2017

1:1 iPad Program

Manheim Central School District

281 White Oak Road
Manheim, PA 17545

Overview –

Manheim Central School District is committed to the implementation of strategies to enhance the education of our students through our 1:1 IPad Program. The 1:1 IPad Program is defined as a flexible and personalized educational program that integrates new instructional strategies and a mixture of technology tools with the goal of transforming classrooms from teacher-centric to student-centered personalized learning environments which focus on high academics and the integration of 21st century skills.

The 1:1 IPad Program is occurring as a result of the District's strategic plan, which included a goal to integrate 21st Century Learning Skills by utilizing computers as instructional tools. Key components of the 1:1 IPad Program include the expanding role of the classroom teacher, use of a learning management system, and use of student mobile computing devices. Teacher roles are expanding to provide a blended approach of traditional and digital learning resources while mentoring students on how to become self-regulated in their own learning. The learning management system enables teachers to organize curriculum content, provide formative assessments to help change instructional practice, and create a more personalized learning path for students. Mobile devices provide the anytime-anywhere access to learning that is needed for our students to become proficient, life-long learners. Student-centered instructional strategies being introduced include project-based learning, active inquiry, computer-based formative assessments, and hybrid learning. The District continues to go to great lengths to provide our educators with ongoing professional development for best practices in using technology and new instructional strategies.

Additionally, as Manheim Central strives to "meet each student where they are," technology-based strategies will play a central role in personalizing the experience of every student. Through digital content, data analysis, and the expert guidance of our teachers, students will reap the benefits of Mass Customized Learning.

Students in Grades K-4 will have assigned iPads that they will use each day at school (and possibly take home, based upon the curriculum needs of MCSD). This iPad has all of the necessary software needed for their curriculum and learning goals in addition to an internet filter that is active anywhere the students access the Internet.

Costs associated with the 1:1 IPad Program are offset with the reduction in printing, curtailment of traditional textbook purchases, and extension of current student and staff computer refresh cycles. The District is always searching and applying for additional grant funding to further offset costs. Parents and/or guardians do not have to pay a fee for their student's technology use, however; damage to technology by the student, willfully or accidentally, shall incur a fee which is listed in the replacement cost table later discussed in this handbook.

Please read this handbook in its entirety. If you should have any questions regarding any of the materials presented, please contact your child's principal.

Student Expectations –

Students are expected to abide by the following expectations when using the iPad, both in school and out of school as appropriate.

- Adhere to the rules and requirements of the district's Responsible Use Policy
- Follow all instructions from District staff regarding use of the iPad
- Ensure the iPad is fully charged and ready for use each day
- Carefully handle and carry the iPad at all times
- Do not remove the iPad's protective case
- Store the iPad in a secure location when not in use (provided in each classroom).
- Do not share your security access code with others
- Report all damage, loss, or theft to a staff member immediately
- Do not remove any district markings or labels from the iPad
- Do not alter, change, or jailbreak the iPad's operating system

Security, Privacy, and Internet Safety –

Management and Remote Control

The district utilizes management software on all iPads to control settings, install applications, and remotely track devices. The software is required on all iPads and cannot be disabled.

- iPads will submit a daily inventory to the district of what apps are installed
- FaceTime and iMessage are disabled
- iCloud Photo Stream is disabled
- Limited ad tracking is enforced
- An iPad's camera and microphone cannot be remotely activated or controlled by any means

Other restrictions and settings may be enforced as necessary.

Content Filtering

All Internet browsing by Safari or other applications on the iPad is filtered for appropriateness before being displayed. This filtering occurs automatically and will work on any wireless network the iPad is connected to. Although this configuration provides a good level of protection, no filter should ever be considered perfect.

Jailbreaking

Jailbreaking is a term used to describe the process of altering the iPad's operating system through the use of security exploits. A jailbroken iPad is able to run software that has not been reviewed or rated by Apple for meeting safety and security guidelines. As a result, this process significantly increases the risk of the iPad being infected with viruses and malware as well as bypasses the security restrictions placed on the iPad by the district.

Jailbreaking an iPad is not permitted.

By definition, Jailbreaking involves the use of security exploits in either the web browser or hardware security of the iPad and isn't something that can be stopped. It is, however, relatively easy to spot using the management software employed by the district. If a student's iPad is suspected of being jailbroken, it may be remotely disabled, banned from the network, or confiscated without warning and appropriate disciplinary action will be taken.

Responsible Use Policy –

As the Manheim Central School District embarks on the journey to enrich learning experiences, students are encouraged to use District resources such as computers, software, e-mail, and the internet for educational or school related activities and for the exchange of useful information. The iPad is the property of the District and is to be used solely by the student it is being issued to for academic reasons.

