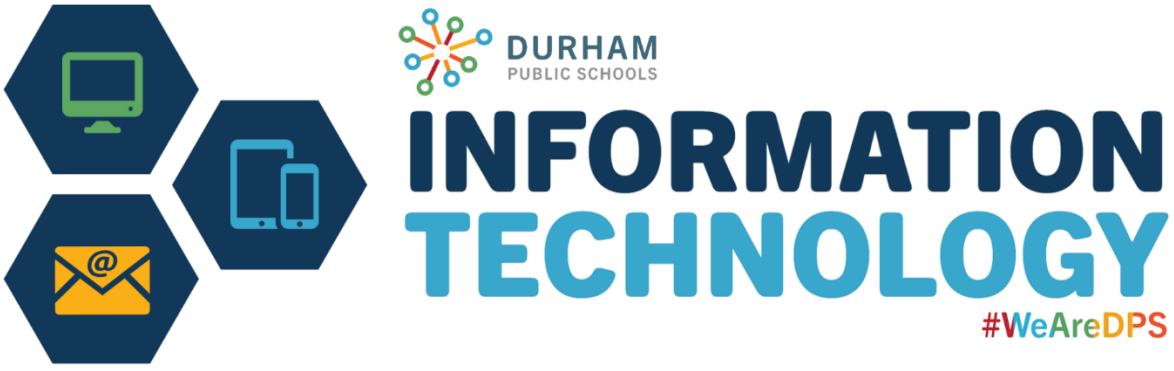
One-to-One (1:1)

Student Device

Handbook



Durham Public Schools

Contents

OVERVIEW

Durham Public Schools Information Technology Services (DPS IT) is committed to the implementation of strategies that align with the DPS Strategic Plan 1D: ***By 2023, 100% of all teachers, leaders, and staff will use technology as a tool for accelerating and personalizing student learning.***

DPS IT will enhance the education of our students through our One-to-One (1:1) program. We define 1:1 as an equitable program that provides students with technology tools that integrate new instructional strategies and 21st century learning skills in all classrooms and learning environments.

The goals of our 1:1 program include:

- Promoting an inclusive environment where students have access to anytime-anywhere learning.
- Equipping teachers and staff with tools necessary to differentiate instruction for personalized learning.
- Preparing students for essential digital literacy skills needed to compete in a global workforce.
- Facilitating deeper learning opportunities that reach beyond traditional classroom settings.
- Motivating students to think critically and apply 21st century learning skills needed for real-work innovation.
- Cultivating self-directed, life-long learning, responsibility and collaboration using digital communication and productivity tools.

Students enrolled in grades PreK-12 will be eligible to participate in the DPS 1:1 program. Participating students will have a device and/or hotspot assigned to them. The device/hotspot has all necessary software needed for students to facilitate instruction and meet their learning goals.

BOARD POLICY: TECHNOLOGY RESPONSIBLE USE

Policy Code: 3225/4312/7320

The board provides its students and staff access to a variety of technological resources. These resources provide opportunities to enhance learning and improve communication within the school community and with the larger global community. Through the school system's

technological resources, users can observe events as they occur around the world, interact with others on a variety of subjects, and acquire access to current and in-depth information.

The board intends that students and employees benefit from these resources while remaining within the bounds of safe, legal, and responsible use. Accordingly, the board establishes this policy to govern student and employee use of school system technological resources. This policy applies regardless of whether such use occurs on or off school system property, and it applies to all school system technological resources, including but not limited to computer networks and connections, the resources, tools, and learning environments made available by or on the networks, and all devices that connect to those networks, interactive whiteboards, phones and mobile devices, copiers, facsimile machines, televisions, and video-recorders.

A. Expectations for Use of School Technological Resources

The use of school system technological resources, including access to the Internet, is a privilege, not a right. Individual users of the school system's technological resources are responsible for their behavior and communications when using those resources. Responsible use of school system technological resources is use that is ethical, respectful, academically honest, and supportive of student learning. Each user has the responsibility to respect others in the school community and on the Internet. Users are expected to abide by the generally accepted rules of network etiquette. General student and employee behavior standards, including those prescribed in applicable board policies, the Code of Student Conduct, and other regulations and school rules, apply to use of the Internet and other school technological resources.

In addition, anyone who uses school system computers or electronic devices or who accesses the school network or the Internet using school system resources must comply with the additional rules for responsible use listed in Section B, below. These rules are intended to clarify expectations for conduct but should not be construed as all-inclusive.

Before using the Internet, all students must be trained about appropriate online behavior as provided in policy 3226/4205, Internet Safety.

Durham Public Schools Board of Education realizes that today's 21st Century classroom teachers must use technology in order to achieve the district's academic goals for its students. Students and employees must understand the school system technological resources and strictly comply with these requirements and acknowledging awareness that the school system uses monitoring systems to monitor and detect inappropriate use of technological resources. All students and employees must be informed annually of the requirements of this policy and the methods by which they may obtain a copy of this policy. Failure to adhere to these requirements will result in disciplinary action, including revocation of user privileges. Willful misuse may result in disciplinary action and/or criminal prosecution under applicable state and federal law. Illegal acts and communications relating to or in support of illegal activities may be reported to the appropriate authorities.

B. Rules for Use of School Technological Resources

1. School system technological resources are provided for school-related purposes only. Acceptable uses of such technological resources are limited to responsible, efficient, and legal activities that support learning and teaching. Use of school system technological resources for commercial gain or profit is prohibited. Student personal use of school system technological resources for amusement or entertainment is also prohibited, unless permitted by school personnel. Because some incidental and occasional personal use by employees is inevitable, the board permits infrequent and brief personal use by employees so long as it occurs on personal time, does not interfere with school system business, and is not otherwise prohibited by board policy or procedure. Accessing chat-rooms or instant messaging software is prohibited unless for a valid educational purpose or official school business.

