



Birmingham City Schools

Believe. Create. Succeed.

Data Governance Policy

Presented to BCS Board of Education

TABLE OF CONTENTS

INTRODUCTION	3
DATA GOVERNANCE COMMITTEE	4
COMMITTEE MEETINGS	4
BIRMINGHAM CITY SCHOOLS DATA GOVERNANCE POLICY	5
I. 5	
II. 5	
III. 6	
IV. 6	
V. 7	
VI. 7	
VIII. COMPLIANCE	11
APPENDICES	13
APPENDIX A LAWS, STATUTORY, REGULATORY, AND CONTRACTUAL SECURITY REQUIREMENTS	14
APPENDIX B INFORMATION RISK MANAGEMENT PRACTICES	16
APPENDIX C DEFINITIONS AND RESPONSIBILITIES	17
APPENDIX D DATA CLASSIFICATION LEVELS	21
APPENDIX E ACQUISITION OF SOFTWARE PROCEDURES	23
APPENDIX F VIRUS, MALWARE, SPYWARE, PHISHING AND SPAM PROTECTION	26
APPENDIX G_BIRMINGHAM BOARD OF EDUCATION POLICY 4.9 – INTERNET SAFETY AND USE OF TECHNOLOGY	27
APPENDIX H_PHYSICAL AND SECURITY CONTROLS	29
APPENDIX I_PASSWORD CONTROL STANDARDS	30
APPENDIX J_PURCHASING AND DISPOSAL PROCEDURES	32
APPENDIX K_BIRMINGHAM CITY SCHOOLS TECHNOLOGICAL SERVICES AND SYSTEMS MEMORANDUM OF AGREEMENT (MOA)	36
RESOURCES	40
<i>Resource: ALSDE State Monitoring Checklist</i>	41
FORMS	42
STUDENT DATA CONFIDENTIALITY AGREEMENT	43
EMPLOYEE DATA CONFIDENTIALITY AGREEMENT	44

Introduction

Protecting student and employee privacy is an important priority and Birmingham 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 Birmingham City Schools Data Governance document includes information regarding the Data Governance Committee, the actual Birmingham 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 Birmingham City 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 Birmingham City 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 Birmingham City Schools website.

Data Governance Committee

The Birmingham City Schools Data Governance committee members are listed below.

Mrs. Melody Alston	Instructional Technology Resource Specialist
Mr. Jay Bradford	Director of Information Management Systems
Ms. Beverly Brown	Technology Coordinator, Parker High School
Dr. Sherene Carpenter	Coordinator of Attendance
Dr. Kecia Chapman	Coordinator of Testing, Research and Accountability
Dr. Dianne Coleman	Network Engineer
Mr. Vollie Cullen	Technology Foreman
Mr. Lovell Edwards	Network Systems Manager
Mr. Prothaniel Harris	Technology Integration Facilitator
Mr. Bernard Mitchell	Accountability Officer
Mrs. Afrika Parchman, Esq.	In-House Attorney
Dr. Joanne Stephens	Director of Information Technology
Dr. Mark Sullivan	Chief Academic Officer
Mr. Cedric Tatum	Principal, Hayes K-8 School
Dr. Teresa Thomas	Director of Student Information Systems
Mrs. Anita Watford	Technology Technician

Committee Meetings

The Data Governance committee will meet one time per month. Additional meetings will be called as needed.

Birmingham City Schools Data Governance Policy

I. PURPOSE

- A. It is the policy of Birmingham 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. Birmingham City 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 Birmingham 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.
- 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. Birmingham City 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 Birmingham City Schools' data networks, systems, policies, and procedures shall be conducted on an annual basis or as requested by the Superintendent, Accountability and Information Officer (AIO), 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 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)*

VI. 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 Birmingham 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 Birmingham City Schools employees or contract personnel on behalf of Birmingham City Schools, licensed or purchased for Birmingham City Schools use is the property of Birmingham 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 Birmingham City Schools shall comply with applicable licensing agreements and restrictions and shall comply with Birmingham City 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 turn off or disable Birmingham City 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 Birmingham 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 will be granted on a “need to Know” basis and shall be authorized by the Superintendent, appropriate director, principal, immediate supervisor, or Data Governance Committee with the assistance of the Technology Director and/or Accountability and Information Officer. Specifically, on a case - by-case basis, permissions may be added 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:** Birmingham City 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 control
 - encryption, where deemed appropriate

Note: Only BCS 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 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.

