



Mountain Brook Schools Responsible Use Policy

J-43

Technology Usage ~~Policy~~ Policy

Purpose	2
Policy Statement	2
Introduction	2
I. Access	3
II. Privacy	3
III. Data Security	4
IV. Copyright	4
V. Email	5
VI. Internet Use	6
VII. Web Publishing	
VIII. Social Media	6
IX. Examples of Inappropriate Use of Resources	7

Guidelines

**Mountain Brook Schools
Email, Text Messaging, and Social Networking Guidelines**

**Mountain Brook Schools
Web Page and Web Publishing Guidelines**

Joani

**Mountain Brook Schools
Copyright Guidelines**

**Mountain Brook Schools
Electronics Purchasing and Disposal Guidelines**

Use of student video and photos, see existing document.

Emerging technologies: Wearable, voice, health and location monitoring

Guidelines about online data collection (Donna)



POLICY J-43 Technology Responsible Use Policy

PURPOSE:

The purpose of the Mountain Brook Schools is to provide an effective, challenging, and engaging education for every one of our students

POLICY STATEMENT:

The primary goal of the Mountain Brook Schools' technology environment is to support the educational and operational endeavors of both student and *employees of Mountain Brook Schools' using technology resources both on and off campus. Use of any and all Mountain Brook Schools technology resources is a by "any user" is privilege and not a right. Failure to comply with this policy may result in termination of said privilege.

** Qualifying contract workers, substitutes, and part-time workers doing work for or on behalf of the school system are referred to as "Employees" in this document for simplicity sake.*

INTRODUCTION:

To ensure that our students receive a quality education and that employees are able to work in a professional and intellectually stimulating environment, it is the policy of the Mountain Brook school district to provide all students and employees with access to a variety of technology resources. **All users of Mountain Brook Schools' technology resources must acknowledge and adhere to this policy.**

The creation of a large and varied technology environment demands that technology usage be conducted in legally and ethically appropriate and responsible ways, consistent with the Purpose Statement and instructional goals of the Mountain Brook school district. We recognize that the use of technology always requires attempts to balance the benefits against the possibilities of danger, security problems, and abuse. Rapid changes in technology and growth in the range of content available makes this a constant challenge.

Thus, it is the intention of the Mountain Brook Schools that all technology resources be used in accordance with any and all school system policies and procedures as well as local, state, and federal laws and/or guidelines governing the responsible use of technology and its component parts. Additionally, it is implied that all students and adult users of Mountain Brook Schools will use the provided technology resources so as not to waste them, abuse them, interfere with or cause harm to other individuals, institutions, or companies. The administrators of each school are responsible for establishing specific practices to enforce this policy at individual schools.

Aspects of this policy may specifically address technology equipment, personally owned by the user that is brought into school facilities or onto school campuses to access school or personal resources. All personal technologies used on any Mountain Brook campus are subject to this policy and may be used only if such use is in compliance with all school system policies, procedures, and guidelines as well as local, state, and federal laws. No technologies may be purchased, brought on campus, downloaded, installed, or used to access school system resources that interfere with or adversely affect functions or operations of school system technology resources/infrastructure.

All electronic content stored on any external storage medium or personal off-site storage location that is brought to or accessed from a Mountain Brook Schools campus is subject to all school system policies and guidelines, as well as local, state, and federal laws.

Employees are prohibited from downloading/exporting, sharing or communicating personally identifiable data outside the school system. Employees are prohibited from storing or saving personally identifiable information on external storage devices or portable devices that do not remain on campus. This information includes, but is not limited to data containing social security numbers, information protected by FERPA, and any other sensitive and/or protected information. In the event that this type of information is stored on a portable or external device and said device is lost or stolen or if the security of this data is believed to have been breached in any way, the Technology Director should be notified immediately.

Any questions about this policy, its interpretation, or specific circumstances shall be directed to the Technology Director before proceeding. Violations of this policy will be handled in a manner consistent with comparable situations requiring disciplinary and/or legal action.

The Mountain Brook Schools Technology department issues further specific guidelines detailing appropriate and legal use of copyright, email, technology resource purchasing and disposal, web page creation and maintenance, and the publication of student work. These guidelines are updated as best practices dictate and as case law emerges. These guidelines are considered appendices of the Mountain Brook Schools Technology Responsible Use Policy. Students and employees are expected to be aware of and follow the guidelines which are updated annually and posted on the Mountain Brook web site's Technology page and referenced in the Employee Handbook and/or the Student Code of Conduct.

