Milton High School
BYOD Digital Learning
Student and Family Manual

Dear Students and Families,

The 2018-19 school year brings with it an exciting new chapter to Milton High School in the form of a digital learning initiative with the aim of enhancing student and teacher learning. This Bring Your Own Device, BYOD, Digital Learning Initiative is built upon the successes attained and the benefits realized from the use of the five-hundred plus Chromebooks shared at MHS. This manual sets out to help you understand the purpose and goals of our BYOD program, to explain how to care for the Chromebook/student owned device, to share our expectations for its use, and to offer guidance on maintaining a safe and responsible digital footprint. This initiative has tremendous potential to improve learning in our school; that potential can be realized by following the guidelines and expectations in this manual.

Thank you,

James Jette
Principal, Milton High School

Ben Kelly
Assistant Principal, Milton High School

Brian Mackinaw
Assistant Principal, Milton High School

Table of Contents

Section 1

Purpose & Goals

The purpose of our BYOD program is to help make our students college and career ready. Students will become productive Digital Citizens who continuously grow as independent, confident, resilient, and thoughtful individuals willing to explore new ideas, reflect on progress, and challenge themselves.

As a result of BYOD students will be able to:

- ❖ demonstrate personal responsibility, character, cultural understanding, citizenship and ethical behavior.
- ❖ make connections between existing information and the content they are creating.
- ❖ actively solve problems, answer questions, brainstorm, work in teams, debate, and formulate questions of their own.
- ❖ use interactive tools, digital resources, and creation/production tools that will enable deeper study.
- ❖ to communicate information clearly and effectively using a variety of tools and media in different contexts..

Milton High School's goals for a BYOD initiative are focused on enhancing curriculum, instruction, and assessment.

- ❖ Our *curricular* goals center on developing personalized learning experiences and providing equitable learning opportunities that promote student ownership of their learning.

- ❖ Technology in the classroom allows teachers to develop timely and targeted *instruction* that supports individualized student learning.

- ❖ Through *assessments* that utilize technology, the teacher and the student receive immediate and frequent feedback on the student's progress toward the learning goals.

Section 2

Student Responsibilities

Students are responsible for:

- Arriving to school with a fully-charged device, carrying case, and personal headphones*
- Attending each class with their device, personal headphones* carrying case
- Agreeing to and signing Milton Public School's Acceptable Use Policy (AUP) and Acknowledgement of Receipt
- Protecting and backing up all electronic files or data

*Headphones may not be worn during school hours (7:50-2:19), unless the student has prior approval from the teacher and the use is directly related to the instruction of the class. This is a matter of safety and we want to make sure all students hear any important announcements/alarms.

Storing & Saving Files:
Milton Public Schools suggests saving all files to Google Drive. Google Drive allows for access of documents online (on the cloud) as opposed to locally on a device. If you decide to save files locally in your file application folder, you will need to backup your data with a flash drive.

Equipment Responsibilities:
Students are responsible for the upkeep of their device and all associated accessories.

- No food or drink should be near the device.
- Do not place paper or pens in the device when closing its cover.
- Do not touch the screen with pens or other objects.
- Please keep the AC adapter in good condition by not damaging the wire or stepping on it.
- If a student is leaving the school district and been loaned a Chromebook, the Chromebook and associated accessories must be returned prior to the student's last day of attendance.
- Please keep the device in a case and out of extreme weather conditions which can cause damage (extreme hot/cold).
- Do not alter the device's appearance in any way (stickers, glitter, markers, tape, etc…) other than a laptop skin.

Device Accidental Damage/Loss Policy, Repairs and Damages:

Level 1 –*Software issues, login issues, general help desk questions*
Students should stop by the Student Technology Assistance Team, STAT, in the library to get help with the problem. A technician will contact you to arrange a time to meet.

Level 2 – *Defective hardware*
Technicians will identify what, if any, parts need to replaced and will make the repair. Students will be provided a loaner Chromebook for the duration of the repair. Student owned devices will not be fixed by MHS technicians. However, students will be provided a loaner Chromebook while their device is being repaired.

Level 3 – *More expensive claim, i.e. spill damage, cracked screen, dropped Chromebook*
Students will be responsible for paying for the parts and labor associated with the repair of a Chromebook due to habitual damage or negligence.