* *See also Appendix G: Birmingham Board of Education Policy 4.9*

5. **Remote Access:** Access into Birmingham City Schools' network from outside is allowed using the BCS Portal. All other network access options are strictly prohibited without explicit authorization from the Technology Director, AIO, 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 the same level of protections as information stored and accessed within the Birmingham 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. Cloud storage is located in Virtual (V) Cloud for Birmingham City Schools.
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 passwords shall be changed annually.
 - 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 H (Physical and Security Controls Procedures.)*

* *See also Appendix I (Password Control Standards.)*

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 AIO 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 (Birmingham City 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:** Birmingham 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. Birmingham 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 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:** Birmingham City 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 Birmingham City Schools can recover from any damage to critical systems, data, or information within a reasonable period of time. BCS Currently has configured its secondary data path to its disaster recovery site at West End Academy Elementary School. Each school, department, or individual is required to report any instances immediately to the Superintendent, Technology Director and/or AIO 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 Birmingham City Schools to restore any loss of data in the event of fire vandalism, natural disaster, or system failure.
 3. A process enabling Birmingham City 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 Birmingham 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 Birmingham 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 Birmingham 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 login code (User ID and password).
 3. An attempt to obtain a login code or password that belongs to another person.
 4. An attempt to use another person's login 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 Birmingham City Schools' technological systems.
7. The intentional unauthorized altering, destruction, or disposal of Birmingham City Schools' information, data and/or systems. This includes the unauthorized removal from BCS 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.

Appendices

Appendix A

Laws, Statutory, Regulatory, and Contractual Security Requirements

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 cyberbullying awareness and response.

For more information, see: <https://www.fcc.gov/consumers/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: <https://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 (PHI). It is a broad standard that was originally intended to combat waste, fraud, and abuse in health care delivery and health insurance, but is now used to measure and improve the security of health information as well.

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.

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 nonemergency, 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 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>

Appendix B

Information Risk Management Practices

The analysis involved in Birmingham City Schools Risk Management Practices examines the types of threats – internal or external, natural or manmade, electronic and nonelectronic – 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.

Appendix C

Definitions and Responsibilities

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 Birmingham City Schools – no matter what their status. This included nurses, residents, students, employees, contractors, consultants, temporary volunteers, substitutes, student teachers, interns, etc.
- H. **Systems:** All data-involved computer equipment/devices and network systems that are operated within or by the Birmingham City Schools physically or virtually. This included all platform (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.
- K. **VCloud:** Virtual Cloud

Responsibilities

- A. Data Governance Committee:** The Data Governance Committee for Birmingham City Schools is responsible for working with the Accountability and Information Officer (AIO) 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. Accountability and Information Officer:** The Accountability and Information Officer (AIO) for Birmingham City 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 Birmingham City Schools Data Governance Committee on Birmingham City Schools' status with regard to information security.
- C. User Management:** Birmingham City 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 AIO and the Data Governance Committee the loss or misuse of Birmingham City 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 Birmingham City 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 AIO the loss or misuse of Birmingham City Schools' data.
7. Initiating corrective actions when problems are identified.
8. Promoting employee education and awareness by utilizing programs approved by the AIO, 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 AIO 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 AIO 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 AIO and/or Data Governance Committee.
6. Promoting employee education and awareness by utilizing programs approved by the AIO, where appropriate.
7. Reporting promptly to the AIO and/or Data Governance Committee the loss or misuse of Birmingham City 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 Birmingham City 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 AIO and/or Data Governance Committee the loss or misuse of Birmingham City Schools' information.
5. Follow corrective actions when problems are identified.

Appendix D

Data Classification Levels

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 Birmingham City 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 Birmingham City 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 Birmingham City Schools, and in some cases within affiliated organizations such as Birmingham City Schools' business or community partners. This type of information is already widely-distributed within Birmingham City 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 Birmingham City Schools. Examples of Public Information may include marketing brochures and material posted to Birmingham City Schools' web pages.
2. This information may be disclosed outside of Birmingham City Schools.

