1:1 HANDBOOK

2021/2022 EDITION

GREENVILLE AREA SCHOOL DISTRICT

GREENVILLE ELEMENTARY SCHOOL
GREENVILLE JUNIOR/SENIOR HIGH SCHOOL

STUDENT & PARENT/GUARDIAN 1:1 HANDBOOK & EXPECTATIONS

Contents

Overview

The vision and ultimate goal of Greenville Area School District's use of technology is to create an environment where students and faculty use technology to foster critical thinking, support the curriculum, improve problem solving, communication, and collaboration in all classrooms for every student. As part of this vision, the District is creating a 1:1 program. Student participation in this program will enhance their learning and prepare them for their post K-12 endeavors.

Device Distribution

Distribution will occur at the start of each school year. During distribution, students, along with a parent/guardianwill be required to sign a usage agreement.

- Students in grades 4 – 6 will be assigned a Google Chromebook for **in-school use** only
- Students in grades 7 – 12 will be assigned a Google Chromebook to be used **in school and at home**.

Home Use and Classroom Routines

General Usage Guidelines

- While on school property, your device should be kept with you.
- **Keep the case on at all times.** Students are not permitted to remove the case for anyreason.
- Keep items off of the device. Avoid placing any object on top of the device that maycause damage.
- **Do not apply any stickers to your device or case.** This will be considered vandalism
- **Do not draw on or mark your device or case in any way**. This will be consideredvandalism

Classroom Habits

- It is at the teacher's discretion if he/she wants the students to use the device during that period
- Keep the device flat on the center of the desk
- Close the device lid (if applicable) before you stand up
- Never leave the device unlocked. If you leave class (ex: bathroom break), log out ofyour device

Care of the Device While at Home

- Charge the device every night. Students are provided a charger with their device, which must be taken home. Their device should be plugged in to charge every night.
- Use the device in a common room of the home
- Keep the device on a desk or table. Never place the device on the floor
- Protect the device from:
  - Extreme heat or cold

- o Food and Liquids
- o Small Children
- o Pets
- o Smoking Environments
- o Other potential hazards

Traveling to/from School

- Do not leave the device in a vehicle
- Devices that are lost or stolen while on school property should be reported to a Teacher or Principal immediately.
- Devices stolen while off of school grounds should be reported to the police. A copy ofthe report should be provided to the school Principal as soon as possible.

Damaged Equipment

Parents/Guardians are required to cover costs for any damaged equipment at a rate indicated by the chart below.

Student Lunch Qualification	Tier 1 Damage	Tier 2 Damage	Tier 3 Damage
Free Lunch	$20.00	$30.00	$75.00
Reduced Lunch	$20.00	$30.00	$100.00
Full Pay Lunch	$20.00	$40.00	$150.00

*No return of device will constitute a $250.00 charge.

*Tiers are defined as below:

- Tier 1: Power Cord, Keyboard, Etc.

- Tier 2: Battery, Screen, Touchpad, Etc.

- Tier 3: Chromebook replacement

It is the responsibility of the parents/guardians to pay for any damage or loss to the device. Failure to pay for damages 30 days after receipt of an invoice may result in charges filed with the District Magistrate.

Acceptable Use Policy

Purpose

The Greenville Area School District believes every child is a candidate for greatness, therefore our mission is to equip all students with knowledge, competencies, and desire to face the challenges necessary to achieve fulfillment in a global society. The Library/Media Center is

committed to providing opportunities and resources for students to access, use evaluate, and create information using traditional and electronic resources.

The purpose of this document is to establish a protocol for administrative, faculty, student, and community use of the Internet in the Greenville Area School District.

The Board supports the use of the Internet and other computer networks in the district's instructional program in order to facilitate learning and teaching through interpersonal communications, access to information, research and collaboration.

The use of network facilities shall be consistent with the curriculum adopted by the school district as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

Authority

The Internet is a way of organizing and delivering information over electronic networks that involve creation of one site that can then be linked to one or more sites. The World Wide Web, a graphical interface to the Internet, allows for the inclusion of pictures, videos, and sounds, text, animation and computer program code. Information can be in full color and can be constantly changing.

Please keep in mind that the Internet is very interactive and makes it possible to send and receive any type of information that can be digitized.

The electronic information available to student and staff does not imply endorsement of the content by the school district, nor does the district guarantee the accuracy of information received on the Internet. The district shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.

The school district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.

The district reserves the right to log network use, monitor electronic mail and fileserver space utilization by district users, while respecting the privacy rights of both district users and outside users. The district reserves the right to restrict utilization of unauthorized hardware.

The Board establishes that the use of the Internet is in accordance with all other district resources established for students. The free use of the Internet may be restricted to appropriately match individual student needs. Failure to comply with regulations may result in regulation of resources access, or civil or criminal action under Pennsylvania or federal law.