I. ACCESS:

- A. The use of all Mountain Brook Schools technology resources is a privilege, not a right, and inappropriate or suspected inappropriate use will result in a cancellation of those privileges, pending investigation. Moreover, users of Mountain Brook Schools' technology must be aware that Mountain Brook Schools cannot assume any liability arising out of the illegal or inappropriate use of technology resources.
- B. Mountain Brook Schools' network may not be used for political activity, personal gain, commercial purposes, or profit.
- C. Users should not purchase or dispose of software applications or code, hardware, peripherals, or other technology-related devices without consulting the technology director or his/her designee. Regardless of purchase date, location or funding source, all personnel should adhere to the *Electronics Purchasing and Disposal Guidelines* in regard to all purchases and disposals.
- D. Individuals may use only accounts, files, applications, and/or other technology resources that are assigned to, provided, or approved for him/her. Any applications (Apps) used for or with students, should follow the approved App vetting process.
- E. Individuals identified as a real or suspected security risk will be denied access.
- F. Any use of technology resources, regardless of ownership, that reduces the efficiency of use for others will be considered a violation of this policy.
- G. Individuals must not attempt to disrupt any technology services or data integrity by engaging in inappropriate activities. Examples include, but are not limited to, spreading viruses, spamming, excessive network and/or Internet activity, or modification of equipment or infrastructure.
- H. Individuals must not attempt to modify technology resources, utilities, and configurations, and/or change the restrictions associated with his/her accounts, or attempt to breach any technology resources security system or filtering systems, either with or without malicious intent.
- I.. Personal technology-related devices used on school grounds are subject to all items covered in this policy and other applicable published guidelines. The permission for personal, portable devices to be brought to school, and the use of such devices, will be at the discretion of the local school administration. Only portable devices will be considered. The user should not access local area network or wide area network resources that require authentication without following the guidelines of the technology department. Public Internet access is available for visiting devices and is subject to the

conditions outlined in this policy and all other school system policies and guidelines, as well as local, state, and federal laws.

- J. With reasonable cause, the Technology Director may deny, revoke, or suspend specific user accounts without notice.

II. PRIVACY:

- A. To maintain network integrity and to ensure that the network is being used responsibly, if any policy violation or inappropriate behavior is suspected, the Technology Director, local school Technology Coordinators, other designated technology staff and/or school or district administrator reserve the right to inspect any and all data, including data stored by individual users on individual school or personal devices. Users should be aware that activities may be monitored at any time, without notice.
- B. Users should not have any expectation that their use of technology resources, including files stored by them on the Mountain Brook Schools' network, will be private and will be secure from access by others. Reasonable steps will be taken to maintain the security of technology resources, but no assurance can be given that penetration of such security will not occur.
- C. Relevant applications and/or storage of personal devices are subject to search by school officials when reasonable suspicion is determined.
- D. The collection of personally identifiable information, (PII) can only be used for the purpose for which it is intended.
- E. Because communications on the Internet are public in nature, all users should be careful to maintain appropriate and responsible communications.
- F. Mountain Brook Schools cannot guarantee the privacy, security, or confidentiality of any information sent or received, either via the Internet, an email facility, telephone, or otherwise.
- G. Users are encouraged to avoid storing personal and/or private information on the district and/or schools technology resources.

III. DATA SECURITY:

- A. Students and staff are expected to follow all local, state and federal laws and system policy regarding the protection of student and staff confidential data.
- B. Users should not have any expectation that their usage of such resources is private. Reasonable efforts will be taken to maintain the security of technology resources, but Mountain Brook Schools cannot ensure that such security will not be penetrated or breached and cannot assume any liability arising out of any such penetration or breach of security.
- C. Individuals must take all reasonable precautions to prevent unauthorized access to accounts and data and any other unauthorized usage within and outside of the Mountain Brook Schools. Any such unauthorized usage shall be reported immediately to the local school Technology Coordinator and/or the district Technology Director.
- D. All employees shall be responsible for reporting suspected or actual breaches of data security whether due to inappropriate actions, carelessness, loss/theft of devices or failures of technical security measures.
- E. Individuals may not attempt to log into the network using any network account and/or password other than the login(s) assigned to him/her. Individuals may not allow someone to use his/her network account and/or password to access the network, email, specific software packages, or the Internet.
- F. Reasonable steps and procedures will be taken to secure student records, media center collections, child nutrition, and accounting information, and such information shall be backed up in a routine manner, with such information being maintained in secure offsite storage.
- G. The system-wide technology staff does perform routine backups in an effort to assure continuity of business. There can be no assurance, however, that technology resources will be available within a

particular time frame following an outage. There is no guarantee that information that existed prior to an outage, malfunction, or deletion, can be recovered. Users are expected to maintain and back up their critical files and data.

- H. In the event of a personnel data breach, Mountain Brook Schools will follow the Alabama Disclosure Laws.

