personal in nature, they (along with personal texts and emails brought to the administration's attention) can be considered public discourse or public comments. Posting, texting, or emailing of comments or images about students, parents, employees, supervisors, departments, schools, the system or job that are of extremely poor taste, unprofessional, demeaning, derogatory, racist, offensive, insulting, inflammatory, hateful, insubordinate or celebrating immoral, improper or illegal actions is unacceptable and may lead to disciplinary action up to termination as those postings may cause a disruption in the workplace.

Any user who violates this policy may have computer/Internet privileges revoked at any time and without prior notice. Employee violations of this policy may also result in administrative leave, suspension, and possible termination. Any illegal use will also result in civil and/or criminal liability.

I have read and understood the full five-page text of the Technology Responsible Use Policy and agree to abide by it,

_____(Employee Printed Name)

_____(Employee Signature)

_____(Date)

Russell County Schools Responsible Use Student Contract

All technology resource use will be governed by the requirement that it must add to the standards-based educational experience and growth of the user and not disrupt the educational process in *any* way.

The Responsible Use Policy outlines the guidelines and behaviors that users are expected to follow when using school technologies or when using personally-owned devices on the school campus.

- The RCSD's network is intended for educational purposes only.
- All activity over the network or using district technologies may be monitored and retained.
- Access to online content via the network may be restricted in accordance with our policies and federal regulations, such as the Children's Internet Protection Act (CIPA).
- Students are expected to follow the same rules for good behavior and respectful conduct online and offline.
- Misuse of school resources can result in disciplinary action.
- Russell County Schools makes a reasonable effort to ensure students' safety and security online but will not be held accountable for any harm or damages that result from use of school technologies.
- Users of the district network or other technologies are expected to alert staff immediately of any concerns for safety or security.

Students will keep personally-owned devices (including laptops, tablets, smartphones, and cell phones) turned off and put away during school hours. They must be turned off and only in use with permission. Students will not be allowed to bring chargers to charge devices. Electronic communication devices and other digital devices will not be allowed to be present in standardized testing situations based on State Department of Education Policy. Neither the Russell County Board of Education nor local schools are responsible for lost, stolen, or damaged items.

<u>Examples of Acceptable Use</u>

- Use school technologies for school-related activities.
- Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- Treat school resources carefully and alert staff if there is a problem.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (images, messages, posts) online.
- Use school technologies at appropriate times, in approved places, for educational pursuits.
- Cite sources when using online sites and resources for research.
- Recognize that use of school technologies is a privilege and treat it as such.
- Be informed about online safety and be cautious to protect the safety of myself and others.
- Help to protect the security of school resources.

This is *not* intended to be an exhaustive list. Users should exercise good judgment when using school technologies.

<u>Examples of Unacceptable Use</u>

- Using school technologies in a way that could be personally or physically harmful.
- Attempting to find inappropriate images or content.
- Engaging in cyberbullying, harassment, or disrespectful conduct toward others.
- Trying to find ways to circumvent the school's safety measures and filtering tools.
- Using school technologies to send spam or chain mail.
- Plagiarizing content I find online.
- Posting personally-identifying information, about myself or others.
- Agreeing to meet someone I meet online in real life.
- Using language online that would be unacceptable in the classroom.
- Using school technologies for illegal activities or to pursue information on such activities.
- Attempting to hack or access sites, servers, or content that is not intended for its use.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Any user who violates this policy may have computer/Internet privileges revoked at any time and without prior notice. Student users are also subject to discipline according to the Russell County Student Code of Conduct. Any illegal use will also result in civil and/or criminal liability.

I have read and understood the Responsible Use Policy and agree to abide by it:

_____(Student Printed Name)

_____(Student Signature)

_____(Date)

I have read and understood the Responsible Use Policy with my child:

_____(Parent Printed Name)

_____(Parent Signature)

_____(Date)