Level 4 – *Lost or stolen device*
Students and families must report the incident to an administrator immediately. A full investigation will be conducted to help retrieve the missing device. Students that violate the rules as stated in the BYOD Manual, or fail to store their device correctly will be responsible for the replacement cost of a new Chromebook.

Use of Technology:

Acceptable Internet Use: Students are responsible for proper behavior on school computer networks just as they are in a classroom or a school hallway. Communications on computer networks are often public in nature. General school rules for behavior and communications apply. Internet access is available through the Milton Public Schools' computer network. The purpose of this is to support the educational programs by providing students and teachers with access to unique resources available through the Internet and the World Wide Web. All uses of Milton's Internet access and computer facilities must be in support of and consistent with the educational mission of the Milton Public Schools.

Access to the Internet is a privilege, not a right. Adherence to these Internet guidelines is a condition for a student's access to the Internet. Failure to abide by these guidelines may subject users to termination of their Milton Public Schools computer network accounts, including Google Apps for Education/G Suite accounts, email accounts, and accounts with other district-provided services.

Network users are expected to abide by generally accepted rules of Internet etiquette as well as rules of school decorum. These include common courtesy and the avoidance of vulgar or offensive language. The following are unacceptable uses of Milton's Internet access, network devices, computers, tablets and other infrastructure:

1. Posting private or personal information about another person or yourself.
2. Attempting to log on through another person's email account or to access another person's files.
3. Accessing or transmitting obscene or pornographic material.
4. Posting chain letters or spamming, i.e., sending unsolicited or annoying messages to large numbers of people.

5. Participating in communications that facilitate any form of criminal activity, such as, but not limited to, the illegal sale or use of drugs or alcohol, gang activity, sexual harassment, threats, or any other forms of intimidation.

6. Plagiarizing any material; the rules for plagiarism that are stated in this handbook are also applicable to students' use of the Internet.

7. Infringing copyrights, i.e., inappropriately reproducing or transmitting material protected by copyright.

8. Participating in any and all commercial activities that are not directly related to the educational purposes of the Milton Public Schools, unless specifically approved in advance by the school's Administration.

9. Damaging or modifying MPS computers, computer systems or computer networks.

10. Removing MPS hardware and/or software from school premises without prior written consent from the school Principal or his/her designee.

11. Using any form of proxy and/or filtering avoidance software, hardware, or website.

12. Using others' passwords and/or impersonating another user.

13. Trespassing in others' folders, work or files.

14. Gaining unauthorized access to MPS or others computer, server, or telecommunications networks.

15. Interfering with the operations of technology resources.

From time to time, the Milton Public Schools' Director of Technology will make determinations on whether specific uses of the network are consistent with the Acceptable Use Policy.

Violation of any of these rules could result in loss of computer privileges, detention, suspension, or any punishment deemed appropriate by the school administration.

Internet use is governed by Milton School Committee policy, school rules and codes of conduct and applicable law and regulation. See School Committee policy IJNDB for further information or obtain a copy of this policy and additional information regarding use of computers in school from the principal.

Parents and students are strongly urged to review the complete School Committee policy on Acceptable Internet Use.

Section 3

Care and Maintenance

- Do not personalize your loaned MHS Chromebook with stickers, markers, glue, or any other foreign substance.
- Do not lean on top of the device when it is closed.
- Use only approved wipes or cleaners that are designed for LCD screens (regular glass cleaners that contain alcohol or ammonia will cause damage).
- Be careful with the screen. Do not touch the screen with your fingers or any other object.
- While the device is off, you may clean the keyboard, trackpad, and surfaces with a lightly dampened cloth. Never spray cleaners directly on your device.
- The trackpad can be damaged if not used properly. Never use a pencil, eraser, or other object on the trackpad.
- Do not place heavy objects on top of the device. This may cause damage to the screen and internal components.
- Do not place anything between the screen and the keyboard when you close the device.
- Use your device on a sturdy surface that allows for adequate air circulation. Placing the Chromebook on an item that blocks the side air vents can cause the device to overheat.
- To maximize the overall life of the battery, once or twice a month, run the battery down completely before charging your device.
- Do not bend the AC adapter cord. Leave plenty of room for the wire to reach the device.
- Work on a flat and level surface and not on top of other items on your desk.