Delegation of Responsibility

Users should have a clear educational or instructional purpose. Users must adhere to copyright laws.

Users must take responsibility for having access to vast services, sites, systems, and people. As a user of the network, users will be allowed access to other networks or computers. Each network or system has its own set of policies and procedures. Users must abide by the policies and procedures of these other networks/systems.

Users are cautioned that it is against the law to commit crimes via the electronic network and that the appropriate authorities will be contacted.

The content and maintenance of a user's electronic mailbox is the user's responsibility. As such, the user must be aware that the Electronic Communications Privacy Act places

electronic mail in the same category as messages delivered by the US Postal Service. This mean that tampering with electronic mail, interfering with or intercepting delivery of mail, and the use of electronic mail for criminal purposes may be a felony offense.

Central and network computer access are protected by password security. Users must follow established guidelines for network security.

Any infractions will be dealt with using the discipline code in place at the school. This information will be updated annually and shared with the student body.

Guidelines

Security

Protect yourself by not divulging your password to others. You will need to change your password on a regular basis. If another user should gain access to your password, change it immediately and report the breach in security to the system administrators.

Users are not to use a computer that has been logged in under another user's name.

The district has curriculum in place to educate all students on appropriate online behavior, including interacting with other individuals on social networking web sites, in chat rooms, and cyberbullying awareness and response.

Maintenance

The user should check electronic mail on a regular basis, and delete unwanted messages immediately.

The contents and maintenance of users own storage area is the user's responsibility. As such, the user must:

1. Keep number of files to a minimum.

2. Exercise common sense using shared resources.

3. Refrain from engaging in deliberately wasteful practices for example, printing large amounts of unnecessary items or copies of lengthy documents.

4. Limit the size and number of files transferred. File transfers can be time consuming. Files accesses should be for educational or instructional purposes only.

Ethics

A user shall not access material that is profane or obscene (pornography) or that advocates violence toward other people. Legitimate research on questionable topics must be preapproved by the faculty member and librarian supervising the assignment.

Unacceptable Use

Unlawful use of a computer is as defined but not limited to:

(a) Offense defined – A person commits an offense if he:

(1) accesses, alters, damages or destroys any computer, computer system, computer network, computer software, computer program or database or any part thereof, with the intent to interrupt the normal functioning of an organization or to devise or execute any scheme or artifice to defraud or deceive or control property or services by means of false or fraudulent pretenses, representations or promises;

> (2) intentionally and without authorization accesses, alters, interferes with the operation of, damages or destroys any computer, computer system, computer network, computer software, computer program or computer data base or any part thereof; or

(b) intentionally or knowingly and without authorization gives or publishes a password, identifying code, personal identification or other confidential information about a computer, computer system, computer network or database.Definitions – As used in this section, the words and phrases shall have the meanings given to them in the section marked "glossary."

District unacceptable/prohibited use includes, but it not limited to the following:

– Violation of any said copyright laws

– Tampering with electronic mail, interfering with or intercepting delivery of mail, and the use of electronic mail for criminal purposes (felony offense). In accordance with the Electronic Communications Privacy Act, electronic mail is placed in the same category as messages delivered by the US Postal Service. Special Note: E-mail is not private; system operators have access to all e-mail messages and the right to monitor such messages sent or received from within the school district.

– Use of district computers and/or related accounts for purposes of communicating with outside parties in the world for non-educational reasons.

– Unauthorized downloading and/or installation of software to include all programs not pre-approved by the Technology Department.

– Vandalism, as defined as deletion, or reconfiguration of data; degradation of system performance; distribution of unsolicited advertising; propagation of computer worm/viruses (including Trojans); and similar behaviors.

– Physical alteration of district equipment such as removal of any internal/peripheral hardware.

– Alteration of district system configurations such as pre-established LANs, networked computers or printers, security setups, protocol setups, established user interfaces, or sharing of devices or drives without given authority from the Technology Department.

– Purposeful accessing of inappropriate web sites containing inappropriate language, vulgar or offensive content, or pornography. The receiving or transmitting of such material through electronic mail.

Any infractions will be dealt with using the discipline code in place at the school. This information will be updated annually and shared with the student body.

Glossary

Access – To intercept, instruct, communicate with, store data in, retrieve data from or otherwise make use of any resources of a computer, computer system, computer network or database.

Computer – An electronic, magnetic, optical, hydraulic, organic or other high speed data processing device or system which performs logic, arithmetic, or memory functions and includes all input, output, processing, storage, software or communication facilities which are connected or related to the device in a system or network.

Computer Network –The interconnection of two or more computers through the usage of

satellite, microwave, line or other communication media.

Computer Program – An ordered set of instructions or statements and related data that, when automatically executed in actual or modified form in a computer system, causes it to perform specified functions.

Computer Software – A set of computer programs, procedures and associated documentation concerned with the operation of a computer system.

