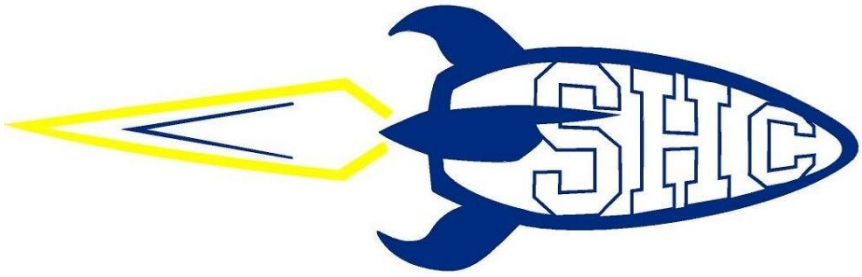
1:1
Student Device
Handbook



Southern Huntingdon
County
School District

Contents

OVERVIEW

Southern Huntingdon County School District is committed to the implementation of strategies to enhance the education of our students through our One-to-One (1:1) program. The 1:1 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-centred to student-centered personalized learning environments which focus on high academics and the integration of 21st century skills.

The 1:1 program is occurring as a result of the District's Five-Year Technology plan, which included a goal to create a 1:1 program. Key components of the 1:1 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 blended learning. The District continues to provide our educators with ongoing professional development for best practices in using technology and new instructional strategies.

Students in grades K-12 will be participating in the 1:1 program. Students in grades 6-12 will have a device assigned that they will take home every night. The tablet/laptop has all of the necessary software needed for their curriculum and learning goals in addition to an internet filter that is active at both school and anywhere the students access the Internet.

Costs associated with the 1:1 program are offset with the reduction in technology costs, 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 in-school technology use, however; damage to technology by the student, willfully or accidentally, shall incur a fee.

1:1 Student Questions and Answers

Q: What are the goals of the 1:1 Program?

- To promote an environment where students have access to anytime-anywhere learning.
- To equip teachers with tools necessary to differentiate instruction for personalized learning.
- To prepare students with essential digital literacy skills needed to compete in a global workforce.
- To provide for deeper learning opportunities that reach beyond a traditional classroom setting.
- To encourage & motivate students to think critically and apply 21st Century Learning Skills needed for real-world innovation.
- To cultivate self-directed life-long learning, responsibility, & collaboration using digital communication and productivity tools.

Q: What is the 1:1 program?

It is a District program to provide students with a District-owned device as a tool to help integrate new instructional strategies in order to integrate 21st century learning skills in the classroom.

Q: How will the 1:1 program help students academically?

Preliminary educational research shows that when students effectively use computer devices in the classroom, students are provided with deeper learning experiences and are more effectively able to apply 21st Century Learning Skills. To compete in our global economy and equip our students for post-secondary education, 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 globally competitive demands which will allow students to manage their own learning at any time and any location. This program is designed to enhance current teaching/instructional strategies through the effective use of technology and 21st Century teaching methods.

Q: When will I receive the District-issued device?

Students will receive their device within the first two weeks of school, barring any manufacturing delays that are out of the District's control.

Q: Can I use a carrying case?

The District does not provide cases but strongly encourages students to use a carrying case.

Q: Who owns the District device?

The Southern Huntingdon County School District owns the District device. It is therefore very important that you take good care of it, leave the tags in place, don't damage it (which includes stickers, labels, nail polish, etc.) or write on it, as it is District property.

Q: May I take the District device home?

Students in grades 6-12 may take the device home. The Parent/Student Agreement form is to be completed, the Responsible Use Policy is to be signed, and the insurance form returned.

Q: May I access the Internet and my printer at home with the District device?

You may use the device at home and access your home internet in support of academics. There is a filter installed, however; parents should not rely on the filter as a catch all for inappropriate content. There is no such thing as a perfect filter. Under no circumstances should anyone try to tamper with the installed filter. Any attempts to remove or manipulate the filter will be considered a violation of the acceptable use policy. You will not be able to print to a home printer because the installation of your printer driver requires that you have administrative rights to the District laptop. Students are prohibited from having administrative rights to the District devices.

Q: What do I do if my District device doesn't work or is damaged?

Please report to the Technology Department as soon as possible. It's important not to delay as one problem can lead to another if not solved right away. If your computer is damaged, we will evaluate the damage and determine if a fix is necessary for proper operation. If repair is needed, we will fix it or send it out for repair. If it needs to be repaired, we will loan you a device to use until it's returned. Under no circumstances should you or anyone else take the device to a third party to try to fix. District provided laptops are property of the school District and District personnel shall fix related problems.

Q: May I put games or software on the District device?

No. Games or other software must be installed by the District. Software shall not be installed unless it is in support of the curricular goals and objectives of the District. Any non-installable games, software, or music that you have legally purchased may be put on your device, however; if you install anything on the computer that causes the computer to stop functioning, it will be reformatted. This means all files will be lost. The District is not responsible for any loss incurred for personally owned software, games, or music. Under no circumstance shall students have pay-for games, pay-for software, or music on the device in which you have not purchased. Unlicensed/illegally obtained media is prohibited and may result in legal action for copyright infringement and/or software privacy by the licensed owners of such.

Q: How do I carry my device?

The hinge on a laptop can become damaged if you carry it open and the risk of tripping or dropping the computer exists if you don't have it in the case. For an iPad, the cover should always be snapped on to protect the screen when transporting the device.

Q: Is there anything special I should do with my District device at home?

Just be sure you plug it in overnight so you come to school with a fully charged battery. You will be responsible if your device is not ready for classwork every day. It will be viewed as if you have left your textbook at home if your device is not charged and ready to go every morning.

Q: How long will I have the District device?