E. Directory Information

Birmingham City Schools defines Directory information as follows:

1. Student first and last name
2. Student gender
3. Student home address
4. Student home telephone number
5. Student school-assigned monitored and filtered email address
6. Student photograph
7. Student place and date of birth
8. Student dates of attendance (years)
9. Student grade level
10. Student diplomas, honors, awards received
11. Student participation in school activities or school sports
12. Student weight and height for members of school athletic teams
13. Student most recent institution/school attended
14. Student ID number

Appendix E

Acquisition of Software Procedures

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 Birmingham City Schools (BCS) as a whole, and
- Minimize the malicious code that can be inadvertently downloaded.

A. Software Licensing:

1. All district software licenses owned by BCS 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 BCS 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 BCS 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:
 - BCS student and/or staff data will not be shared, sold, or mined with or by a third party,
 - BCS student and/or staff data will not be stored on servers outside the US unless otherwise approved by Birmingham City Schools' Data Governance Committee,
 - the company will comply with BCS guidelines for data transfer or destruction when contractual agreement is terminated, and

- No API will be implemented without full consent of BCS 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 BCS District Technology site.
2. It is the responsibility of the BCS 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 BCS owned devices.
4. When staff recommends apps for the BCS 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 Academic Officer 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 BCS 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 BCS 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. From this point forward, the BCS Data Governance Committee will evaluate recommended apps for the use of mobile technology and testing. It is the responsibility of the BCS Data Governance Committee to properly vet the app or software to ensure that is instructionally sound, is in line with curriculum or behavioral standards, and is age appropriate.

Appendix F

Virus, Malware, Spyware, Phishing and SPAM Protection

Virus, Malware, and Spyware Protection

Birmingham City desktops, laptops, and file servers run the Symantec endpoint.

Internet Filtering

Student learning using online content and social collaboration continues to increase. Birmingham City 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 resources 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 using the user’s network credentials. For companion devices and guest devices, users see a “pop-up screen” that requires them to login to the iBoss Internet filter with his/her network credentials or a guest login and password to gain access to the Internet. This process sets the filtering level appropriately based on the role of the user, such as, student, staff or guest, and more specifically for students, the grade level of the child. All sites that are known for malicious software, phishing, spyware, etc. are blocked.

Phishing and SPAM Protection

In addition to the built in spam filtering for Microsoft Exchange, email is filtered for viruses, phishing, spam, and spoofing using Fortinet.

Security Patches

Windows security patches and other Windows patches are scheduled to “auto-download” and “schedule install.” BCS updates are applied on Saturday and Sunday.

Appendix G

Birmingham Board of Education Policy 4.9 – Internet Safety and Use of Technology

- 4.9.1 Access to Technology Resources – The Board permits restricted and conditional access to and use of its technology resources, including but not limited to computers, the “Internet,” network storage areas, and electronic mail. Such access and use is restricted to employees, students, and other persons who are engaged in *bona fide* educational and administrative activities that serve and are consistent with identified educational objectives or authorized support functions, and who, by signing an “Acceptable Use Agreement,” agree to abide by all Board policies, rules, and regulations regarding technology use. The Acceptable Use Agreement will be developed by the Superintendent for approval by the Board.
- 4.9.2 Restriction or Loss of Technology Privileges – Persons who violate any Board policy, rule, or regulation regarding technology use may be denied use of the Board’s technology resources and may be subject to additional disciplinary action.
- 4.9.3 Ownership of Technology Resources and Data – All technology resources, including network and Internet resources, e-mail systems, and computers or other access devices owned, leased, or maintained by the Board are the sole property of the Board. Board personnel may, at any time and without prior notice, access, search, examine, inspect, collect, or retrieve information of any kind from the Board’s technology resources, including computer or related equipment, files, and data, to determine if a user is in violation of any of the Board’s policies, rules, and regulations regarding access to and use of technology resources, for or in connection with any other matter or reason related to the safe and efficient operation or administration of the school system, or for any other reason not prohibited by law. Users of school system technology resources have no personal right of privacy or confidentiality with respect to the use or content of such resources.
- 4.9.4 Adoption of Rules and Regulations – The Superintendent is authorized to develop for Board approval additional or more specific rules and regulations regarding access to and use of its technology resources and to require adherence to such rules and regulations through such means as the “Acceptable Use Agreement” and application of appropriate disciplinary policies and procedures. Such rules and regulations will address or provide:
- a. Measures to block or filter Internet access to pictures that are obscene, that constitute child pornography, or that are harmful to minors;
 - b. Restriction of access by minors to inappropriate material on the