IV. COPYRIGHT:

- A. Illegal copies of software/media may not be created or used on school equipment.
- B. Any questions about copyright provisions should be directed to the district Technology Director, local school Technology Coordinator, or local school Media Specialist.
- C. Legal and ethical practices of appropriate use of technology resources are reviewed with students and employees in the system (i.e. as part of the Technology Education Curriculum, during orientation sessions, faculty meetings, or through online methods, etc). Again, all questions regarding legal and ethical practices of appropriate use should be directed to the local school Technology Coordinator and/or district Technology Director.
- D. Copyright is implied for all information (text, data, and graphics) published on the Internet. Student and employee web page authors will be held responsible for the contents of their pages. Do not "borrow" icons, sounds, or graphics from other pages without documented permission. It is the student's or employee's responsibility to secure proper usage permission and/or review the terms and conditions of any site being linked.
- E. Duplication of any copyrighted materials are prohibited unless specifically allowed in the license agreement and, then, should occur only with the knowledge of the appropriate staff.
- F. Digital media and all applications must be used in accordance with the licensing agreement.
- G. All binding contracts/agreements must be signed by the Superintendent.
- H. The district technology staff, local Technology Coordinator or their designee is responsible for the installation of all software on Mountain Brook Schools' devices.
- I. Written permission to post student work on the Internet is obtained through the ***Mountain Brook Schools Technology Usage Agreement***.

V. EMAIL:

- A. Mountain Brook Schools provides access to email accounts for all employees, long-term substitutes, and, in our secure cloud (secure online applications and storage), for students. Email accounts may be granted for school-related organizations or classes with designated employee sponsors.
- B. Mountain Brook Schools make a reasonable effort to maintain (backup) email for normal business operations. Backups are maintained for a maximum of 30 days.
- C. Technical support is provided for Mountain Brook Schools email accounts used to conduct educational and/or instructional business.
- D. Use of Mountain Brook Schools' email accounts for bullying, harassment, intimidation or threat of violence is strictly prohibited.
- E. Mountain Brook Schools' email accounts may not be used for political activity, personal gain, commercial purposes, or profit.
- F. Mountain Brook Schools' email accounts may not be used for attempting to send or sending anonymous messages.
- G. Mountain Brook Schools' email accounts may not be used for sending mass emails unless to parent lists or for other for educational purposes.
- H. Mountain Brook Schools' email accounts may not be used for posting or forwarding other user's personal communication without the author's consent.
- I. Mountain Brook Schools' email accounts may not be used for illegal purposes.
- J. Because email is not securely transmitted, discretion must be used when sending, or encouraging the receipt of the email containing sensitive information about students, families, school system

employees, or any individuals. There can be no assurance that email will be confidential and/or private.

- K. There is a system-imposed limit on storage for employee email accounts. Employees meeting or exceeding the limit will be unable to send or receive emails.
- L. Employees required to maintain email(s) for more than 365 days should print said emails and file or stored electronically in a different format.
- M. The technology staff, administrative staff, or Mountain Brook Board of Education do not technically support or maintain individual user initiated email archives.
- N. Incoming and outgoing email is filtered by the district for inappropriate content, viruses, phishing, and/or malware. However, no filtering system is foolproof, and material deemed inappropriate by individual users or harmful may be transmitted in spite of filtering. Mountain Brook Schools cannot assume any liability for such breaches of the filter.
- O. Employee email accounts will automatically expire on the last full day of employment. Student email accounts will expire the last full day of enrollment. Limited time extensions may apply to graduating seniors.
- P. With reasonable cause, the Technology Director may disable email accounts without notice.
- Q. All employees and students shall use only district approved communication systems to conduct school-related business.

VI. INTERNET USE:

- A. The intent of Mountain Brook Schools is to provide access to resources available via the Internet with the understanding that staff and students will access and use information that is appropriate for their various curricula.
- B. All school rules and guidelines for appropriate technology usage, as well as local, state, and federal laws apply to usage of the Internet.
- C. Teachers shall screen all Internet resources before projecting them in the classroom.
- D.. Internet activity is monitored, along with other aspects of technology usage. However, no filtering or monitoring system is foolproof, and material deemed inappropriate or harmful may be accessed in spite of the systems in place. Mountain Brook Schools cannot assume any responsibility for such breaches.
- E.. Internet access for all users is filtered through one central point by URL (web address) and by IP address and may be filtered by keyword.
- F. URLs (web addresses) and IP addresses may be added to or deleted from the filtered list by the Technology Director.
- G. Individuals may request to review filtered categories.
- H. Successful or unsuccessful attempts to bypass the Internet filter by using proxies or other resources are a violation of this policy.
- I. Internet use refers to internet access via all Mountain Brook Schools/Private and public networks.
- J. Mountain Brook Schools' internet access is CIPPA compliant.

VII. WEB PUBLISHING:

- A. The Mountain Brook Schools' website is limited to usage associated with activities of Mountain Brook Schools. The website cannot be used for commercial purposes, to express personal opinions, to editorialize, or for profit other than school sponsored events.
- B. The Technology Staff reserves the right to reject all or part of a proposed or posted web page.
- C. All pages posted on the Mountain Brook Schools' website must be designed/written with approved software.
- D. It must be easy to determine the name or title of the person responsible for the content on each web page or sections of web pages housed on the Mountain Brook Schools' website.
- E. A staff member's primary web page should be housed on the Mountain Brook Schools' website.