Computer System – A set of related, connected or unconnected computer equipment, devices and software.

Database – A representation of information, knowledge, facts, concepts or instructions which are being prepared or processed or have been prepared or processed in a formalized manner and are intended for use in a computer, computer system or computer network, including, but not limited to, computer printouts, magnetic storage media, punched cards or data stored internally in the memory of the computer.

Property – Includes, but is not limited to, financial instruments, computer software and programs in either machine or human readable form, and anything of value, tangible or intangible.

Services – Includes, but it not limited to computer time, data processing and storage functions

Liability
The 1:1 device is issued to the student who, with his or her parents or legal guardians, are the <mark>only authorized users of that device</mark>. Although each student accepts responsibility for the care and use of the device, the device remains the sole property of the district. In the event of damage to the device and accessories the student and parent/guardian may be responsible for the cost of repairs or replacement. <mark>Any damage must be reported ASAP.</mark>

Case
In instances where the student's device has been equipped with a school issued protective case, the device must be transported in the provided case at all times, especially when carrying it between classes and to and from school. <mark>Students may not personalize the district provided carrying case</mark> nor are students permitted to purchase their own case. Lost or damaged cases will be the parent/guardian's responsibility to pay for its repair or replacement. <mark>Students are not permitted to remove Chromebook cases.</mark>

Daily Use
<mark>Students are expected to arrive at school every day with their device in its case and fully charged.</mark>

Network Access
Use of the District network is governed by the District Acceptable Use Policy (Board Policy 815)

Email Access
Students may 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.

Athletics / Extra Curricular
Under no circumstances should devices be left on the practice/game field before, during, or

after practice or games. Students are responsible for damage or theft if left unsecured. Students should exercise extreme caution when taking the device to away games or other events.

Care
Devices should not be left in temperatures below 35 degrees or above 90 degrees. To avoid damage, food, liquids, or pets are not permitted near the device. Rain, wet hands, and high humidity may damage the device and should be avoided. **Students are discouraged from leaving the device in a vehicle** as this may expose the device to extreme temperatures and make it vulnerable to theft. Students may not personalize the device, district provided case, or peripherals in any way. This constitutes vandalism and may be subjected to appropriate disciplinary action and where appropriate, monetary restitution.

Loaned Devices
Should the device require repair, the student may be issued a loaner on a case-by-case basis while their device is being repaired. The loaner device assumes all aspects and policies of the student's originally issued device.

Troubleshooting
Students are encouraged to follow the "Ask 1-2-3" rule. Students should ask 2 other students for help. If the issue is still not resolved, students should then report any problems (i.e. 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 device shall be reported to the Technology Department. Failure to abide by this policy, regardless of the resolution, may be considered vandalism and/or negligence.

Damage or Theft
All physical damage to the 1:1 device must be reported immediately to a school official. The Technology Department may arrange for repair and a loaner as needed.

Headphones
The District will not be providing headphones to students for hygienic reasons. Instead, **we ask that parents/guardians purchase a pair of headphones for their child**. Any headphones that use the standard 3.5mm plug will work. We encourage you to choose unique headphones or customize them so that your child's is easily identifiable. Sharing of headphones is highly discouraged to help prevent the spread of germs.

Opt Out

Participation in the 1:1 program is mandatory for all students in grades 4 – 12. A parent/guardian may choose to decline a school owned 1:1 device for their child only if they provide a personally purchased/owned device in its place. **All students in 4 – 12 must have a 1:1 device, either school owned or personally owned.**

To opt out, the 1:1 Handbook Agreement must be completed during scheduled deployment.

An important consideration: Should your child opt-out and choose to use a personally owned device instead, please understand that software (apps) purchased by the District may not be available or distributed to personally owned devices.

Why opting out is discouraged:

- **Students who opt-out will not receive technical support** for any personally owned devices. It will be the responsibility of the student & parent to ensure the device isworking properly and effectively every day.
- **Students who opt-out will be prohibited from using any District owned Chromebook.**Normally, those enrolled in the 1:1 program have the benefit of having access to loaner devices should they encounter issues. This will not be the case for those who opt-out.
- **Students using personally owned devices are responsible to purchase any software/apps required for a class.** The District will purchase software/apps forDistrict owned devices only.

Suggestions for personally owned devices:

- Chromebooks are preferred. They can be from any major computer manufacturers such as Dell, HP, Lenovo, Samsung, etc.
- Windows laptops and Apple Laptops are discouraged due to their battery life. A student's device must have a battery life extending beyond 8 hours of continuous usage.
- Tablets, such as iPads, are not recommended. Students in grades 4 – 12 routinely use keyboards. As students progress into higher grades, they will type more and more. Although you can get keyboards for tablets, they are small, non-standard, and not suited for extensive typing.