When moving about with your device:

- Save all open documents.
- Put the device to sleep by closing the lid.
- When not using the device in class, it should be placed into the carrying case. Do not leave it out where it could be knocked off of a desk.
- Use the device carrying case to transport the device between home and school.
- Use the carrying case when transporting the device between classes.
- Do not put pens, scissors or paper clips in the same compartment as your device; they may damage the screen or one of the ports.

Device Security:

- **During the school day**, devices must be stored in a secure location, or a locked locker.
- **At the end of the day,** students should take their device home. If attending an extracurricular activity, the device must be locked in a locker.

Never leave the device unattended in a classroom, hallway, or locker room. The safest and best option is always to secure the device in a locked locker.
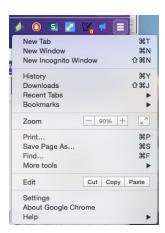
To maximize battery life:

- Turn down volume.
- Turn down brightness.
- Charge the device fully before the beginning of the day.
- Dim the screen to conserve power and make the battery charge last longer.
- Only keep open applications and websites that are being actively used. This saves processor power, memory and extends battery life.
- Save early, save often. Do not wait until the end of class to save documents (if not using Google Applications). Make sure to save regularly while working.
- At the end of class, save all work, put the device to sleep, and place it in the carrying case only after it is asleep (cover closed).

After school and at home:

- Use a surge protector, when possible, instead of plugging directly into the wall to protect from power surges.
- When connecting to power, plug in to the wall first, then the device.
- When disconnecting from power, unplug from the device first, then from the wall.
- Use the device on a sturdy surface that allows for adequate air circulation. Placing the device on an item that blocks the side air vents can cause the device to overheat.
- Be wary of "borrowing" wireless access from others. Others may be accessing your information.
- Use the device away from food and liquids. Spills will damage the device.
- Leave the device in a locked locker during and after school sports and activities.
- Do not leave the device in a car overnight or for long periods. Extreme heat or cold can damage the device.
- Do not keep metal items like paper clips or staples near the power port on the device. The magnetic charge on the port will attract them and may cause damage.
- Please restart your device at least once a week.
- Shut down your device if you do not plan to use your device for one or more days.

Troubleshooting a Chromebook

Force quit an application by going to the "hamburger" menu (three horizontal lines at top right of Chrome browser) and selecting Task Manager, or by using the key-combination: Shift + Escape

- If your Chromebook is slow or certain applications are not working properly, save your work (applications that do not save automatically) and restart.
- If your Chromebook will not power up, check your battery to ensure there is enough power left.
- If your Chromebook is not responding, try a hard reboot. Unplug your AC adapter and hold down the power button for seven seconds. Once the Chromebook has turned off, it can be turned on again. If the Chromebook is still not responding, bring it to the library for a technician to inspect.

Section 4

Technology Tips

Connecting to the Internet

Chromebooks & BYOD devices need to be equipped with a wireless card. Wireless connectivity is available at school. For home use, students need to connect to a password-protected wireless network. The cards can also access unprotected networks, although this is not suggested as it will leave the device and data vulnerable.
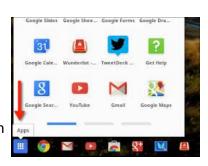
Printing at Home

To be able to print at home, printers must be "Cloud print" capable. For further instructions on setting this up, select this link.

Technical Support

Technical support is available during school hours from the STAT help desk and/or MPS Technology Department. In the event that a loaned Chromebook needs repair, report it to the school computer technician by bringing the device to the librarian and completing a technology request ticket. Every effort will be made to repair or replace the Chromebook in a timely fashion. Depending on the severity and nature of the issue, a loaner Chromebook may be provided until your Chromebook is repaired and returned to you. Devices brought from home will not be fixed by the school, however they will help diagnose the problem, troubleshoot connectivity and login issues, and provide a loaner Chromebook until the student's device is repaired.

Section 5

Files and Folders

- Chromebooks allow for 16GB of local storage. Files are stored locally in a "Files App" that can be launched from the apps manager or the Google Apps suite.
- It is the responsibility of the student to backup all local files on their device. It is highly recommended to save all important files in Google Drive.