- F. Links from pages housed on the Mountain Brook Schools' website to personal blogs, social networking sites, advertisements unrelated to school system business, and/or personal web pages are prohibited. Only external sites authorized by the Data Governance Committee and linked from Mountain Brook Schools website are deemed official.
- G. All Mountain Brook web pages must be ADA **compliant**.
<https://www.w3.org/WAI/standards-guidelines/wcag/>
- H. All public video must include closed caption.
• <https://www2.dpsk12.org/architecture/accessibilityguide/>
- I. Student pictures or other personally identifiable information can be used in accordance with the "Mountain Brook City Schools Technology Usage Agreement" and in accordance with FERPA guidelines and the Mountain Brook Schools' Data Governance Policy. Full names may only be used in reporting student participation in school-sponsored extracurricular activities, achievements, and other positive recognition.
- J. No written permission is required to list faculty/staff **names** and their school contact information (phone extension, email address, etc.)
- K. Permission for publishing employee photographs on the Mountain Brook website is assumed unless the employee specifies otherwise in writing to his or her **principal or** direct supervisor.
- L. Infringement of copyright laws, obscene, harassing or threatening materials on websites are against the law and are subject to prosecution.
- L. ~~All Mountain Brook School webpages must follow the Accessibility Guidelines~~

VIII. EXAMPLES OF INAPPROPRIATE USE OF RESOURCES: MOVE TO TRAINING

This list is not all-inclusive but is intended to provide general guidance. Anything that would be considered inappropriate in "paper form" or "verbal form" is also considered inappropriate in electronic form. Information, such as but not limited to SIS data, accessed through school system technologies may not be used for any private business activity. The following are examples of inappropriate activities when using any Mountain Brook Schools' network, email system, hardware, software, technology services, and/or Internet access:

- A. Using another user's password or attempting to discover another user's password
- B. Sharing passwords
- C. Trespassing in another user's files, folders, home directory, or work
- D. Saving information on any network drive or directory other than your personal home directory or a teacher-specified and approved location
- E. Downloading, installing, or copying software of any kind onto a computer, laptop, home directory, network drive, or other edevice (except for approved updates or apps)
- F. Harassing, insulting, embarrassing, or attacking others via technology resources
- G. Damaging/abusing technology resources, including, but not limited to, printers, telephones, computers, computer systems, any e-device, or computer networks (this includes changing workstation configurations such as screensavers, backgrounds, printers, BIOS information, preset passwords, etc.)
- H. Intentionally wasting limited resources such as Internet bandwidth, disk space, and printing capacity
- I. Accessing inappropriate material stored on resources such as, but not limited to, digital cameras, flash drives, iPods, online storage, cell phones, websites, etc.
- J. Accessing inappropriate material from websites or attempting to bypass the Internet filter to access websites that have been blocked (Examples: information that is violent; illegal; satanic; sexual; demeaning; racist; inflammatory; and/or categorized as social networking, blogging, or journaling sites, etc.)
- K. Sending, displaying, or downloading offensive messages or pictures
- L. Using obscene, racist, profane, discriminatory, threatening, or inflammatory language in a

document, email, etc.

- M. Using a digital camera, camera phone, or any other device capable of storing a still or video image to take inappropriate, harassing, and/or embarrassing pictures
- N. Editing or modifying digital pictures with the intent to embarrass, harass or bully is prohibited
- O. Participating in unsupervised or non-instructional on-line chat rooms without the permission/supervision of an adult staff member
- P. Posting any false or damaging information about other people, the school system, or other organizations
- Q. Posting of any personal information as defined previously in this document
- R. Broadcasting network messages or participating in sending/perpetuating chain letters
- S. Violating copyright laws
- T. Plagiarism of materials
- U. Use of technology resources to create illegal materials (i.e. counterfeit money, fake identification, etc.)
- V. Use of any Mountain Brook Schools Technology resource for personal gain, commercial or political purposes
- W. Accessing any website or other resources by falsifying information
- X. Downloading games or playing games online that are not instructional in nature
- Y. Streaming video or audio not related to the core business of the School System

Adopted: September 11, 1995

Revised: July 6, 1998

Revised: November 13, 2000

Revised: June 2007

Revised: May 2011

Revised: December 2018

Revised: January 2019

Mountain Brook Schools Email, Text Messaging, and Social Networking Guidelines

The purpose of these guidelines is to ensure the proper use of Mountain Brook Schools' **email and messaging systems, as well as social media platforms** and Internet communication systems and to make users aware of what Mountain Brook Schools deems as acceptable and unacceptable use of its email and Internet communication systems. We reserve the right to amend these guidelines as necessary. In case of revisions, users will be informed by email, by posting on the District Technology web page, through professional development, at faculty meetings, grade level meetings, or department meeting, assemblies, in class, and/or by other means deemed appropriate by the administration.

