C-9

Mountain Brook Schools Data Governance Policy

I. PURPOSE

A. It is the policy of Mountain Brook 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, digital code, 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. Mountain Brook 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 Mountain Brook 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. Mountain Brook 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. Payment Card Industry Data Security Standard (PCI DSS)
E. 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 Mountain Brook 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 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

A. 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 Mountain Brook Schools and shall be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or code-based. All technological applications are considered "digital code" in this document. **Ownership of Digital Code:** All digital code developed by Mountain Brook Schools employees or contract personnel on behalf of Mountain Brook Schools and all digital code licensed or purchased for Mountain Brook Schools use is the property of Mountain Brook Schools and shall not be installed for use at home or any other location, unless otherwise specified by the license agreement.

B. Digital Code Installation and Use: All digital code that reside on technological systems within or used by Mountain Brook Schools shall comply with applicable licensing agreements and restrictions and shall comply with Mountain Brook Schools' acquisition of digital code procedures.

**See also Appendix E (Acquisition of Digital Code Procedures)*

C. **Virus, Malware, Spyware, Phishing, Ransomware, 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, ransomware, and SPAM. Users shall not delete or disable Mountain Brook Schools' protection systems or install other similar systems.

**See also Appendix F (Virus, Malware, Spyware, Phishing, Ransomware 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 Mountain Brook Schools. In particular, the data governance committee shall document roles and rights to the student information system and other like systems. Mechanisms to control access to PII, confidential information, internal information and computing resources include, but are not limited to, the following methods:

1. **Authorization:** Access shall be granted on a "need to know" basis and shall be requested by the superintendent, principal, or principal designee. Requests are reviewed and approved by the 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 shall be held accountable for all actions performed on the system with their user ID. User accounts and passwords shall NOT be shared.

3. **Data Integrity:** Mountain Brook 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 cloud service 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 MBS 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.
    See also Resource 3: Excerpts from Email Guidelines

5. **Remote Access:** Access into Mountain Brook Schools' network from outside is only allowed using authorized methods per the District Technology Department. 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 Mountain Brook Schools' network. PII shall only be stored in cloud storage if said storage has been approved by the Data Governance Committee or its designees.

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

    - No PII, confidential and/or internal information shall be stored on a device's internal storage, a mobile device of any kind, or an external storage device that is not located within a secure area.
    - No PII shall be stored in personal cloud storage.
    - 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 F (Physical and Security Controls Procedures.)
See also Appendix G (Password Control Standards.)
See also Appendix H (Purchasing and Disposal Procedures.)

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) or equivalent 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 I (Mountain Brook 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: Mountain Brook 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. Mountain Brook 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, digital code, 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: Mountain Brook 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 Mountain Brook 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 Mountain Brook Schools to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.

3. A process enabling Mountain Brook 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 Mountain Brook 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 Mountain Brook 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 Mountain Brook 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 digital code on Mountain Brook School technological systems.
7. The intentional unauthorized altering, destruction, or disposal of Mountain Brook Schools' information, data and/or systems. This includes the unauthorized removal from MBS 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.

Adopted: 10.20.14
Revised: 07.17.17

Laws, Statutory, Regulatory, and Contractual Security Requirements

Appendix 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 must include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

For more information, see: http://www.fcc.gov/guides/childrens-internet-protection-act

COPPA, the Children's Online Privacy Protection Act, regulates operators of commercial websites or online services directed to children under 13 that collect or store information about children. Parental permission is required to gather certain information;

See www.coppa.org for details.

FERPA, the Family Educational Rights and Privacy Act, applies to all institutions that are recipients of federal aid administered by the Secretary of Education. This regulation protects student information and accords students specific rights with respect to their data.

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

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.

Payment Card Industry Data Security Standard (PCI DSS) was created by a consortium of payment brands including American Express, Discover, MasterCard, and Visa. It covers the management of payment card data and is relevant for any organization that accepts credit card payments.
See www.pcisecuritystandards.org for more information.

PPRA, the Protection of Pupil Rights Amendment, affords parents and students who are 18 or emancipated minors ("eligible students") certain rights regarding our conduct of surveys, collection and use of information for marketing purposes, and certain physical exams.