Appropriate or acceptable educational uses of the iPad include:

- The use of software, hardware, email, and the intranet/internet for academic purposes.
- Accessing the Internet to retrieve information from libraries, databases, and websites to enrich and expand learning opportunities.
- E-mail and online work to facilitate communication and for school projects and/or assignments.

All users are expected to conduct their online activities in an ethical and legal fashion. The use of these resources is a privilege, not a right. Misuse of these resources will result in the suspension or loss of these privileges, as well as possible disciplinary, legal, or other action necessary. Examples of inappropriate or unacceptable use(s) of these resources include, but are not limited to, those uses; that violate the law or the Acceptable Use Policy (Board Policy 815), the rules of network etiquette, and that would disrupt the educational environment or hamper the integrity or security of school network. Some unacceptable practices include:

- The use of Instant Messaging or screen-sharing programs with other students during school hours.
- Transmission of any material in violation of any U.S. or state law, including but not limited to: copyrighted material without the written permission of the author or creator; threatening, harassing, pornographic, or obscene material; or material protected by trade secret.
- As with all forms of communications, e-mail or other network resources may not be used in a manner that is disruptive to the work or educational environment. The display or transmission of messages, images, cartoons or the transmission or use of email or other computer messages that are sexually explicit constitute harassment, which is prohibited by the Manheim Central School District.
- The use for personal financial, political, or commercial gain, product advertisement, or the sending of unsolicited junk mail or chain letters is prohibited.
- The forgery, reading, deleting, copying, or modifying of electronic mail messages of other users is prohibited.
- The creation, propagation, and/or use of computer viruses or other malicious logic is prohibited.
- Deleting, examining, copying, or modifying files and/or data belonging to other users is prohibited.
- Unauthorized copying/installation of software programs belonging to the school is prohibited.
- Intentional destruction, deletion, or disablement of installed software on any computer is prohibited.
- Vandalism is prohibited. This includes, but is not limited to, any attempt to harm or destroy the data of another user, the network/Internet, or any networks or sites connected to the network /Internet. Attempts to breach security codes and/or passwords are considered a form of vandalism.
- Destruction of hardware or software or attempts to exceed or modify the parameters of the system is prohibited.
- Intentional overloading of school computer resources.

Access to school e-mail and similar electronic communication systems is a privilege, and certain responsibilities accompany that privilege. District users are expected to demonstrate the same level of ethical and professional manner as is required in face-to-face or written communications. All users are required to maintain and safeguard password protected access to both personal and confidential District files and folders.

Unauthorized attempts to access another person’s e-mail or similar electronic communications or to use another's name, e-mail, or computer address or workstation to send e-mail or similar electronic communications

are prohibited and will subject the individual to disciplinary action. Anonymous or forged messages will be treated as violations of this policy. Nothing in this policy shall prohibit the District from intercepting and stopping e-mail messages that have the capacity to overload the computer resources. All users must understand that the District cannot guarantee the privacy or confidentiality of electronic documents and any messages that are confidential as a matter of law should not be communicated over e-mail.

The District reserves the right to access e-mail to retrieve information and records, to engage in routine computer maintenance and housekeeping, to carry out internal investigations, to check Internet access history, or to disclose messages, data, or files to law enforcement authorities. Any information contained on any computer, cloud, or internet transmitted through or purchased by the Manheim Central School District are considered the property of the District. Files stored or transmitted on District equipment, cloud services, or the network are property of the District and are subject to review and monitoring. The District reserves the right to confiscate the property at any time.

This agreement applies to stand-alone computers as well as computers connected to the network or Internet. Any attempt to violate the provisions of this agreement will result in revocation of the user's privileges, regardless of the success or failure of the attempt. In addition, school disciplinary action, and/or appropriate legal action may be taken. The decision of Technology Department and building administrators regarding inappropriate use of the technology or telecommunication resources is final. Monetary remuneration may be sought for damage necessitating repair, loss, or replacement of equipment and/or services.

Guidelines for Cyber Safety –

The District needs to provide a learning environment that integrates today's digital tools, accommodates mobile lifestyles, and encourages students to work collaboratively in team environments. Through providing this learning environment, we will meet these demands which will allow students to manage their own learning at any time and any location. However, the Internet is not the place for an all-access pass. Students of all ages need supervision.

