

# Mountain Brook Schools Technology Usage Policy

J-43

## **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 technology environment is to support the educational and instructional endeavors of students and employees of Mountain Brook Schools. Use of any and all technology resources is a privilege and not a right.

## **INTRODUCTION:**

To ensure that 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 Mountain Brook students and staff 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 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 usage of technology and its component parts. Additionally, it is implied that all students and employees 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 school system employees and/or students and brought into school facilities or onto school campuses to access school resources and/or personal resources. All personal technologies used on any Mountain Brook campus are subject to this policy and may be used only if such usage 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, 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 emailing outside the school system or storing/saving on external storage devices or portable devices that do not remain on campus, electronic copies of student or staff personal information. 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 Usage Policy. Students and staff 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. Users should not purchase or dispose of software, hardware, peripherals, or other technology-related devices without consulting the technology staff. 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.
- C. Individuals may use only accounts, files, software, and/or other technology resources that are assigned to, provided, or approved for him/her.
- D. Individuals identified as a real or suspected security risk will be denied access.
- E. Any use of technology resources, regardless of ownership, that reduces the efficiency of use for others will be considered a violation of this policy.
- F. 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.

- G. 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.
- H. Personal technology-related devices such as, but not limited to laptops, cell phones, smart-phones, iTouch/iPods/iPads, cameras or other eDevices, etc. used on school grounds are subject to all items covered in this policy and other applicable published guidelines. The permission for such personal devices to be brought to school and the use of such devices will be at the discretion of the local school administration. The user should not access local area network or wide area network resources that require authentication without the explicit permission of the technology staff. 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.
- I. The district Technology Director, local school Technology Coordinators and/or school system administrators will determine when inappropriate use has occurred, and they have the right to deny, revoke, or suspend specific user accounts.

## II. PRIVACY:

- A. To maintain network integrity and to insure that the network is being used responsibly, if any policy violation or inappropriate behavior is suspected, the Technology Director, local school Technology Coordinators and/or other designated technology staff 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. Because communications on the Internet are public in nature, all users should be careful to maintain appropriate and responsible communications.
- D. 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.
- E. 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 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 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.

#### 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.
- E. Duplication of any copyrighted software/media is prohibited unless specifically allowed in the license agreement and, then, should occur only with the knowledge of the technology staff.
- F. A backup copy of all purchased software programs may be made and, thus, become the working copy.
- G. All original copies of software programs regardless funds used will be stored in a secure place.
- I. In almost every case, if a single copy of given software package is purchased; it may only be used on one computer at a time. Multiple loading or "loading the contents of one disk onto multiple computers," (1987 Statement on Software Copyright) is NOT allowed.
- J. If more than one copy of a software package is needed, a site license, lab pack, network version, or Internet portal license must be purchased. The district Technology Director and/or local Technology Coordinator and the person requesting the software will be responsible for determining how many copies should be purchased.
- K. Either the district Technology Director or the local school Technology Coordinator is authorized to sign license acknowledgements for a school within the system. Copies of any system-wide license agreements must be signed by the district Technology Coordinator and/or Superintendent and

distributed to all schools that will use the software. All binding contracts/agreements must be signed by the Superintendent.

- L. The district technology staff or local Technology Coordinator is responsible for installation of all software in use on the wide area network, local area network and/or individual devices within and purchased by Mountain Brook Schools. Technology assistants or other designated staff may install software on technology devices with permission by the district Technology Director and/or local school Technology Coordinator.
- M. **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 provide 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. **Personal use of email is permitted as long as it does not violate Mountain Brook Schools' policy and/or adversely affect others or the speed of the network.**
- E. Use of Mountain Brook Schools' email accounts for harassing or threatening is strictly prohibited.
- F. **Mountain Brook Schools' email accounts may not be used for political activity, personal gain, commercial purposes, or profit.**
- G. **When employing email, all users are responsible for maintaining professionalism at all times. Avoid impulsive and informal communication. Users must be constantly mindful of the need to review carefully and reconsider email communications before responding to and/or sending email. As a general rule, the content of an email should be acceptable to a general audience.**
- H. Mountain Brook Schools' email accounts may not be used for attempting to send or sending anonymous messages.
- I. Mountain Brook Schools' email accounts may not be used for sending mass emails unless to parent lists or for other for educational purposes.
- J. **Mountain Brook Schools' email accounts may not be used for posting or forwarding other user's personal communication without the author's consent.**
- K. Because email is not securely transmitted, discretion must be used when sending, or encouraging the receipt of 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.
- L. There is a system imposed limit on storage for email accounts. Users meeting or exceeding the limit will be unable to send or receive emails.
- M. Users required to maintain email(s) for more than 365 days should print said emails and file or store electronically in a different format.
- N. The technology staff, Mountain Brook Schools' administrative staff, or Mountain Brook Board of Education do not technically support or maintain individual user initiated email archives.
- O. 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.
- P. **Email accounts will automatically expire on the last full day of employment.**
- Q. At the discretion of the Technology Director, email accounts may be locked without notice.