Internet;

- c. The safety and security of minors when they are using electronic mail, chat rooms, and other forms of direct electronic communications;
- d. Prevention of “hacking” and other forms of unauthorized use of or access to computer or Internet files, sites, databases or equipment; and
- e. Unauthorized disclosure, use, and dissemination of personal information regarding minors;
- f. Restriction of minors’ access to harmful material; and
- g. Educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

4.9.5 Limitation on Liability – The Board makes no warranties of any kind, either express or implied, that the functions or the services provided by or through the Board’s technology resources will be error-free or without defect. The Board will not be responsible for any damage users may suffer, including but not limited to loss of data or interruption of service.

[Reference: 47 U.S.C. §254(h) and (l)]

Date Adopted 12/11/2012

Appendix H

Physical and Security Controls

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. Local School Main Distribution Frame (MDF) rooms and Intermediate Distribution Frame (IDF) rooms are secured by badge access and/or keys.
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.

****See also Appendix J (Purchasing and Disposal Procedures.)***

Appendix I

Password Control Standards

The Birmingham City Schools Data Governance and Use Policy require the use of strictly controlled passwords for network access and for access to secure sites and information. In addition, all users are assigned to Microsoft security groups that are managed through Microsoft Group Policies. The security groups include separate groups at each school for Office Staff, Tech Staff, Instructional Staff, Students, and Users.

Password Standards:

A. Users are responsible for complying with the following password standards for network access or access to secure information:

1. Passwords shall never be shared with another person, unless the person is a designated security manager.
2. Network passwords and Student Information System passwords for parents and students will be changed yearly if not more frequently.
3. Passwords shall, where possible, have a minimum length of eight (8) characters.
4. When possible, for secure sites and/or software applications, user created passwords should adhere to the same criteria as required for network access. This criteria is defined in the BCS Network Group Policy Criteria for Passwords and is listed below:
 - Shall not contain the user's account name or parts of the user's full name that exceed two consecutive characters.
 - Contain characters from three of the following four categories:
 - English uppercase characters (A through Z)
 - English lowercase characters (a through z)
 - Base 10 digits (0 through 9)
 - Non-alphabetic characters (for example, !, \$, #, %)
5. Passwords shall never be saved when prompted by any application with the exception of central single sign-on (SSO) systems as approved by the Technology Department. This feature shall be disabled in all applicable systems.
6. Passwords shall not be programmed into a PC or recorded anywhere that someone may find and use them.
7. When creating a password for secure information or sites, it is important not to use passwords that are easily guessed due to their association with the user (i.e.

children's names, pets' names, birthdays, etc.). A combination of alpha and numeric characters is more difficult to guess.

B. Where possible, system software should enforce the following password standards:

1. Passwords routed over a network shall be encrypted.
2. Passwords shall be entered in a non-display field.
3. System software shall enforce the changing of passwords and the minimum length.
4. System software shall disable the user password when more than five consecutive invalid passwords are given. Lockout time shall be set at a minimum of 30 minutes.
5. System software should maintain a history of previous passwords and prevent their being easily guessed due to their association with the user. A combination of alpha and numeric characters is more difficult to guess.

Appendix J

Purchasing and Disposal Procedures

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 Birmingham City Schools' (BCS) district Technology Director.

All involved systems and information are assets of Birmingham City 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 Birmingham City Schools' technology resources or purchased, regardless of funding, shall be purchased from an approved list or be approved by the BCS Data Governance Committee, AIO 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 Examiner's office. Refer also to the State ALJP website.

In the event that a desired product is not included in one of these agreements, Birmingham City 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. Inventory

All technological devices or systems over \$500 are inventoried by the Technology Department in accordance with the Birmingham City Schools' Finance Department using Nextgen. There are some exceptions under \$500, as determined by the Technology Director, such as but not limited to companion devices or peripherals that are inventoried. District inventory control personnel are responsible for ensuring that any network equipment, file servers, or district systems, etc. are inventoried.

D. 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.

The local school principal, Technology Director, and the Director of Finance shall approve school disposals by discard or donation. Written documentation in the form of a spreadsheet including but not limited to the

following shall be provided to the District Technology Office no later than Wednesday at 9:00 a.m. prior to the next Board of Education meeting on the following Monday:

1. Fixed asset tag (FAT) number,
2. Location,
3. Description,
4. Serial number, and
5. Original cost and account code if available.