Employee Email

Mountain Brook Schools considers email as an important means of communication and recognizes the importance of proper email content and prompt replies in conveying a professional image and in delivering good customer service. Email is a school business or educational communication tool, and users are obliged to use this tool in a responsible, effective, and lawful manner. Although by its nature, email seems to be less formal than other written communication, the same laws apply. Any email is discoverable in a due process situation or other legal action and is seen as official communication. In addition, any email exchanged by a school system employee is public record. ~~Other legal risks of email for Mountain Brook Schools and/or their network users include the following:~~

- ~~• sending emails with any libelous, defamatory, offensive, racist or obscene remarks;~~
- ~~• forwarding emails with any libelous, defamatory, offensive, racist or obscene remarks;~~
- ~~• forwarding confidential information;~~
- ~~• forwarding or copying messages without permission or implied permission; and/or~~
- ~~• knowingly sending an attachment that contains a virus that severely affects another network.~~

By following the guidelines in this document, the email user can minimize the legal risks involved in the use of email. If any user disregards the rules outlined ~~set out~~ in these guidelines, the user will be fully liable and Mountain Brook Schools will legally disassociate itself from the use.

The following information should be used as guidelines for the use of email. ~~r as far as legally possible.~~

- Do not send or forward emails containing libelous, defamatory, offensive, racial, harassing or obscene remarks. If you receive an email containing this type of communication, promptly notify your supervisor or administrator.
- Do not forward confidential information unless the intended party is a member of Mountain Brook Schools and falls under "need to know" basis.
- Use caution if you forward a message without implied permission or without acquiring permission from the sender first, especially if it contains sensitive or personal information.
- Do not forge or attempt to forge email messages.
- Do not send email messages using another person's or unauthorized email account.
- Do not copy a message or attachment belonging to another user without the permission or implied permission of the originator.
- Do not disguise or attempt to disguise your identity when sending email.
- Employees should not use school provided email account for retail and other commercial sites unrelated to school business.
- Do not knowingly send an attachment that contains a virus or malicious code.

- Employee must be cautious of phishing emails and should report any incident to your technology coordinator or the technology director.
- The forwarding of chain emails, junk mail, inappropriate jokes, and executables is strictly forbidden.
- Do not send personal mass mailings.
- Do not send emails for personal gain, to solicit business for friends, family, etc., or for political purposes.
- All messages distributed via the school system's email and Internet communication systems, even personal emails, are Mountain Brook Schools' property.
- Reasonable, personal use of email should not interfere with work.
 - When using Mountain Brook resources, personal emails must adhere to the guidelines in this policy.

Maintenance ¶

Email Security and Technical Specs

- Messages in the Deleted Items folder will be automatically removed in 14 days.
- ~~A more frequent manual deletion of items by the individual user is recommended. ¶~~
- ~~User deleted emails will be permanently purged in 7 days.~~
- ~~A more frequent manual deletion of items by the individual user is recommended. ¶~~
- ~~Emails older than 365 days will be removed from all email folders.~~
- Incoming emails may be blocked if the message size is over 25 MB or if there are multiple attachments.
- Quota limits are set to 1GB for Outlook. This includes Inbox, Sent items, Calendar and folders.
- Incoming and outgoing emails sent to or received from Mountain Brook Schools' Outlook Exchange email server are scanned for viruses, spam, and content.
- Users must have no expectation of privacy in anything they create, store, send or receive on the Mountain Brook Schools' computer system. Emails can be monitored without prior notification if Mountain Brook Schools deems this necessary. If there is evidence that users are not adhering to the guidelines set out in this policy, Mountain Brook Schools reserves the right to take disciplinary steps, including termination and/or legal action.
- Email accounts are assigned to new employees when their employment is approved by the Board of Education and when the new employee has completed the Mountain Brook Schools on boarding process. All email accounts maintained on the Mountain Brook email and Internet communication systems are the property of Mountain Brook Schools. Mountain Brook maintains student accounts, employee accounts and employee-sponsored accounts. Only contract employees working 15 hours or more per week will be issued a district email account.
- Passwords should not be given to other people and should be changed if the user believes his/her password is no longer secure.
- Email accounts are disabled and deleted when employees retire, resign, or leave the school system.

Disclaimer

Mountain Brook Schools recommends that employees add a disclaimer to outgoing emails or automatically attach a disclaimer such as the one below to each email sent outside the school system.

“This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this email in error please notify the system manager. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the Mountain Brook Schools. Finally, the recipient should check this email and any attachments for the presence of viruses. The company accepts no liability for any damage caused by any virus transmitted by this email.”

Student Digital Communication

Mountain Brook Schools considers digital communication as an important means of communication and recognizes the importance of proper content. Users are obligated to use tools in a responsible, effective, and lawful manner. All student email and partial cloud content created or received using school accounts are scanned for inappropriate content, self harm and harm to others. If any user disregards the rules set out in these guidelines or other student governing documents, the user will be assigned discipline as outlined in the student code of conduct.

The following information should be used as guidelines for the use of digital communication tools.