## **VI. INTERNET USE:**

- A. The intent of the 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 should screen all Internet resources before projecting them in the classroom.
- D. Students gain access to the Internet by agreeing to conduct themselves in a considerate and responsible manner and by providing written permission from their parents.
- E. Students are allowed to conduct independent research on the Internet upon the receipt of the appropriate permission forms.
- F. Permission is not transferable, and therefore, may not be shared. Existing permission forms are valid until new forms are received. Students are required to have new forms signed when changing schools.
- G. Students who are allowed independent access to the Internet have the capability of accessing material that has not been screened.
- H. Internet activity can and will be monitored, along with other aspects of technology usage.
- I. 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.
- J. URLs (web addresses) and IP addresses may be added to or deleted from the filtered list by the Technology Director.
- K. Staff members may request to review filtered categories. Users requesting sites for blocking or unblocking, must list specific URLs.
- L. Successful or unsuccessful attempts to bypass the Internet filter by using proxies or other resources are a violation of this policy.
- M. Internet use refers to internet access via all Mountain Brook Schools/Private and public networks.

## **VII. WEB PUBLISHING:**

- A. The Mountain Brook Schools' web site is limited to usage associated with activities of Mountain Brook Schools. The web site cannot be used for profit, for commercial purposes, to express personal opinions, or to editorialize.
- 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' web site 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' web site.
- 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.
- G. Student pictures or other personally identifiable information can be used in accordance with the signed "Mountain Brook City Schools Technology Usage Agreement" and in accordance with FERPA guidelines.

H. Student posting of personally identifying information of any kind on the Mountain Brook website or linking to personal information from the Mountain Brook website is prohibited. Personally identifying information includes home address, work address, home and/or cell phone numbers, social security number, etc.

I. 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 only be used in reporting student participation in school sponsored extracurricular activities, achievements, and other positive recognitions.

J. No written permission is required to list faculty/staff 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 direct supervisor.

L. Infringement of copyright laws, obscene, harassing or threatening materials on web sites are against the law and are subject to prosecution.

### **VIII. EXAMPLES OF INAPPROPRIATE USE OF RESOURCES:**

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 STI 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 screen savers, 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, web sites, etc.

J. Accessing inappropriate material from web sites or attempting to bypass the Internet filter to access web sites that have been blocked (Examples: information that is violent; illegal; satanic; sexual; demeaning; racist; inflammatory; and/or categorized as a 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 on-line 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

Proposed Revision: April 2011

The purpose of these guidelines is to ensure the proper use of Mountain Brook Schools' email 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.

## **Email**

### Legal Risks

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. 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 set out in these guidelines, the user will be fully liable and Mountain Brook Schools will disassociate itself from the user as far as legally possible.

- Do not send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks. If you receive an email containing libelous, defamatory, offensive, racist or obscene remarks, promptly notify your supervisor.
- 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 a bogus 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.

### **Best Practices**

Mountain Brook Schools considers email as an important means of communication and recognizes the importance of proper email content and of speedy replies in conveying a professional image and in delivering good customer service. The use of email in education, however, is proliferating and the precise legal issues regarding appropriate use are yet to be determined. We are confident that—

- Any email exchanged by school system employees about individual students is public record.
- Any email pertaining to a particular student is discoverable in a due process situation or other legal action.
- The nature of email lends itself to impulsive, overly informal, and sometimes unprofessional communication.