E. Methods of Disposal

Once equipment has been designated and approved for disposal, it shall be handled according to one of the following methods. It is the responsibility of the Instructional Technology Department to modify the Nextgen to reflect any in-school transfers, in-district transfers, donations, or discards for technological systems. The district technology staff is responsible for modifying the inventory records to reflect any transfers within the central offices, transfers of central office electronic equipment to local schools, central office donations, or central office discards.

1. Transfer/Redistribution

If the equipment has not reached the end of its estimated life, an effort shall be made to redistribute the equipment to locations where it can be of use, first within an individual school or office, and then within the district. Service requests may be entered to have the equipment moved, reinstalled and, in the case of computers, laptops, or companion devices, have it wiped and reimaged or configured.

2. Discard

All electronic equipment in the Birmingham City Schools district shall be discarded in a manner consistent with applicable environmental regulations. Electronic equipment may contain hazardous materials such as mercury, lead, and hexavalent chromium. In addition, systems may contain Personally Identifiable Information (PII), Confidential, or Internal Information. Systems shall be wiped clean of this information prior to leaving the school district.

A district-approved vendor shall be contracted for the disposal of all technological systems/equipment. The vendor shall provide written documentation verifying the method used for disposal and a certificate stating that no data of any kind can be retrieved from the hard drive or any other component capable of storing data.

Under no circumstances should any technological systems/equipment be placed in the trash. Doing so may make Birmingham City Schools and/or the employee who disposed of the equipment liable for violating environmental regulations or laws.

4. Donation

If the equipment is in good working order, but no longer meets the requirements of the site where it is located, and cannot be put into use in another part of a school or system, it may be donated upon the written request of the receiving public school system's superintendent or non-profit organization's director. It shall be made clear to any school or organization receiving donated equipment that BCS is not agreeing to and is not required to support or repair any donated equipment. It is donated AS IS.

BCS staff should make every effort before offering donated equipment, to make sure that it is in good condition and can be re-used. Microsoft licenses or any other software licenses are not transferred outside the Birmingham City School system.

Donations are prohibited to individuals outside of the school system or to current faculty, staff, or students of Birmingham City Schools. The donation of or sale of portable technology-related equipment is permissible to retiring employees if the following criteria have been met:

- a. the portable equipment has been used solely by the retiring employee for over two years;
- b. the equipment will not be used by the employee assuming the

- responsibilities of the retiring employee; and
- c. the equipment has reached or exceeded its estimated life.

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

F. Required Documentation and Procedures

1. For purchases, transfers and redistributions, donations, and disposal of technology-related equipment, it is the responsibility of the BCS Inventory Control Personnel to create/update the inventory to include previous location, new school and/or room location, and to note the transfer or disposal information. When discarding equipment, the fixed asset tag is removed from the equipment and turned in with other documentation to the BCS Inventory Control Personnel. A spreadsheet export from Nextgen is sent to the district technology office. The Technology Director in turns submits to the CFO for approval and to the Superintendent's Office for Board approval.
2. When equipment is donated, a copy of the letter requesting the equipment shall be on-file with the district technology office prior to the donation. Equipment is donated in order of request.
3. Any disposed equipment shall be completely wiped of all data. This step will not only ensure that no confidential information is released, but also will ensure that no software licensing violations will inadvertently occur. For non-sensitive machines, all hard drives shall be fully wiped using a wiping program approved by the district technology office, followed by a manual scan of the drive to verify that zeros were written. Vendor disposed equipment will also be wiped by the vendor. A certificate of the wipe will be kept on file with BCS Inventory Control Personnel.
4. Any re-usable hardware that is not essential to the function of the equipment that can be used as spare parts shall be removed: special adapter cards, memory, hard drives, zip drives, CD drives, etc.
5. A district-approved vendor SHALL handle all disposals that are not redistributions, transfers, or donations. Equipment shall be stored in a central location prior to pick-up. Summary forms shall be turned into district technology office and approved by the Finance Director prior to the scheduled "pickup" day. Mice, keyboards, and other small peripherals may be boxed together and shall not be listed on summary forms.