Guidelines for Online Safety

Greenville Area School District intends 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 may meet these demands which may 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.

- Spend time with your child on-line by having them show you his/her favorite online websites and activities. Make sure your child keeps passwords secret from everyone except you.
- Instruct your child that the device 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 device screen isactively being watched by responsible adults.
- 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:
  - o To never arrange a face-to-face meeting with someone they met online;
  - o To never upload (post) pictures of themselves onto the Internet or on-line service to people they do not personally know;
  - o To never give out identifying information such as their name, home address, school name, ortelephone 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;
  - o That what they see and read online may or may not be true.
  - o 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.
  - o 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 may increase the chances that you'll hear about what's happening online.
  - o 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 may 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 let you know.
  - o 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. Remember that <u>anything that is put on the internet is permanent</u>.
  - o 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 Greenville Area 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, <u>the School District may not tolerate any form or level of bullying</u> by students. For more information, see GASD Policy # 249

- **What Is a Cyber-bully?**
  - o A cyber-bully is someone who uses Internet technology to repeatedly act cruellytowards another person over a period of time. 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 with a much larger audience observing. Online attacks can take on a life of their own: A false rumoror a cruel prank can spread quickly among classmates and live on forever in cyberspace. A fresh new attack threatens wherever there's an Internet connection, including the one place where they should feel safe: home.
  - o **A Cyber-bully might:**

- Use a phone to make repeated prank calls or send unwanted textmessages to the victim
- Post inappropriate or offensive comments to the victim's social networksite, send unkind emails or IMs to the victim
- Create a fake social networking profile to embarrass the victim
- Use a victim's password to break into his/her account, change settings,lock the victim out, or impersonate the victim
- Forward the victim's private messages or photos to others. The bully maytrick the victim into revealing personal information
- Forward or post embarrassing or unflattering photos or videos of the victim
- Spread rumors through IM, text messages, social network sites, or otherpublic forums
- Gang up on or humiliate the victim in online virtual worlds or online games

- **Five suggestions to protect your child from Cyber-bullying:**
  - Remind your child never to share his/her passwords, even with good friends
  - If your child has a bad experience online, he/she should tell you right away. Ifpossible, save the evidence in case you need to take further action
  - 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
  - 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
  - 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 theonline time to strictly academics.

- **Is your child a victim of Cyber-bullying?**
  - Most children won't tell their parents that they're being bullied because they're afraid their parents may 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 <u>nobody deserves to be mistreated</u>. Tell themthat 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.

- **If you suspect your child is involved in cyber-bullying, you might:**
  - **Contact the bully's or victim'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.
  - **Contact your school officials.** Make them aware of the problem and ask them tobe on the lookout for signs that your child is being bullied or may be bullying at school. The school counselor or principal may have strategies and/or programs in place.
  - **Look into filing a complaint against the bully if the behavior persists**. Most internetservice providers, websites (Ex: Facebook), and cell phone companies have strictpolicies against harassment. You may be able to have the bully's account revoked. For more information about cyber-bullying on Facebook, see: https://www.facebook.com/safety/bullying/
  - **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.

Elastic Clause

This handbook may not cover all possible events or situations that may occur during the school year; thus, if a situation arises that is not specifically covered in this handbook, the administration will act fairly andquickly to resolve the situation. In reaching a solution, the interest of the students, parents, school district, and community may be taken into consideration.   All terms, conditions, and definitions in this handbook is subject to change at any time for any reason when deemed necessary by District Administration or Board of Education.

1:1 Handbook Agreement

Greenville Area School District

9 Donation Road, Greenville, PA 16125   (724) 588-2500

☐ I wish to enroll my child in the 1:1 Program and I accept and understand thefollowing:

- ➔ I have read and understand the 1:1 Handbook and agree to follow all rules and expectationsregarding the use and care of 1:1 devices.
- ➔ I understand and accept financial responsibility should my child's device be damaged.

☐ I decline to enroll my child in the 1:1 Program because I am providing my child apersonally owned device and I accept and understand the following:

- ➔ I am fully responsible for my child's device including, but not limited to, ensuring the device isfully charged and in working condition each school day.
- ➔ My child's school <u>will not provide</u> technical support for personally owned devices.
- ➔ **I will provide my child with a personally owned device.**

_____   _____   _____

Parent/Guardian Name (Printed)   **Parent/Guardian Signature**   **Date**

Students:

I have read the 1:1 handbook and agree to follow **<u>all the rules</u>** it contains including, but not limited to, the following:

- ❏ I promise to take care of my Chromebook
- ❏ I promise not to put stickers on my Chromebook or mark it in any way.
- ❏ I promise to charge my device every night
- ❏ I promise to report any damage, even superficial, to the Tech Dept as soon aspossible.

_____   _____

Student Name (Printed)   **Student Signature**

This agreement is in effect during the 2021/2022 School Year.