These include the right to the following:

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

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

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

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

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

Information Risk Management Practices
Appendix B

The analysis involved in Mountain Brook 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 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. 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. **Customers:** Staff, parents, employees (including contract), and students are considered customers of the school district.
D. **Data:** Facts or information
E. **Digital Code:** Including but not limited to any program, software, application, extension, add-on, plug-in, etc.
F. **Information:** Knowledge that you get about something or someone; facts or details.
G. **Data Integrity:** Data or information has not been altered or destroyed in an unauthorized manner.
H. **Involved Persons:** Every user of Involved Systems (see below) at Mountain Brook Schools – no matter what their status. This includes nurses, residents, students, employees, contractors, consultants, temporaries, volunteers, substitutes, student teachers, interns, etc.
I. **Involved Systems:** All data-involved computer equipment/devices and network systems that are operated within the Mountain Brook Schools physical or virtual (cloud) environment. This includes all platforms (operating systems), all computer/device sizes (personal digital assistants, desktops, telephones, laptops, tablets, game consoles, etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.
J. **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.
K. **Risk:** The probability of a loss of confidentiality, integrity, or availability of information resources.

Responsibilities

A. **Data Governance Committee:** The Data Governance Committee for Mountain Brook Schools is responsible for working with the Information Security Officer to ensure security policies, procedures, and standards are in place and adhered to by entity. Other responsibilities include:
   1. Reviewing the Data Governance and Security Policy annually and communicating changes in policy to all involved parties.

2. Educating data custodian and user management with comprehensive information about security controls affecting system users and application systems.

B. **Information Security Officer:** The Information Security Officer (ISO) for Mountain Brook 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.)
   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 Mountain Brook Schools Data Governance Committee on Mountain Brook Schools' status with regard to information security.

C. **User Management:** Mountain Brook 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 the loss or misuse of Mountain Brook 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 Mountain Brook 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 Mountain Brook 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.

C. **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 Information Privacy/ Security Officer for use and disclosure using procedures that protect the privacy of the information.
6. Maintaining information security policies, procedures and standards as appropriate and in consultation with the ISO.
7. Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
8. Reporting promptly to the ISO the loss or misuse of Mountain Brook Schools data.
9. Identifying and responding to security incidents and initiating appropriate actions when problems are identified.

D. **User:** The user is any person who has been authorized to read, enter, 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 Mountain Brook Schools Data Governance and Use 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.
5. Report promptly to the ISO the loss or misuse of Mountain Brook Schools' information.
6. 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 Mountain Brook 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 must be restricted to those with a legitimate business need for access.
   Examples of Confidential Information may include: personnel information, key financial information, proprietary information of commercial research sponsors, system access passwords and information file encryption keys.
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 Mountain Brook Schools, its customers, or its business partners. Decisions about the provision of access to this information must always be cleared through the information owner and/or data governance committee.

C. Internal Information

1. Internal Information is intended for unrestricted use within Mountain Brook Schools, and in some cases within affiliated organizations such as Mountain Brook Schools' business or community partners. This type of information is already widely-distributed within Mountain Brook 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 Mountain Brook Schools. Examples

of Public Information may include marketing brochures and material posted to Mountain Brook Schools' internet web pages.

2. This information may be disclosed outside of Mountain Brook Schools.

E. Directory Information

Mountain Brook Schools defines Directory information as follows:

Student first and last name
Student gender
Student home address
Student home telephone number
Student school-assigned email address
Student photograph
Student place and date of birth
Student dates of attendance (years)
Student grade level
Student diplomas, honors, awards received
Student participation in school activities or school sports
Student weight and height for members of school athletic teams
Student most recent institution/school attended
Student ID number

Digital Code Acquisition Procedures
Appendix E

Introduction:

The purpose of the Acquisition of Digital Code 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 digital code including but not limited to software, applications, extensions, apps, and plug-ins,
- minimize licensing costs, and
- increase data integration capability and efficiency of Mountain Brook Schools (MBS) as a whole.

Licensing:

All district licenses for digital code owned by MBS will be:

- kept on file at the central office,
- accurate, up to date, and adequate, and
- in compliance with all copyright laws and regulations

All other licenses for digital code 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

Digital code installed on MBS computer 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 MBS employee purchasing and installing to ensure proper licensing

Purchased digital code accessed from and storing data in a cloud environment will have a Memorandum of Agreement (MOA) or equivalent assurances on file:

- that confirms that MBS student or staff data will not be stored on servers outside the US
- that the company will comply with MBS guidelines for data transfer or destruction when contractual agreement is terminated
- that no API will be implemented without full consent of MBS and the ALSDE.

Digital code with or without physical media (e.g. downloaded from the Internet, apps, extensions, apps or accessed online) must 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 all agreements before requesting use. Staff members are also responsible for ensuring that parents have given permission for staff to act as their agent when creating student accounts for online resources.

Supported Digital Code:

- For digital code to be supported all downloads and/or purchases must be approved by the district technology director or designee such as a local school technology coordinator or member of the technical staff.
- A list of supported online applications will be maintained on the MBS District Technology site.
- It is the responsibility of the MBS Technology Team members to keep the list current.
- Currently unsupported digital code is considered new and must be approved or it will not be allowed on MBS owned devices.
- Digital materials that accompanies adopted instructional materials will be vetted by the Curriculum and Instruction Director and the Technology Director and is therefore supported.