Appendix K

Birmingham City Schools Technological Services and Systems Memorandum of Agreement (MOA)

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 BIRMINGHAM CITY SCHOOLS (BCS), 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 BCS Student Records. The Company hereby agrees that it shall maintain, in strict confidence and trust, all BCS 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 BCS Student Records during the term of the Agreement (collectively, the “Authorized Representatives”) to maintain in strict confidence and trust all BCS Student Information. The Company shall take all reasonable steps to insure that no BCS Student information is disclosed to any person or entity except those who (a) are Authorized Representatives of the Company performing functions for BCS under the Agreement and have agreed to be bound by the terms of this Agreement; (b) are authorized representatives of BCS, or (c) are entitled to such BCS student information from the Company pursuant to federal and/or Alabama law. The Company shall use BCS 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 BCS 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 BCS 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 BCS 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 BCS of planned system changes that may impact the security of BCS data; (g) return or destroy BCS data that exceed specified retention schedules; (h) notify BCS of any data storage outside the US; (i) in the event of system failure, enable immediate recovery of BCS information to the previous business day; (j) provide a protocol in the event of a security breach. The Company should guarantee that BCS 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 BCS immediately 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 BCS student

information compromised by the breach; (c) return compromised BCS data for review; (d) provide communications on the breach to be shared with affected parties and cooperate with BCS efforts to communicate to affected parties by providing BCS 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 BCS 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 BCS 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 BCS with notice immediately of notice or service on Company, whichever occurs first, of any lawsuits resulting from, or government investigations of, the Company's handling of BCS data of any kind, failure to follow security requirements and/or failure to safeguard BCS data. The Company's compliance with the standards of this provision is subject to verification by BCS 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 BCS 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 BCS student data and/or staff data. The Company hereby acknowledges and agrees that, solely for purposes of receiving access to BCS 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 BCS 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 BCS 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]

BIRMINGHAM CITY SCHOOLS

By: _____
Dr. Lisa Herring, Superintendent
Birmingham City Schools

[] Attachments included

Resources

Resource: ALSDE State Monitoring Checklist

(Desk Audit Only)					
	YES	NO	N/A	Indicators	Notes
1. Has a data governance committee been established and roles and responsibilities at various level specified?				<ul style="list-style-type: none"> ● 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?				<ul style="list-style-type: none"> ● Copy of the adopted data governance and use policy ● Dated minutes of meetings and agenda 	
3. Does the data governance policy address physical security?				<ul style="list-style-type: none"> ● Documented physical security measures 	
4. Does the data governance policy address controls and possible sanctions?				<ul style="list-style-type: none"> ● Current list of controls ● Employee policy with possible sanctions 	
5. Does the data governance policy address data quality?				<ul style="list-style-type: none"> ● Procedures to ensure that data are accurate, complete, timely, and relevant 	
6. Does the data governance policy address data exchange and reporting?				<ul style="list-style-type: none"> ● 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 accessible way to all stakeholders?				<ul style="list-style-type: none"> ● Documented methods of distribution to include who was contacted and how ● Professional development for all who have access to PII 	

Forms



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 the Birmingham City Schools Student Data Confidentiality Agreement.
- Student data will only be accessed for students for whom I have a legitimate educational interest and will 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 will not share any student's information from any source with another student.
- I will securely log in and out of the programs that store student specific data. I will not share my password. Any documents I create containing student specific data will be stored securely within the District network or within a password protected environment. I will 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 will treat all information with respect for student privacy. I will 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 Birmingham City Schools Student Data Confidentiality Agreement.

Signature of Employee

Date _____

Job Title _____

School _____



EMPLOYEE DATA CONFIDENTIALITY AGREEMENT

I acknowledge my responsibility to respect the confidentiality of employee records and to act in a professional manner in the handling of employee data. I will ensure that confidential data, including data on individual employees, 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 employee data collected by myself or made available to me from other school/system employees, NextGen, 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 and the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g and 34 CFR Part 99.
- Employee data will only be accessed for employees for whom I have a legitimate interest.
- I understand that employee specific data is never to be transmitted via e-mail or as an e-mail attachment unless the file is encrypted.
- I will securely log in and out of the programs that store employee specific data. I will not share my password. Any documents I create containing employee specific data will be stored securely within the District network or within a password protected environment. I will 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 will treat all information with respect for employee privacy. I will not leave employee 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 Birmingham City Schools Employee Data Confidentiality Agreement.

Signature of Employee

Date

Job Title _____

School _____