Apps and Extension

All required school apps and extensions will be installed on the Chromebook by the school's technology department. Students will not have the ability to add apps or extensions directly. Individual apps or extensions can be requested by a student to the technology team by emailing helpdesk@miltonps.org. The technology team will consider the request and, if approved, it will be "pushed out" to the student's device. Please do not attempt to delete or manipulate the Chrome OS.

Students are not permitted to download or install programs to their Chromebooks.

Illegal File Sharing

File sharing programs that illegally download music, videos, games, etc. may not be installed or used on the Chromebook. It is a violation of Milton Public School's Acceptable Use Policy and may be a violation of federal copyright laws.

Password

Students login under their assigned username and password and should not share either with others.

Student Files

In order to stay organized, we highly recommend that students create folders within Google Drive for each subject. As you create documents, save them to the appropriate subject folder to make it easier to find your documents and stay organized. For example: documents in a Documents folder for each class, movies in a Movies folder, pictures in a Pictures folder, and music in the Music folder.

      To create a new folder in Google Drive:
      Through Google Suite, click the Google Drive App
      Click the blue "New" button
      Click "folder"

Section 6

Email and Internet Use

Email
Students will use Gmail as their email accounts for school. When an email is sent, the name and user identification are included in the email message. Students are responsible for all email that they send. In association with any investigation, email, stored data, transmitted data or any use of online services will be made available to district, local, state, and federal officials.

Internet Use
Milton Public Schools maintains filtering and firewalls as required by the Children's Internet Protection Act (CIPA). The firewall and filtering restrict access to unacceptable sites, chat rooms, and online games. However, no filter is as reliable as adult supervision. It is the responsibility of the student to appropriately use the device, network and the Internet.

Internet Use At Home
While the same filtering is used at home and at school, it is the responsibility of the parent/guardian to monitor student device use, especially Internet access, while at home. We highly recommend that devices be used in locations that can be easily monitored and supervised by the parent/guardian.

Milton Public Schools provides Internet filtering software while devices are connected to the Internet from outside of school which meets the CIPA guidelines. It is the responsibility of the parent/guardian to contract with an Internet Provider in accessing Internet from home and it is the financial responsibility of the parent/guardian.

Basic Internet Safety Rules:

- Never give to anyone personal information such as addresses, phone numbers, passwords, and social security numbers.
- Obey all copyright laws.
- Never use or transmit anything that is abusive, threatening, demeaning, slanderous, racist or sexually explicit.
- Students should notify a family member, teacher, administrator, or counselor if they access information or messages that are inappropriate, dangerous, threatening, or if the content makes them feel uncomfortable.

Internet Safety Links

The following links to websites offer tips for the safe and responsible use of the internet:
- Safe Teens, Common Sense Media, Wired Safety, NetSmartz Workshop

Section 7

Internet Safety Tips

Internet Safety Tips: Know the Risks

Students and parents should be aware of the risks associated with using the internet in order to to avoid them or minimize their impact and help keep children's online time constructive.

It is essential to be aware. In considering the risks, it is important to take into account what may reach students through the Internet as well as what they may share over the Internet with the outside world. Not all students will encounter all of the potential hazards listed below, but by being aware of them, families can consider how to respond before ever going online.

- **Inappropriate Content**
  There is always concern regarding student's access to websites that promote pornography, violence, or self-destructive behaviors. While parents/guardians should be concerned about the content they see on the web, they also need to consider sites that look legitimate, but are fake; sites that have been infected by malicious software; sites that are used by malicious hackers to steal passwords and other information. It is important to be aware of a website's security and privacy practices, especially if it requires a young person to provide personal information in order to use the site or features and software on it. Digital security and appropriateness of content are both important factors to think about when considering which sites are appropriate for young people.

  Safety Tip
  • Keep the device in a common area where you can supervise as needed.
  • Use the parental control features available in security software to block categories of sites, set time limits, and prevent personal information from being posted online.

- **Unwanted Contact**
  As a social medium, the Internet enables students to stay in touch with friends when they are separated from them or to meet new people who share their interests. When students are socially active on the Internet, they are most likely managing at least one personal profile on a social networking site which requires or allows them to publicly share something about themselves. There may be people familiar or unfamiliar to them who could take advantage of this. Behaviors such as online grooming (technique used by a sexual predator to convince an underage person to have relations with them offline) and cyberbullying are some examples of unwanted online contact that parents and caregivers should understand and help students recognize and act on if they ever experience it. In both cases, the first and best response is to alert their parents/guardians so they can figure out next steps together.