New Digital Code:

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

Evaluation may include but is not limited to the following:

- Conducting beta testing.
- Determining how the code will impact the MBS technology environment such as storage, bandwidth, etc.
- Determining digital device requirements.
- Determining what additional devices or components would be required to support a particular digital code package.
- Outlining the license requirements/structure, number of licenses needed, and renewals.
  Determining any Maintenance Agreements including cost.
- Determining how the code is updated and maintained by the vendor.
- Developing a plan for training.

Determining funding for the initial purchase and continued licenses and maintenance.

Physical and Security Controls
Appendix F

The following physical and security controls must be adhered to:

1. Network systems must be installed in an access-controlled area. The area in and around the facility must afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations.
2. File servers and/or storage containing PII, confidential and/or internal information must be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.
3. Computers and other systems must 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.
4. 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.
5. 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.
6. 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%.
7. Monitor and control the delivery and removal of all asset-tagged and/or data-storing IT equipment. 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 should be moved without the explicit approval of the technology department.
8. Ensure that equipment being removed for transfer to another organization or being designated as surplus property is appropriately sanitized in accordance with applicable policies and procedures.

Password Control Standards

Appendix G

The Mountain Brook Schools Data Governance and Use Policy requires the use of strictly controlled passwords for network access and for access to secure sites and information. Listed below are the minimum standards that must be implemented in order to ensure the effectiveness of password controls.

Standards:

1. Users are responsible for complying with the following password standards for network access or access to secure information:
2. Passwords must never be shared with another person, unless the person is a designated security manager.
3. Every password must, where possible, be changed yearly if not more frequently.
4. Passwords must, where possible, have a minimum length of six characters.
5. 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 MBS Network Group Policy Criteria for Passwords and is listed below:
   - Should 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, !, $, #, %)
6. Passwords must 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 should be disabled in all applicable systems.
7. Passwords must not be programmed into a PC or recorded anywhere that someone may find and use them.
8. When creating a password for secure information or sites, it is important not to use 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.

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

1. Passwords routed over a network must be encrypted.
2. Passwords must be entered in a non-display field.
3. System applications must enforce the changing of passwords and the minimum length.
4. System applications must disable the user password when more than five consecutive invalid passwords are given. Lockout time must be set at a minimum of 30 minutes.
5. System applications should maintain a history of previous passwords and prevent their reuse.

Purchasing and Disposal Procedures
Appendix H

This procedure is intended to provide for the proper purchasing and disposal of technology-related electronic equipment (including but not limited to computers, laptops, televisions, monitors, Chromebooks, iPhones, printers, fax machines, copiers, cell phones, data projectors and bulbs, copiers, sound systems, document cameras, related cords and battery packs, related parts, etc.) hereafter referred to as electronic equipment. For further clarification of the term "technology-related electronic equipment," contact the Mountain Brook Schools' (MBS) district Technology Director.

Purchasing Guidelines

All electronic equipment is used in conjunction with Mountain Brook Schools' technology resources or is purchased, regardless of funding, should be purchased from an approved list of equipment 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 or denied access to other technology resources.

Alabama Bid Law

Section 41-16-20 of the Code of Alabama, Public Contracts, (as amended by Act 94-207) states that "All contracts of whatever nature for labor, services, work, or for the purchase or lease of materials, equipment, supplies or other personal property, involving fifteen thousand ($15,000.00) or more, made by or on behalf of any state department, board, bureau, commission, committee, institution, corporation, authority, or office shall, except as otherwise provided in this article, be let by free and open competitive bidding, on sealed bids, to the lowest responsible bidder."

On items that must be bid, full specifications and names of vendors who can furnish the items should be provided to the Purchasing Department in electronic format. At least two weeks is usually allowed from the day requests for quotations are mailed until the day of opening bids.

The bid process is not limited to items over $15,000.00. Purchasing will solicit formal responses for any items, regardless of price, for which competitive bidding might lower the costs.

Items available from only one vendor/manufacturer may be approved as sole source after a review by the Purchasing Agent. To facilitate this review, a detailed statement, written and signed by the user and attested to by the Department Head, must accompany the requisition.

As a general rule, the Mountain Brook School district uses the Alabama K-12 Joint Purchasing Agreement or the

Inventory Guidelines

All electronic equipment over $500 should be inventoried in accordance with the inventory guidelines. It is the responsibility of the local school Technology Coordinator to ensure that technology-related equipment used in the local school is inventoried and/or check-out if the item leaves campus. The district technology staff is responsible for ensuring that any network equipment, fileservers, or district computers, printers, etc. are inventoried. All technology related inventory is audited each summer. Any equipment not accounted for will be considered lost or stolen.