Below are a few tips that can help keep your child safe online:

- You should spend time with your child on-line by having them show you his/her favorite online destinations. At the same time, explain what about online dangers. Make sure your child keeps passwords secret from everyone (except you). Even best friends have been known to turn against one another & seize control of each other's online accounts.
- Instruct your child that the computer is to be used in a common open room in the house, not in their bedroom. It is much more difficult for children to fall prey to predators when the computer screen is actively being watched by others.
- If you can, utilize additional content filters at the modem/router level. Remember that even though the school has a filter on the District computer, it will not be able to block all objectionable material. Content filters are not 100% fail safe. Do not rely on the content filter to protect your child.
- Always maintain access to your child's social networking and other on-line accounts and randomly check his/her e-mail. Be up front with your child about your access and reasons why. Tell him or her that protecting them is your job as a parent.
- Teach your child the responsible use of the resources on-line. Instruct your child:
    - To never arrange a face-to-face meeting with someone they met on- line;
    - To never upload (post) pictures of themselves onto the Internet or on-line service to people they do not personally know;
    - To never give out identifying information such as their name, home address, school name, or telephone number. Teach your child to be generic and anonymous on the Internet. If a site

encourages kids to submit their names to personalize the web content, help your child create online nicknames that do not give away personal information;
    - To never download pictures from an unknown source, as there is a good chance there could be sexually explicit images;
    - To never respond to messages or bulletin board postings that are suggestive, obscene, belligerent, or harassing;
    - That whatever they are told on-line may or may not be true.
- Set clear expectations for your child. Does your child have a list of websites that he/she needs to stick with when doing research? Is your child allowed to use a search engine to find appropriate sites? What sites is your child allowed to visit just for fun? Write down the rules and make sure that he/she knows them.
- Stay involved with your child's school by remaining in close contact with your child's teachers and counselors. If trouble is brewing among students online, it may affect school. Knowing what's going on at school will increase the chances that you'll hear about what's happening online.
- Tell your child that people who introduce themselves on the Internet are often not who they say they are. Show your child how easy it is to assume another identity online. Don't assume your child knows everything about the Internet.
- Video-sharing sites are incredibly popular with children. Children log on to see the funny homemade video the other children are talking about; to watch their favorite soccer player score a winning goal; even to learn how to tie a slip knot. With a free account, users can also create and post their own videos and give and receive feedback. With access to millions of videos comes the risk that your child will stumble upon something disturbing or inappropriate. YouTube has a policy against sexually explicit content and hate speech, but it relies on users to flag content as objectionable. Sit down with your child when they log onto video-sharing sites so you can guide their choices. Tell them that if you're not with them and they see something upsetting, they should get you.
- Remind your child to stop and consider the consequences before sending or posting anything online. He should ask himself, "Would I want my parents, my principal, my teacher, and my grandparents to see this?" If the answer is no, then they shouldn't send it.
- Learn to use privacy settings. Social networking sites, instant messaging programs, even some online games offer ways to control who your child can chat with online or what they can say to each other. Visit the sites where your child goes and look for the sections marked "parents," "privacy," or "safety."

Cyber-Bullying –

The Manheim Central School District is committed to providing all students with a safe, healthy, and civil school environment in which all members of the school community are treated with mutual respect, tolerance, and dignity. The school District recognizes that bullying creates an atmosphere of fear and intimidation, detracts from the safe environment necessary for student learning, and may lead to more serious violence. Therefore, the School Board will not tolerate bullying by District students. For more information, please see Board Policy 249.

1. What Is a Cyber-bully?
    a. A cyber-bully is someone who uses Internet technology to act cruelly toward another person. Online attacks often hurt more than face-to-face bullying because children can be anonymous over the Internet and behave in ways they never would in person. Online attacks can take on a life of their own: A false rumor or a cruel prank can spread quickly among classmates and live on forever in personal computers and cell phones. A fresh new attack threatens wherever there's an Internet connection, including the one place where they should feel safe: home.

2. A cyber-bully might:
    a. Use a phone to make repeated prank calls or send unwanted text messages to the victim.

b. Post cruel comments to the victim's social network site, send unkind emails or IMs to the victim.
c. Create a fake social networking profile to embarrass the victim.
d. Use a victim's password to break into his/her account, change settings, lock the victim out, or impersonate the victim.
e. Forward the victim's private messages or photos to others. The bully may trick the victim into revealing personal information for this purpose.
f. Forward or post embarrassing or unflattering photos or videos of the victim.
g. Spread rumors through IM, text messages, social network sites, or other public forums.
h. Gang up on or humiliate the victim in online virtual worlds or online games.