Safety Tip
• Ignore contact from strangers or from people that are attempting to bully.
• Report repeated, hurtful, or troubling contact to the website and to a responsible adult who can help track the communications for remedial action.

- **Aggressive or Undesired Commercialism**
The Internet is a powerful marketing tool, and advertising messages targeting students are plentiful. Parents/guardians should be mindful of messages that entice them to acquire products or services in exchange for information or money. It is important to be aware of how this type of commercialism is delivered, what is being offered, and what students may do as a result of it. Vendors are using more creative ways to promote their goods and embed their marketing messages which may make it difficult for a young person to differentiate between an advertisement and the content they are accessing (a technique called immersive advertising). Free offers and promotions for age-inappropriate products and services (dating services, gambling services, etc.) may also be compelling enough to a student to enter personal information that could later be used by the advertiser to deliver continuous, intrusive advertising (as spam or pop-up advertising) or worse, may end up in the wrong hands (to perpetrate hack attacks, identity theft, etc.).

  Safety Tip
  • Think critically about offers that are too good to be true. Turn on pop-up blockers in the web browser.
  • Use up-to-date security software and, if available, the ad-blocking feature which can prevent ads being displayed.

- **Computer Security Threats**
Risks of spyware, spam, viruses, or hack attacks exist. In the case of social media, attackers mask their attempts by preying on behavior that is normal or intuitive to a young person using the Internet. This is called "social engineering" and attacks can be cloaked with as simple a message as, "Hey, check out this video" in a video sharing site. The attacker's motive is simple: to make money, and the Internet is an attractive place to make it, since it offers anonymity and a large user base comprised of many unsuspecting users who are more susceptible of falling for the techniques they use.

  Safety Tips
  • Always use up-to-date security software.
  • Stick to reputable sites and read the user license agreements carefully for anything being downloaded.

Internet Safety Tips: What Students Share with the World

- *Personal/Private Information*
  The majority of students' online activities involve creating personal profiles, communicating with friends, and sharing things about themselves with others. In order to take advantage of online social venues, they have to provide self-identifying information from user names to photos to personal opinions, likes, and dislikes. In this vein of self-expression, they may also provide too much information which could be used by people with bad intentions or that may damage their own reputations among people they never intended to see it. It could also be used by hackers for the purposes of identity theft. Information posted online could be accessible at any point in the future, so young people should think before publicly sharing anything personal, through any online medium.

  Safety Tip
  • Understand anything posted online could be made public and is permanent. Avoid sharing too much information–in words, pictures or videos–that could hurt you.
  • Use privacy settings and never share your username or password with anyone.

- **Disparaging Comments and Inappropriate Content**
  The anonymity of the Internet can unfortunately encourage offline bad behavior to continue and be exacerbated online. As noted earlier, students can become targets of cyberbullying, but they can also be as much a participant as a victim in this behavior. Because the information they post can be accessed by anyone virtually forever and can potentially be traced back to them, it is best always to be respectful of others, online or off. More severe comments, particularly those involving physical threats, may be considered a criminal offense.

  A trend is the use of cell phones by children is "sexting," the act of sending sexually explicit messages or photos electronically, primarily between cell phones. The photos are often of students themselves or others that they know. Most students do not realize that they could be charged with the distribution of child pornography, a serious criminal offense.

  Safety Tip
  • Do not post or forward anything online that could hurt another person. Some types of harassment or content can be considered a criminal offense, and can be traced back to you.
  • Report any bullying or inappropriate content that can be hurtful to another.

- **Peer-to-Peer (P2P) File-Sharing Services**
  File-sharing services are a popular tool that enables students to share media files such as music, movies, or video games. The public discussion and concerns surrounding these types of services have focused on the legal issues (copyright infringements), as well as the age-appropriateness of the media being shared (such as pornography or violent games). In addition to these risks, file-sharing services have increasingly become a destination for cybercriminals to fool people into downloading fake or malicious software. As noted before, their primary motivation is money. A combination of awareness of what is legal and what is

not, proper use of the file-sharing service, and security technology can help students safely and securely enjoy sharing their favorite forms of media with their friends.