- Do not send or forward content containing libelous, threatening, offensive, racial, harassing or obscene remarks. If you receive an content containing this type of communication, promptly notify your administrator.
- Do not forward, send or post sensitive, personal, or inappropriate information.
- Do not send or post messages or content using another person’s account.
- When representing Mountain Brook Schools, only school authorized accounts may be used.
- Do not impersonate or attempt to disguise your identity when sending or posting digital content.
- Do not knowingly send or access content that contains a virus or malicious code.
- Students must be cautious of phishing emails and should report any incident to your teacher or technology coordinator.
- Do not send personal mass communications.
- Do not send communication to solicit business for friends, family, etc., or for political purposes.
- When using Mountain Brook resources, personal emails must adhere to the guidelines in this policy.

Messaging and Social Media For Employees

Digital messaging and the use of social media platforms are recognized as powerful tools to engage students and parents. However, an employee's online actions and conduct reflect upon them personally, as well as professionally. The following are employee guidelines regarding the use of these tools.

General Guidelines:

- Mountain Brook School employees should not post or update personal social media statuses or content during school hours.
- Never accept currently enrolled students as “friends” on personal social media accounts. Cautiously filter who is allowed to view your social media.

- School approved communication resources should be the path for communication between faculty, students, and parents. Personal texts or personal email accounts should not be used.
- Any communication between faculty and students via social media or messaging should be in a group format, avoiding individual messaging when possible.
- The posting of student pictures or student work should comply with the Mountain Brook Schools Acceptable Use Policy agreement. Avoid posting pictures of students receiving special education and homeless services without parental/guardian permission.
- Do not say or post anything on a personal social media account that would reflect negatively on your position as a Mountain Brook employee.
- Any posts or messages that violate board policy, disrupt the school environment, impede an employee's ability to do their job, or are not in accordance with local, state, and national laws may lead to disciplinary consequences or termination.
- Messaging and social media should never be used to discuss school related confidential information.
- Notify an administrator if a student attempts to contact you with any alarming concerns or information.
- Be clear about the purpose of digital media expectations for users.
- Be aware of security settings and data governance requirements when using social media for instructional purposes.
- All school or district sponsored social media accounts must be created and authorized through Mountain Brook Schools. Private social media accounts should not be utilized for the promotion of any school or instructional activity not occurring in a public arena.

~~Guidelines below are presented in a Q&A format.~~

~~¶~~

~~Q: Is it ok for me to initiate electronic communications with a student?~~

~~¶~~

~~A: If a teacher initiates overly personal contact with students outside of school, whether in person or electronically, he or she may create an impression of an unhealthy interest in that student's personal life and may leave himself or herself open to an accusation of inappropriate conduct. Therefore, caution should be exercised in this type of communication.~~

~~Q: What if I receive an email or other electronic message such as a text from a student?~~

~~¶~~

~~A: This very much depends on the nature of the communication received. We would strongly discourage any use of texting, instant messaging or "chat" type communication with students for purposes other than school-related communications. If a communication is received which appears to be a social greeting, you might do best just to acknowledge it in an appropriate way at school. A very brief acknowledging electronic response might be appropriate in some circumstances. However, it is perfectly OK not to respond to such greetings. If you choose to not respond, making an extra effort to cheerfully greet the student at school might be appropriate.~~

~~¶~~

~~If a student sends a message with disturbing content, you should discuss this with your administrator or supervisor, including a school counselor in the discussion as needed.~~

~~¶~~

~~If a student sends a message that appears to suggest an emergency (an allegation of abuse or a student sharing suicidal thoughts or plans), try to contact your administrator or supervisor at once.~~

~~¶~~

~~Q: What about Facebook accounts or other social networking sites? Should I respond to an invitation to become a student's "Friend"?~~

~~¶~~

~~A: We recommend that you not engage in online social networking with students unless the site is used for school information or academic reasons only. This would only be an issue, of course, if you choose to maintain a Facebook, or similar account. If you do so, we recommend that you be extremely cautious about the content of your profiles and pages. ¶¶~~

~~If you are strictly using a social networking site for school related topics and stay away from personal content then these sites should be treated much like any other educational blog. However, the use of comments, "writing on walls," and so on, would be likely to lead to major problems if an approval process is not in place before posting. You may find that it is easier to simply tell your students that you have a policy not to accept students as "friends." ¶¶~~

Mountain Brook Schools Emerging Technologies

As with all technology, new devices and programs are constantly emerging that challenge standard operating in a school and classroom. While we work to stay informed of new trends, there is personal and professional judgement that is called upon in dealing with emerging technologies. Please note that any new technologies should be discussed with the technology director and coordinator and administrator before being utilized for instructional purposes.

General Guidelines:

- Emerging technologies, such as wearable technologies, should only be allowed if a similar device were allowed in the same situation. i.e. A smart watch would be allowed in situations when a cell phone would be allowed.
- Smart speaker and digital voice assistance technologies are not deemed appropriate for classroom settings.
- Devices used to communicate health related situations with school personnel should be allowed at all times.
- Data governance committee approved location monitoring technologies are only used in situations where students are monitored related to a school sponsored event or activity.
- Parents must give the school system permission to collect data about a student using health related or location monitoring technologies. The data collected should only be used for the purpose in which it is intended.
- Be increasingly cautious of asking students to register in software or other technologies. Data privacy approval must be vetted through the data governance process.
- Before using any new technology, ensure that it has been approved by the technology department and administration.