3. Here are five suggestions to protect your child:
    a. Remind your child never to share his/her passwords, even with good friends.
    b. If your child has a bad experience online, he/she should tell you right away. If possible, save the evidence in case you need to take further action.
    c. Don't respond to the bully. If the bully sees that your child is upset, he/she is likely to torment even more. Ignore the harassment if possible, if not, block the bully from contacting your child by using privacy settings and preferences.
    d. Remind your child to treat others as he/she wants to be treated. This means not striking back when someone is mean and to support friends and others who are being cyber-bullied.
    e. Finally, limit the amount of social time your child is online. Studies show that children are more likely to get into trouble on the Internet—including bullying others or being bullied—the more time they spend online. If you need to, limit the computer time to strictly academics.

4. Is Your Child a Victim?
    a. Most children won't tell their parents that they're being bullied because they're afraid their parents will take away the Internet or insist on complaining to the bully's parents. Sometimes children who are bullied are ashamed and blame themselves. Reassure your child that nobody deserves to be mistreated. Tell them that some people try to hurt others to make themselves feel better or because they've been bullied themselves. Let your child know that it's important for you to know what's going on so you can help.

5. Signs that your child is being bullied can be hard to spot but may include:
    a. Seeming nervous or unusually quiet, especially after being online.
    b. Wanting to spend more or less time than usual on online activities.
    c. Not wanting to go outdoors or to school.
    d. Problems sleeping or eating.
    e. Headaches or stomachaches.
    f. Trouble focusing on schoolwork.

6. If you suspect your child is being cyber-bullied, talk to him/her. Tell your child that by talking it over, you can work out a plan to deal with bullying. You might:
    a. Contact the bully's parents. Be careful if you decide to do this because it can backfire and make the bullying worse. It's best if you already know the other child's parents and get along with them.
    b. Contact your school officials. Make them aware of the problem and ask them to be on the lookout for signs that your child is being bullied at school. The school counselor or principal may have some strategies or even programs in place for handling bullying in school.
    c. Look into filing a complaint against the bully if the behavior persists. Most internet service providers, websites, and cell phone companies have policies against harassment. You may be able to have the bully's account revoked.

d. Contact the police if you fear for your child's safety. Cyber-bullying can cross into criminal behavior if it includes threats of violence, extortion, child pornography, obscenity, stalking, extreme harassment, or hate crimes.

7. If you learn that your child is being cruel to someone online, find out why. Often, cyber-bullies are victims themselves. If this is the case with your child, go over the suggestions to help protect them against being bullied. But remind them that bullying someone online or off is never ok.

8. If your child notices someone else being picked on, encourage him/her to support the victim. Many social websites, such as YouTube and Facebook, allow users to report abuse. Bullies often back down when others make it clear they won't tolerate rude or nasty behavior.

9. Cyber-bullying may be the most common online danger, but as a parent, talking openly about the issue is the best way to give your child the tools to protect him/herself from virtual sticks and stones.

Damage –

MCSD Technology Services will attend to all repair needs for this program. Accidental damage, including cracked screens, will be fully covered for up to two (2) incidents per year. However, incidents beyond this allotted amount may result in a financial obligation to the student and their family. Each iPad is issued with a protective case to help minimize the potential for damage, and this must remain on the iPad at all times.

The lists below are not comprehensive, but cover most of the situations typically seen. The district reserves the right to review all damage incidents and loss on a case-by-case basis.

- Damage, Repairs, and Replacements Covered in Part or in Full by MCSD
    - Accidental damage including drops and breaks

- Damage, Repairs, and Replacement That Students and Families Are NOT Responsible For
    - Factory defects
    - Hardware failures not resulting for drops or breaks
    - Stolen iPads when a police report is provided within one week
    - Loss, theft, or accidental damage occurring at school (the iPad's last network check- in must occur on district property)

- Damage, Repairs, and Replacement That Students and Families Are FULLY Responsible For
    - Intentional or malicious damage
    - Damage occurring when the iPad is not in its protective case
    - Lost, stolen, or damaged charging adapters and cables
    - Three or more incidents of accidental damage
    - Failure to return the iPad on the specified date, typically the end of each school year.

Studies of iPad 1:1 programs in other districts have shown that cracked screens are the most common form of damage. Repairing a cracked screen or touch sensor typically runs between $25 and $100 depending on the model of iPad, specific part being replaced, and market costs of the replacement part.

If it is determined that it is the responsibility of the parents/guardians to pay for damages or loss, invoices should be paid within 30 days of receipt. If bills are not cleared within 30 days, students/parents will be invoiced for labor costs as well. Invoices over 90 days may be filed with the District Magistrate. Payment plans can be setup (if necessary) by contacting the Manheim Central Business Office at 717-664-8520.