The device is yours to use during the school year. Prior to the beginning of summer, we will collect the devices and reformat them. Once school starts up again, you will receive a District device.

1:1 Program Laptop Responsible Use Policy

As the Southern Huntingdon County 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 device 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 device include:

1. The use of software, hardware, email, and the intranet/internet for academic purposes.

2. Accessing the Internet to retrieve information from libraries, databases, and websites to enrich and expand learning opportunities.

3. E-mail and online work to facilitate communication and for school projects and/or assignments.

4. 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 without teacher consent.

    - Transmission of any material in violation of any U.S. or state law, including but not limited to: copyrighted material without the permission of the author or creator; threatening, harassing, pornographic, or obscene material; or material protected by trade secret.

5. 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 Southern Huntingdon County School District.

6. The use of personal finance, political, or commercial gain, product advertisement, or the sending of unsolicited junk mail or chain letters is prohibited.

7. The forgery, reading, deleting, copying, or modifying of electronic mail messages of other users is prohibited.

8. The creation, propagation, and/or use of computer viruses or other malicious logic is prohibited.

9. Deleting, examining, copying, or modifying files and/or data belonging to other users are prohibited.

10. Unauthorized copying/installation of software programs belonging to the school are prohibited.

11. Intentional destruction, deletion, or disablement of installed software on any device is prohibited.

12. 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.

13. Destruction of hardware or software or attempts to exceed or modify the parameters of the system is prohibited.

14. 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 Southern Huntingdon County School District is 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 devices as well as devices 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 the District 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 Usage

Liability

The laptop is issued to the student who, with his or her parents or legal guardians, is the only authorized user of that computer. Although each student accepts responsibility for the care and use of the device, the device remains the sole property of the District. The District owns licenses for the software installed on the device. Under no circumstances may any of this software be transferred to any other device. In the event of damage to the laptop or power cord caused by vandalism or negligence, parents will be charged for the required repair or replacement.

Daily Use

Students are expected to arrive at school every day with their device battery fully charged. Students that fail to have their battery fully charged will be subject to appropriate disciplinary action.

Network Access

Use of the District network is governed by the District Acceptable Use Policy. Students have a personal folder in the cloud accessible only to them and District personnel. They also have access to group folders, shared by other students and teachers.

Web Access and E-mail Access

Students will utilize their school issued e-mail account to communicate to teachers and administrators. Under no circumstances shall students use their own personal email to communicate with District employees.

Power adapters

On a case by case basis, loaner batteries and power adapters are available in the library. A student may borrow a charger during the day by signing it out. It must be returned at the end of the day.

Care

Devices should not be left in temperatures below 35 degrees or above 90 degrees. Food, drinks, or pets should not be near the device to avoid damage. Rain, wet hands, and high humidity are risky to devices and should be avoided. Devices are not to be left in a vehicle; this encourages theft and exposes the device to temperature changes outside of their operating limits. This is considered negligence (please refer to the section titled Liability). Students may not personalize the device, case, or peripherals in any way. This constitutes vandalism and will be subjected to appropriate disciplinary action and where appropriate, monetary restitution.

Loaner Devices

Should the device become inoperable, a student will be issued a loaner device while their device is being repaired. The loaner device assumes all aspects and policies of the student originally issued device.

Backing Up

Students are responsible for backing up their personal files to their District home folder located in the cloud. The District or school is not responsible for students who lose files or data because they failed to save it in the right place. If a device fails or has a virus, it will be wiped clean and imaged. The Technology Department will not take any measures to save or recover data stored on the device.

Troubleshooting

Students should report any device problems (i.e. printing, software issues, syncing, etc.) to the classroom teacher or to the Technology Department as soon as possible. Students are prohibited from trying to troubleshoot any hardware problem. Under no circumstances shall the District owned device be taken to a third party for repair or troubleshooting. All issues relating to the functionality of the laptop shall be reported to the Technology Department. Failure to abide by this policy, regardless of the resolution, will be considered vandalism and or negligence. (Please refer to the section titled Liability)

Damage / Theft

All physical damage to the device must be reported immediately to a responsible adult-either at home or at school. It must be reported to the Technology Department no later than the next school day. The Technology Department will arrange for repair and a loaner as needed. Accidental or intentional damage is not covered by our warranty. The parent/student is responsible for all damages to District issued laptops and subject to a cost of repair or replacement. Insurance can be purchased to help offset the cost of accidental damage.

Guidelines for Safe and Responsible Use

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 Southern Huntingdon County 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 stomach aches.

   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.

Device Use and Classroom Routines

Lockers

- Your device should be stored at all times in your locker or a charging station, if it is not stored with you. If an elementary student, it should be stored in the classroom cart.
- Never pile things on top of your device.
- Never leave your device at the bottom of the locker.
- Never leave the locker set to open without entering the combination.

Hallways

- Never leave the device unattended for any reason.
- Close the lid of your laptop before you change classes to put the computer to sleep. Do not shutdown the computer.

Classroom Habits

- Center the device on the desk.
- Close the lid of the laptop before standing up.
- Lock the computer before walking away from it.
- Do not put any foreign objects (i.e. pencil) on the laptop keyboard (if the lid closes, it will break the screen).
- Follow all directions given by the teacher.

Care of Device at Home

- Charge the device fully each night.

- Use the device in a common room of the home.
- Store the device on a desk or table – never on the floor!
- Protect the device from:
    - Extreme heat or cold
    - Food and drinks.
    - Small children.
    - Pets.

Traveling To and From School

- Do not leave the device in a vehicle.
- Use your carrying case by the handle or shoulder strap.
- If ever in a situation when someone is threatening you for your device, give it to them and tell a staff member as soon as you arrive at school.
- Stolen devices are to be reported to the local police department as soon as possible.