Therefore Mountain Brook Schools urges users to adhere to the following guidelines:

### **Guidance On Email Between School Employees And Parents/Guardians**

Examples of generally **appropriate** use of email between school employees and parents/guardians:

- Teachers invite parents to provide email addresses and then send out emails to those addresses reporting on classroom activities, projects, and assignments. **These messages are generic and do not refer to specific students.**

- Teachers may initiate or respond to email from a parent or guardian about a specific child, exchanging objective not subjective information such as the student's attendance, participation, homework, and performance in class.

**Examples of inappropriate use of email between school employees and parents/guardians:**

- Using email to report on serious problems regarding individual students.
- Using email to discuss confidential and sensitive matters, including:
  - o Medical/psychiatric/psychological diagnoses and treatments.
  - o Contents of special education and/or Section 504 evaluations, intervention plans, IEPs, 504 plans, disciplinary matters.
  - o Family problems and other sensitive family information.
- Using, in email, language that is subjective, judgmental, unprofessional, pejorative, and/or labeling. Examples:
  - o "Have you considered that Johnny might have ADHD?"
  - o "Overall, I think that Johnny is unmotivated/lazy."
  - o "I don't think there is anything wrong with Johnny except his negative attitude."

Email between teachers and parents should be positive and/or general in nature when possible. Discussions involving serious problems and any and all protected information (medical, psychological, psychiatric, Special Education, and Section 504, and disciplinary matters) should occur in person or by telephone.

Parents may initiate inappropriate email exchanges. Example:

"Johnny is in your American History class and is failing. His father is an alcoholic and we are divorced. Johnny has ADHD and clinical depression. Can you please tell me how he is doing in your class and what I can do to help him?"

That kind of message should be deleted and the teacher receiving it should call the parent who sent it. Alternately, the teacher could reply to it, deleting everything from the body of the email sent by the parent, and then respond with directions about how the teacher can be reached by telephone or in person.

**Guidance On Email Between School Employees Concerning Students**

Examples of generally **appropriate** use of email between school employees:

- Emails which provide positive information, objective comments, and/or neutral information regarding school performance. In other words, conducting straight-forward business, staying away from sensitive and confidential areas.

Examples of **inappropriate** use of email between school employees:

- Using email to report on serious problems regarding individual students.
- Using email to discuss confidential and sensitive matters, including
  - o Medical/psychiatric/psychological diagnoses and treatments.
  - o Contents of special education and/or Section 504 evaluations, intervention plans, IEPs, 504 plans, disciplinary matters.
  - o Family problems and other sensitive family information.
- Using, in email, language that is subjective, judgmental, unprofessional, pejorative, and/or labeling. Examples:
  - o “I think Johnny has ADHD”
  - o “Overall, I think that Johnny is unmotivated/lazy”
  - o “I don’t think there is anything wrong with Johnny except his negative attitude.”
  - o “I think this child’s problem is his home life.”

Discussions involving severe problems, subjective comments, and any and all protected information (medical, psychological, psychiatric, Special Education, and Section 504, and disciplinary matters) should occur in person or by telephone.

General **Best Practices** involving all email are as follows:

#### **Writing emails:**

- Use short, descriptive **Subject:** lines.
- Avoid lengthy, detailed email messages. Consider using an attachment for “How To” information, directions, procedures, processes, or similar types of information
- Avoid unnecessary attachments or large file attachments such as multiple pictures, mini movies, etc. **AVOID USING ALL CAPITALS.**
- If using cc or bcc feature, take steps to inform the cc or bcc recipient of any action expected unless the action is explicit in the email. The bcc option is often used to avoid revealing recipient email addresses to the entire group receiving the email; otherwise, the bcc option should be used sparingly if at all.
- If you forward emails, state clearly what action you expect the recipient to take.
- Use the spell checker before you send out an email.
- If the content of an email is not of a public nature, consider using another form of communication or protect the information by using a password.
- Only mark emails as important if they really are important.

### **Replying to emails:**

- Emails should be answered within 24 hours, and at minimum employees are expected to check email at least once per day
- Responses should not reveal confidential information and should be professional.

### **Newsgroups/ListSrvs:**

Users should exercise caution before subscribing to a listserv, newsletter or news group. This type of email may be overwhelming and cancelling a newsgroup and/or newsletter subscription is often difficult if not unsuccessful.