Safety Tip
• Determine if your child needs to use these services at all. These services can open up your system to security risks and may be encouraging him/her to share illegally copied material.
• Always use up-to-date security software to help prevent hackers from installing malicious software on your Chromebook and stealing your personal information.

Internet Safety Tips: Be Prepared for What May Reach Students

Below are some additional basic safety measures you and your child can do together today particularly if your children are just beginning to explore the Internet:

- **Keep the device in a common area** where you can be present while your child is using the Chromebook or spot-check its use, as appropriate to the child's age.

- **Agree to time limits for using the Internet and all social devices** per day, per week, etc. Some security software will allow you to set specific times when your child can access the Internet.

- **Agree on websites your student can visit** and make sure he or she only uses sites that are age-appropriate (most social networking sites have minimum age requirements.

- **Review content and privacy and security policies of the sites your student frequents;** make sure you understand how and what type of personal information might be collected by the site and how it may be used.

- **Talk with your student about entering personal information online** and advise your student to stay on the agreed-upon websites only and not give out personal information such as name, address, phone number, age. If he/she is tempted to do this because of a contest, poll, or membership form, ask them to discuss with you first and only proceed with your permission and involvement; it could be opening the door to spam or something more harmful such as spyware.

- **Ignore unwanted contact from people they have never met** as not responding or reacting will typically deter future contact. If it persists, advise him/her to let you or any adult know about it. You should also report this to the site or service being used to contact your student, and the authorities if you or your child feels he/she is in danger in any way.

- **Check browser history,** after they are finished using the device. This will help ensure they did not wander off onto websites they should not have visited.

Internet Safety Tips: Be Prepared for What Students Might Share

In general, common sense and critical thinking are the foundation for students to become safe, responsible users of the Internet. Any interactions they have online should be done with the same approach as they would offline, so talk to your student about using the guidelines below:

- **Be cautious and wise about what you post.**
  Think before sharing thoughts, photos, videos that are very personal or less than positive about you, knowing they could also be used against you.

- **Use the privacy tools available in social networking sites.**
  Only those you invite to join your network should be able to see details about you and the people in your network. Even so, it is still wise to think twice before posting anything that is not intended for others to see or know because it can be passed along by friends.

- **Where possible, use nicknames, not your real name, to identify yourself** on social-networking sites, in chat rooms, on blogs.

- **Be respectful of others.**
  Avoid posting anything about another person that is libelous, lewd, racist or in violation of a site's or service's terms of service. Not only will it be taken down, but it could be traced back to you and—if it is considered illegal—may land you in trouble.

- **Use legal file-sharing services only and ensure they are set up properly.**
  If files are being shared illegally, whether it was intentional or not, you could be held legally responsible for copyright infringement. Also, having the proper settings for the service will ensure that your device and its contents are not vulnerable to hackers, viruses, spam, spyware, etc.

Section 8

Social Networking Tips

As a social medium, the Internet enables students to stay in touch with friends when they are physically separated from them and sometimes to meet new people who share their interests. Social networking sites, chat rooms, message boards, and blogs are some of the many ways this is possible on the Internet.

Know the Risks

If students are socially active on the Internet, they are very likely managing at least one personal profile on one or more social networking sites which requires or allows them to publicly divulge something. While this is not inherently bad, there may be people familiar or unfamiliar to them who could take advantage of this.

- **Unwanted Contact**
  Behaviors such as online grooming (technique used by a sexual predator to convince an underage person to have relations with them offline) and cyberbullying (online harassment of classmates or peers) are some examples of unwanted online contact that parents and caregivers should understand and help students recognize and act on if they ever experience it. In both cases, the first and best response is to encourage students not to respond to such messages and to alert a parent to determine the next steps together. It is also a good idea to save the messages in case they later need to be used as evidence.

- **Aggressive Commercialism**
  In addition to unwanted contact, parents and caregivers should be mindful of online messages - sometimes legitimate, sometimes malicious – that entice students to acquire products or services in exchange for information or money. It is important to be aware of how this type of commercialism is delivered, what is being offered, and what students may do as a result of it. Vendors are using more creative ways to promote their goods and embed their marketing messages, which may make it difficult for a student to differentiate between an advertisement and the content they are accessing or even interacting with (a technique called immersive advertising). Free offers and promotions for age inappropriate products and services (dating services, gambling services, etc.) may also be compelling enough to a student to enter personal information that could later be used by the advertiser to deliver continuous, intrusive advertising (as spam or pop-up advertising) or worse, perpetrate cyber-crime (hack attacks, identity theft, etc.).

