Discussion Points for Teachers on Tech Policy and Appropriate Use

Discussing appropriate use, including MBS technology policy, is in all grade levels' technology curriculum—**see bottom of page**--, so periodic discussion of appropriate use helps meet those standards for your class.

Remind students about being responsible users of school technology and of their expectations when using technology. Also remind students that we are capable of checking their usage of the computers and Internet usage.

Full Tech Policy: http://www.mtnbrook.k12.al.us/Images/Users/9/Policy/J-policies/J-43.pdf

Two Main Points from our Tech Policy: (highlights to help hit the high points)

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.

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

Example: Sixth Grade Technology Curriculum for Digital Citizenship:

11. Identify safe and responsible ways to use technology systems, the Internet including but not limited to social/professional networking, communication tools, and applications.

- Recognize dangers of online predators.
- Understand and explain how to avoid and report online predators.
- Understand the meaning of cyber-bullying, the consequences, and ways to avoid it.

- Identify safe and responsible practices of social networking and electronic communication.
- Understand the meaning of legal versus ethical, as it pertains to digital content and use of technologies.

12. Practice responsible, ethical, and legal use of technology systems, the Internet, communication tools, and applications.

- Keep passwords private.
- Recognize/avoid cyber-bullying tactics.
- Understand consequences of committing cyber-bullying
- Identify ways to prevent cyber-bullying.
- Understand and demonstrate the use of on-line communication tools and social or professional networking tools safely, effectively and responsibly (email, IM, Facebook, Twitter, LinkedIn, texting, voice threads, blogs, wikis, webpages, YouTube, etc.).
- Understand ramifications of posting information, pictures, and videos online.

13. Follow local acceptable use policies regarding technology.

- Follow local acceptable use policies regarding technology