### **Maintenance**

- Delete email messages in a timely manner.
- Print email messages required for documentation.
- 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.
- Messages in the Sent Items folder will be removed in 90 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.
- Email accounts are assigned a mailbox size quota of 500MB. Failure to stay at or below the quota will result in the user being unable to send or receive email.
- Avoid responding to request in emails that could be “phishing” attempts.
- Avoid opening attachments that are suspicious or mass forwarding virus hoaxes.
- Check with the technology staff when in double of the suspicious nature of emails.

## **Electronic Social Networking, Instant Messaging including Texting, etc.**

Electronic social networking and/or instant messaging, such as but not limited to Twitter, IM, or texting, among staff and students is a particularly sensitive matter in a time when growing numbers of school employees maintain social networking accounts, email extensively in their personal lives, and are accustomed to using instant messaging services.

An absolute prohibition of communicating electronically with students seems excessive. On the other hand, teachers and school staff must maintain the highest standards should they choose to interact with students through electronic media. Below are some typical situations on which employees might need guidance.

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.”

## **General Email Information**

### Virus Protection and Filtering

Incoming and outgoing emails sent to or received from Mountain Brook Schools' Exchange email server are scanned for viruses, spam, and content. However, users are expected to exercise caution when opening emails from unknown users or when using the web-based email client from home computers.

Incoming emails may be blocked if the message size is over 100,000 KB or if there are multiple attachments.

### 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.”

### System Monitoring

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 action, including termination and/or legal action.

### Email Accounts

Email accounts are assigned to new employees when their employment is approved by the Board of Education and when the new employee has read and signed acknowledgement and understanding of the Mountain Brook Schools Technology Usage Policy (J-43). All email accounts maintained on the Mountain Brook email and Internet communication systems are property of Mountain Brook Schools. Mountain Brook maintains student accounts, employee accounts and employee-sponsored accounts.

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 deleted immediately when employees retire, resign, or leave the school system for a period of six months or more. Only Mountain Brook employees are given email accounts. Upon request by the administration, Mountain Brook employee sponsored accounts, such as PTA accounts, may be created. Employee-sponsored accounts are subject to these guidelines and it is the responsibility of the sponsoring employee to educate the user of this and all other relevant technology-related policies and guidelines.

## Electronic Communications for Personal Use

Although Mountain Brook Schools' email and Internet communication systems is meant for school business, Mountain Brook Schools allows the reasonable use of email for personal use if certain guidelines are adhered to:

- Personal use of email should not interfere with work.
  - Personal emails must also adhere to the guidelines in this policy.
  - Personal emails should be deleted regularly so as not to clog up the system.

The forwarding of chain letters, 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.

## **Questions**

If you have any questions or comments about these guidelines, please contact your principal or immediate supervisor. If you do not have any questions Mountain Brook Schools presume that you understand and are aware of the rules and guidelines and will adhere to them.

## General Webpage Guidelines

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.

- 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 sites, Moodle pages, glogs, voice threads, etc, qualify as “web pages.”
- Web pages, pictures, and/or video/audio must adhere to *Mountain Brook Schools Technology Usage Policy*.
- 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’s personal information, including but not limited to, phone numbers, email addresses, or mailing addresses may 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.
- 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.

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](http://halldavidson.net/copyright_chart.pdf)>.

This procedure is intended to provide for the proper purchasing and disposal of technology-related electronic equipment (including but not limited to computers, televisions, printers, monitors, fax machines, copiers, cell phones, data projector bulbs, copiers, 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 that will be used in conjunction with Mountain Brook Schools' technology resources or purchased, regardless of funding, should be purchased from an approved list or be approved by a local school Technology Coordinator and/or the district Technology Director. Failure to have the purchase approved may result in lack of technical support or denied access to other technology resources.

All electronic equipment is subject to Alabama bid laws.

All electronic equipment over \$50 should be inventoried in accordance with the Mountain Brook Schools' Finance Department guidelines using the approved Fixed Asset Form. 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, file servers, or district computers, printers, etc. are inventoried using the Fixed Asset Form.

### **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 number, description, and serial number must be provided to the district Technology Office using the appropriate form.

### **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 Fixed Asset Form to reflect any in-school transfers, in-district transfers, donations, or discards. The district technology staff is responsible for modifying the appropriate Fixed Asset Form 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-ghosted 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 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.

*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 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 Fixed Asset Form 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: special adapter cards, memory, hard drives, zip drives, CD drives, etc.

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.