Disposal Guidelines

Equipment should be considered for disposal for the following reasons:

- end of useful life,
- lack of continued need,
- obsolescence,
- wear, damage, or deterioration,
- excessive cost of maintenance or repair.

The local school principal, Technology Director, and the Director of Finance must approve school disposals by discard or donation. Typed documentation must be provided to the district Technology Office including the following information and using the appropriate format:

- fixed asset number,
- description,
- location,
- serial number,
- purchase date, and
- purchase cost.

The Technology Director will review and forward to the appropriate staff to present to the Board of Education for approval.

Methods of Disposal

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

Transfer/Redistribution

If the equipment has not reached the end of its estimated life, an effort should 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 and reinstalled and, in the case of computer equipment, to have it re-imaged and re-installed.

Discard

All electronic equipment in the Mountain Brook Schools district must be discarded in a manner consistent with applicable environmental regulations. Electronic equipment may contain hazardous materials such as mercury, lead, and hexavalent chromium.

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

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

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 should be made clear to any school or organization receiving donated equipment that MBS is not agreeing to and is not required to support or repair any donated equipment. It is donated AS IS.

MBS 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 are not transferable outside the Mountain Brook School system.

Donations are prohibited to <u>individuals</u> outside of the school system or to current faculty, staff, or students of Mountain Brook 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 exceed its estimated life. All donations and/or sales must be approved by the Finance Director and Technology Director.

Required Documentation and Procedures

For purchases, transfers and redistributions, donations, and disposal of technology-related equipment, it is the responsibility of the appropriate technology team member to create/update the inventory record to include previous location, new school and/or room location, and to check the appropriate boxes for transfer or disposal information. When discarding equipment, remove the fixed asset tag from the equipment and attach it to the fixed asset form. Copies of the forms should be sent to the local school bookkeeper or designated district level bookkeeper and a spreadsheet sent to the district technology office including all relevant information.

When equipment is donated, a copy of the letter requesting the equipment should be on-file with the district technology office prior to the donation.

Any equipment that is being donated should 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 should 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.

Remove any re-usable hardware that is not essential to the function of the equipment that can be used as spare parts. A district-approved vendor MUST handle all disposals that are not redistributions, transfers, or donations. Equipment should be stored in a central location prior to pick-up. Summary forms must be turned into district technology office and approved by the Finance Director prior to the scheduled "pick up" day. Mice, keyboards, and other small peripherals may be boxed together and should not be listed on summary forms.

Mountain Brook Schools Technological Services and Systems Memorandum of Agreement (MOA)
Appendix I

THIS MEMORANDUM OF AGREEMENT, executed and effective as of the _____, by and between _____, a corporation organized and existing under the laws of _____ (the "Company"), and **MOUNTAIN BROOK SCHOOLS (MBS)**, 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 MBS Student Records. The Company hereby agrees that it shall maintain, in strict confidence and trust, all MBS 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 MBS Student Records during the term of the Agreement (collectively, the "Authorized Representatives") to maintain in strict confidence and trust all MBS Student Information. The Company shall take all reasonable steps to insure that no MBS Student information is disclosed to any person or entity except those who (a) are Authorized Representatives of the Company performing functions for MBS under the Agreement and have agreed to be bound by the terms of this Agreement; (b) are authorized representatives of MBS, or (c) are entitled to such MBS student information from the Company pursuant to federal and/or Alabama law. The Company shall use MBS 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 MBS 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 MBS 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 MBS 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 MBS of planned system changes that may impact the security of MBS data; (g) return or destroy MBS data that exceed specified retention schedules; (h) notify MBS of any data storage outside the US; (i) in the event of system failure, enable immediate recovery of MBS information to the previous business day. The Company should guarantee that MBS 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 MBS 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 MBS student information compromised by the breach; (c) return compromised MBS data for review; (d) provide communications on the breach to be shared with affected parties and cooperate with MBS efforts to communicate to affected parties by providing MBS 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 MBS 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 MBS 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 MBS 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 MBS data of any kind, failure to follow security requirements and/or failure to safeguard MBS data. The Company's compliance with the standards of this provision is subject to verification by MBS 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 MBS 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 MBS student data and/or staff data. The Company hereby acknowledges and agrees that, solely for purposes of receiving access to MBS 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 MBS 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 MBS 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]

MOUNTAIN BROOK SCHOOLS

By: _____
Richard (Dicky) Barlow
Superintendent
Mountain Brook Schools

*_____signed the Student Privacy Pledge. (https://studentprivacypledge.org)