Use of Student Photos and Videos

Mountain Brook Schools Web Page and Web Publishing Guidelines

General Webpage Guidelines

MBS schools requires that departments within the district, schools, and faculty have a web presence on our district provided website. Mountain Brook Schools (MBS) web pages are developed for curriculum and instructional use, school-authorized activities, or information about the Mountain Brook School District or its purpose.

- Web pages, pictures, images, and/or video/audio must adhere to *Mountain Brook Schools Technology Usage Policy*
- All digital content should follow WCAG web content accessibility guidelines 2.0 level AA. <https://www.w3.org/WAI/standards-guidelines/wcag/>
 - When using multimedia, we must provide means for everyone to consume the media. Multimedia is anything that uses audio and video.
 - All images should have alt attributes for screen readers. Example would be naming the images.
 - Text has sufficient color contrast according to webpage contract guidelines. The current MBS web page provided templates and font meets color contrast guidelines.
 - Site is keyboard accessible
 - Site is free of keyboard traps
 - All form inputs have explicit labels
 - Pages should include contact of individual, feedback email is currently listed on all webpages, newest guidelines are W3C web content accessibility guidelines 2.0 level AA
- No student pictures may be posted unless parent permission was obtained during data verification process.
- Text, graphics, audio, and/or video posted on any web based page such as but not limited to web pages, wikis, on-line journals, blogs, twitter, Moodle pages, glogs, voice threads, etc, qualify as “web pages.”
- All public video must include closed caption so they will meet alternative use guidelines.
- MBS web pages cannot be used for profit, or commercial, or political purposes. All posted work must be of publishable quality with regard to spelling, usage, and mechanics. All web page authors are responsible for the maintenance of their own pages, including, but not limited to, adding new content, updating existing content, and deleting outdated content.
- All links should be checked regularly to make sure they are current and working. Pages that are not updated in a timely fashion, that contain inaccurate or inappropriate information, that violate copyright laws, or that contain links which do not work will be removed. The author will be notified.
- Unfinished pages should not be posted until they are fully functional.
- Staff and/or student work may be published only as it relates to a class project, course, or other school-related activity.
- Written permission is obtained from the student and guardian via the Technology Resource Agreement before posting student work on the Internet.
- No Student personal information, including but not limited to, phone numbers, email addresses, or mailing addresses may not be posted on MBS web pages.
- Staff is prohibited from linking to personal blogs, journals and/or personal web pages from class or organization web pages and should post and use school-sponsored email accounts for communicating with students and/or parents.

- Web pages are subject to approval by the district technology coordinator, local school technology coordinator, and building principal and must adhere to the regulations and restrictions established by Mountain Brook Schools.
- ~~Work must be of publishable quality in regard to correct spelling, usage, mechanics, etc.~~
(mentioned above ahead)
- Each school's main page, at a minimum, should include the school's name, address, phone number, fax number, and a link to Mountain Brook Schools District main page.
- Each web page should contain a link back to the previous level in the school's site, and a link to the site's main navigational page.
- Pages that contain time-sensitive information, such as calendars, school events, staff information, etc., should be updated regularly.
- Unauthorized use of copyrighted material is prohibited.
- Web page counters may be added on a site only if an "invisible" counter type and approved by school technology coordinator.
- Links to sites that are not accessible inside the network (blocked by school filter) should not be used.
- The district technology staff and/or local school technology coordinator may remove any web page(s) or content that is deemed inappropriate.
- "Guest books," "chat areas," "message boards," or similar tools must have curriculum value and should be evaluated by and approved by the district Technology Coordinator and/or local school Technology Coordinator prior to use.

Technical Web Publishing Guidelines

- Pages should be sized so they will display properly in a variety of screen resolutions. Pages should be previewed and tested at least at "800 x 600," and "1024 x 768".
- Regular text entries on web pages should be limited to the standard fonts.
- Avoid color schemes or backgrounds that make the information on the page hard to read.
- Colors should be "web safe" as much as possible, so they will display.
- Photos should be sized and named appropriately. Photos should be in .jpeg format. .Png files should not be posted.
- Graphics should be used judiciously. Photos albums using the in10sity template should not contain more than 12 photos.
- Photo albums that are larger than 12 photos should be created using an appropriate web page tool and may be only stored on the designated Mountain Brook Schools web server. The publisher may be asked to or a school or school system webmaster may remove these albums at anytime if space becomes an issue. If a publisher is unsure of the location for storing photo albums, he/she should consult his/her technology coordinator.
- Animated GIF files should be used very sparingly and need to be relatively small. The amount, size, and type of graphics used have the most direct affect on the "load time" of web pages.
- Video and audio files may be used when they are appropriate and are compressed properly. They are generally large files that take long "load times" for the user, and many times require some users (non-district networked machines) to have special plug-ins or viewers/players, in order to view or hear the files.
- Web Pages should be easy to navigate and quick to load. Paths of information should be clearly defined, while allowing for non-sequential browsing.
- Web pages should not be overcrowded.
- Full screen images and multiple images should be avoided whenever possible.
- Web Page content and links should be checked and updated frequently.