- **Cybercrime**
  Social networking sites are also an increasingly popular place for cybercriminals to trick people into divulging information or downloading software onto their device for any number of uses. Their methods range from simple to elaborate.

  Sometimes a student will see an advertisement or link to download seemingly harmless software that he/she can use on their own social networking profiles, but which in fact has been infected with malicious software that gets downloaded along with the legitimate software. Some applications that run on social networking sites may encourage students to complete a survey or provide information that might not be appropriate to share with others. Other times, a student can be lured to see an "attractive" video but is told it is necessary to download a viewer in order to see it. While downloading a viewer is a normal action necessary to see videos online the viewer could be infected with other software that, once installed, can be used by the cyber-criminal to steal information from the computer, spy on the activities of its owner, or other uses depending on the type of malicious software installed.

- **Behaviors Toward Others**
  Students and adults believe everything they do online is anonymous and cannot be tracked back to us. Unfortunately, this belief can encourage bad behavior done offline to continue and be exacerbated online. Students can be victims as well as participants in behaviors such as cyberbullying and harassment. It is important for them to know that information they post can be accessed by anyone virtually forever and can potentially be traced back to them, so it is best to be respectful of others, online or off. More severe comments, particularly those involving physical threats, may also be considered a criminal offense.

Be Prepared

Parents/guardians, teachers, and others who care for students who are socially active online should first set reasonable expectations. Forbidding young people to use social networking sites may force them to go "underground" and find other avenues (e.g. library computers, mobile phones, friends' computers) to continue their social life online. A positive alternative is to teach them how to think critically about what they are seeing, reading, hearing and sharing online.

Below are some guidelines **for students** to follow when they are using social networking sites, chat rooms, blogs, or message boards:

- **Use a nickname or code name.**
  It is best not to use your real name or to use names that might be sexually suggestive or offensive to others in any way. This can help reduce the likelihood of your being harassed online.

- **Set your profiles to private.**
  Social networking sites can be a great tool for connecting with others. A good way to stay safe using these services is to use the highest level of privacy settings possible, that still allows

flexibility to use the site in a way that is useful.

- **Keep personal information to yourself.**
  It is best not to share your address, phone number or other personal information online, with strangers. Do not reveal your actual location or when and where you plan to be somewhere.

- **Think about what you post.**
  Be cautious about sharing provocative photos or intimate details online, even with people you know or even in a private email or text conversation. The information or conversation could be copied and made public by anyone you share it with - and tough to get removed. Remember: what you say in a chat room or instant messaging session is live - you cannot take it back or delete it later.

- **Keep your security software up-to-date.**
  Social networking sites are very popular. Because there are so many people using them, cybercriminals have been known to use stealthy tactics in order to infect the computers of people who use them.

- **Read between the "lines."**
  It may be fun to meet new people online for friendship, but be aware that, while some people are nice, others act nice because they are trying to get something. Flattering or supportive messages may be more about manipulation than friendship.

- **Avoid in-person meetings.**
  The only way someone can physically harm you is if you are both in the same location, so – to be 100% safe – do not meet him/her in person.

- **Be nice online.**
  Treat people the way you would want to be treated. Harassing or bullying anyone online, if considered threatening, can also be considered a criminal offense.

- **Think about how you respond.**
  If someone says or does something that makes you uncomfortable, block them and do not respond. If it continues, let your parents or another adult know. If the messages are threatening in any way, save the messages and tell your parents as this may be considered a criminal offense.

- **Be smart when using a cell phone.**
  All the same tips apply with phones as with computers. Be careful who you give your number to and how you use GPS and other technologies that can pinpoint your physical location. If your phone has a camera, be sure that the photos you take or share will not get you into trouble. Sending or sharing inappropriate photos of yourself or others to friends on social networks (or text) can end up getting you and others into serious trouble.

Be Prepared

It is important to note that most major social networking sites require all users to be age 13 or older, as noted in their Terms of Use. If a student meets the site's minimum age, below are some guidelines <u>for parents/guardians and teachers</u> to consider when it comes to allowing students to use social networking sites, chat rooms, blogs, or message boards.