Publishing Student Information

- Individual students may be identified by full name unless permission to do so is denied by the parent or guardian in writing on the *Technology Resource Agreement* form. Full names may be used in reporting student participation in school sponsored extracurricular activities, achievements, and other positive recognitions.
- Group photographs of students may be identified by the group name.
- Student photos or videos of students may be posted on the web with parent or guardian permission as indicated on the *Technology Resource Agreement*.
- No other personally identifying information about a student is allowed, such as email address, phone number, home address, etc.

Mountain Brook Schools Copyright Guidelines

The purpose of these guidelines is to ensure all staff and students in the Mountain Brook School System are aware of and adhere to the provisions of the copyright law (Title 17, United States Code). We reserve the right to amend/modify these guidelines as necessary. In the case of revisions, staff and students will be informed appropriately.

General Information

Copyright regulations pertain to all types of materials including print and nonprint.

The "Copyright and Fair Use Guidelines for Teachers" chart available from your school media specialist may be used to inform staff and students of what is permissible under the law.

The four criteria of fair use for copyrighted works are these:

- 1 The purpose and character of the use of the work (whether the use is of a commercial nature or is for nonprofit educational purposes),
- 2 The nature of the copyrighted work (factual work versus fictitious work),
- 3 The amount and substantiality (extent) of the portion used in relationship to the copyrighted work as a whole (quantity and quality of portion used),
- 4 The effect of the use upon the potential market for or value of the copyrighted work.

Teachers and staff are responsible for copyright compliance for themselves and for their students in their students' assigned work.

Multimedia

Multimedia refers to the combining of different types of media, including, but not limited to, text, music, film, digitized images, and graphics. Teachers and students must follow copyright guidelines for each type of media used in creating a multimedia production or project. In addition to listing all of their sources in a concluding bibliography, authors must include on the opening screen a statement that the presentation contains copyrighted material which has been used under the fair use exemption of the U. S. Copyright Law. Students may use their own multimedia projects that contain copyrighted material only in the class or course for which they were created. An educator is required to obtain permission for each portion of copyrighted material after two years of fair use.

Web Publishing

The fair use provisions of the Copyright Law do not extend to Web publishing. Written permission from the owner of each piece of copyrighted material **must** be obtained before any work is published on the Internet. Information about obtaining permission is available from local school media specialists.

Student Work

Written permission must be obtained from the student and parent before posting student work on the Internet via the Technology Usage Agreement form or signed note.

Citations

Examples of bibliographic citations for use in Mountain Brook Schools are based on MLA format and are available in each school and online.

Davidson, Hall. "Copyright and Fair Use Guidelines for Teachers." October 2002. Technology and Learning. 30 June 2003 <http://halldavidson.net/copyright_chart.pdf>.

Mountain Brook Schools Electronics Purchasing and Disposal Guidelines

This procedure is designed to provide purchasing and disposal guidelines for technology equipment in its entirety or in parts (including but not limited to computers/laptops, copiers, mobile devices, flat panels, data projectors, bulbs and batteries, document cameras, sound systems, printers, network equipment, etc.) hereafter referred to in these guidelines as technology equipment..

Purchasing Guidelines

All technology equipment, services, and software purchased for use in Mountain Brook Schools or for Mountain Brook School employees, regardless of funding, should be purchased in accordance with Alabama bid laws and be vetted and approved by the Technology Director or his/her designee. Failure to obtain prior approval may result in lack of technical support, denied access to other technology resources, or disciplinary measures.

All approved technologies over \$200 and any other technology equipment that is not considered a consumable should be inventoried as follows:

- use MBS fixed asset tags,
- complete the district technology information form supplying the specific device and financial information
- email the information form to the Technology Department Administrative Assistant for uploading into the department's inventory program.

It is the responsibility of the local school Technology Coordinator to inventory technology-related equipment used in the local school. The district technology staff is responsible for ensuring that any network equipment, servers, or district technologies. are inventoried.

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. Written documentation including Fixed Asset Tag number, description, serial number, purchase order number, account code, and per unit cost must be provided to the district Technology Office using the appropriate form. All technologies submitted to the Board for approval must be to the District Technology Office no later than end of business day on Wednesday before the following Monday's Board meeting.

It is the responsibility of the local school Technology Coordinator to modify the record in the department's inventory program to reflect any in-school transfers, donations, or discards and must coordinate with the District office for any in-district transfers . **The district technology staff is responsible for modifying the inventory records for any central office transfers, donations, or 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 devices with internal storage, to have the equipment wiped and re-imaged.

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 hard drive 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.

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.

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.

Donations are prohibited to individuals 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 exceeded its estimated life. All donations and/or sales must be approved by the Finance Director and Technology Director.

•