- **Ease into the process together.**
  If you are going to help your child use social networks safely and responsibly, it is a good idea to use them yourself. There is no need to be a power-user or a technology expert. Spend a few minutes setting up a profile, using the privacy settings, and connecting with a few close friends or family. It is the best way to help your own child use it safely.

- **Consider keeping an eye on your child's social network use.**
  If your child does meet the site's minimum age limit, connect with your child so that you can help him or her navigate this online world.

- **Be reasonable and try to set reasonable expectations.**
  Pulling the plug on your child's favorite social site is like pulling the plug on his or her social life. Instead of being protective, it can shut down communication and send kids "underground" where they are more at risk. It is too easy for them to set up free blogs and profiles from anywhere, including friends' houses or even a cell phone.

- **Talk with your child about how he/she uses the services.**
  Your child, not news reports or even experts, is the one to consult about his/her online social experience. Help him/her understand basic safety guidelines, such as protecting privacy (including passwords), not harassing peers, never talking about sex with people they do not know, avoiding in-person meetings with people "met" online, and taking care in what is posted. Help him or her understand that anything put online can be used against him/her.

- **Support critical thinking and civil behavior.**
  No laws or parental-control software can protect better than a child's developing good sense about safety and relationships. Research shows that children who are aggressive and mean online toward peers or strangers are at greater risk of becoming victims themselves. Teach your child to be a good citizen and friend online as much as offline.

- **Consider requiring Internet use in a high-traffic place in your home.**
  Try to stay aware of your child's time online by keeping the device in a shared area of the house. This way, you can encourage a balance between online time and the offline academic, sports, and social times. Know that there are also many ways kids can access the Internet away from home, including on many mobile phones and game players.

Safety Tips for Sharing Videos and Photos Online

Below are some guidelines for young people to follow when posting and sharing videos and photos online.

- **Tough to Take Back**
  Whatever you post is permanent. Even if you later delete it, there is a chance that it has been copied, forwarded, or reposted. In addition, there are Web archive services that retain content years after it has been taken down.

- **What the Background Reveals**
  Think about what is in the scene you are recording: posters on your wall, photos on a shelf, school or team t-shirts people are wearing, address signs in front of a house or car license-plate numbers all can reveal your identity or location.

- **'You Are What You Wear'**
  Think about what your appearance "says" about you. Would you feel comfortable showing this video to your relatives, boss, potential employer, or college recruiter?

- **Respecting Others' Privacy**
  Be respectful of the privacy rights of people in your video. If taping in a public place, be sure to ask permission before including bystanders, and never take video of children without their parents' permission.

- **Everybody's a Videographer**
  Most cell phones and still cameras are also now video recorders. Be aware that when people take out a cell phone, they could be using it to take photos or to record videos.

- **Be a Good Citizen**
  It is your right to express your point of view, but keep in mind that you can be held legally responsible if you slander, libel or defame someone.

- **Respect Terms of Use**
  Most video sites have terms of service to which you must adhere. Most prohibit sexually explicit content, gratuitous violence, and videos that are harassing, defamatory, obscene, libelous, hateful, or violating other people's privacy. Most responsible sites report videos depicting child exploitation and threatening or illegal acts.

- **Respect Copyrights**
  All reputable video-sharing sites prohibit the unauthorized use of copyrighted material. Of course that means that you cannot take segments from TV shows or movies. It also means you must think about the music tracks you use in videos.

- **Talk with children About Video Bullying**
  Creating a video that makes fun of or ridicules another person can be extremely hurtful. This and other forms of cyberbullying are a growing problem on the Internet which affects many children and teens.

- **Kids' Web Video Viewing**
  As with all media, parental discretion is not only advised - it is a necessary part of parenting. Even though most of the major sites prohibit pornography and gratuitous violence, there are videos that are not suitable for younger children and there are some sites that do permit video that may be inappropriate for children or teens. Depending on the age of your child and their maturity, consider using the filtering features of sites like YouTube or be nearby whenever they are using video sites.

Section 9

Acknowledgement of Receipt and Understanding

For further information on our BYOD initiative, please visit our MPS Technology website. Should you have any questions, please contact James Jette or AJ Melanson.