2. Under no circumstance may software purchased by the school system be copied for personal use. Users must obtain permission from the technology department prior to copying or loading school system software onto any computer, whether the computer is privately owned or is a school system computer.

3. Students and employees must comply with all applicable laws, including those relating to copyrights and trademarks, confidential information, and public records. Any use that violates state or federal law is strictly prohibited. Plagiarism of Internet resources will be treated in the same manner as any other incidents of plagiarism, as stated in the Code of Student Conduct.

4. No user of technological resources, including a person sending or receiving electronic communications, may engage in creating, intentionally viewing, accessing, downloading, storing, printing, or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages, or other material that is obscene, defamatory, profane, pornographic, harassing, abusive, advocating illegal acts, or considered to be harmful to minors.

5. The use of anonymous proxies to circumvent content filtering is prohibited.

6. Users may not install or use any Internet-based file sharing program designed to facilitate sharing of copyrighted material.

7. Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).

8. Users must respect the privacy of others. When using e-mail, blogs, or other forms of electronic communication, students must not reveal personal identifying information or information that is private or confidential, such as the home address or telephone number, credit or checking account information, or social security number of themselves or fellow students. For further information regarding what constitutes personal identifying information, see policy 4705/7825, Confidentiality of Personal Identifying Information. In addition, school employees must not disclose on school system websites or web pages or elsewhere on the Internet any personally identifiable, private, or confidential information concerning students (including names, addresses, or pictures) without the written permission of a parent or guardian or an eligible student, except as otherwise permitted by the Family Educational Rights and Privacy Act (FERPA) or policy 4700, Student Records. Users also may not forward or post personal communications without the author's prior consent.

9. Users may not intentionally or negligently damage computers, computer systems, electronic devices, software, computer networks, or data of any user connected to school system technological resources. Users may not knowingly or negligently transmit computer viruses or self-replicating messages or deliberately try to degrade or disrupt system performance. Users must allow the Technology Department to scan any downloaded files for viruses. The technology department provides antivirus software for all system-owned or leased computers. Users must not disable any antivirus programs from running on those computers.

10. Users of school system computers are expected to respect school system property and be responsible in using the equipment. Users are to follow all instructions regarding maintenance or care of the equipment. Users may be held responsible for any loss or damage caused by intentional or negligent acts in caring for computers while under their control. The school system is responsible for any routine maintenance or standard repairs to school system computers. Users are expected to notify the technology department in a timely manner of any need for service.

11. School system technological resources may not be used to interfere with or disrupt other users, services, or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising; distribution of large quantities of information that may overwhelm the system; and the posting of information that will cause damage or endanger students or staff.

12. Users may not create or introduce games, network communications programs, or any foreign program or software onto any school system computer, electronic device, or network without the express permission of the technology director or designee. This prohibition pertains to freeware, shareware, copyrighted commercial and non-commercial software, and all other forms of software and files

not directly related to the instructional and administrative purposes of the school system.

13. Users are prohibited from engaging in unauthorized or unlawful activities, such as "hacking" or using the computer network to gain or attempt to gain unauthorized or unlawful access to other computers, computer systems, or accounts.

14. Users are prohibited from using another individual's ID or password for any technological resource without permission from the individual. Students must also have permission from the teacher or other school official.

15. Users may not read, alter, change, block, execute, or delete files or communications belonging to another user without the owner's express prior permission.

16. Employees shall not use passwords or user IDs for any data system (e.g., the state student information and instructional improvement system applications, time-keeping software, etc.) for an unauthorized or improper purpose.

17. If a user identifies a security problem on a technological resource, he or she must immediately notify a system administrator. Users must not demonstrate the problem to other users. Any user identified as a security risk will be denied access.

18. Teachers shall make reasonable efforts to supervise students' use of the Internet during instructional time.

19. Views may be expressed on the Internet or other technological resources as representing the view of the school system or part of the school system only with prior approval by the superintendent or designee.

C. Restricted Material on the Internet

The Internet and electronic communications offer fluid environments in which students may access or be exposed to materials and information from diverse and rapidly changing sources, including some that may be harmful to students. The board recognizes that it is impossible to predict with certainty what information on the Internet students may access or obtain. Nevertheless school system personnel shall take reasonable precautions to prevent students from accessing material and information that is obscene, pornographic, or otherwise harmful to minors, including violence, nudity, or graphic language that does not serve a legitimate pedagogical purpose. The superintendent shall ensure that technology protection measures are used as provided in policy 3226/4205, Internet Safety, and are disabled or minimized only when permitted by law and board policy. The board is not responsible for the content accessed by users who connect to the Internet via their personal mobile telephone technology (e.g., 3G, 4G service).

D. Privacy

Students, employees, visitors, and other users have no expectation of privacy in anything they create, store, send, delete, receive, or display when using the school system's network, devices, Internet access, email system, or other technological resources owned or issued by the school system, whether the resources are used at school or elsewhere, and even if the use is for personal purposes. Users should not assume that files or communications created, transmitted, or displayed using school system technological resources or stored on servers or on the storage mediums of individual devices will be private. The school system may, without notice, (1) monitor, track, and/or log network access, communications, and use; (2) monitor and allocate fileserver space; and (3) access, review, copy, store, delete, or disclose the content of all user files, regardless of medium, the content of electronic mailboxes, and system outputs, such as printouts, for any lawful purpose. Such purposes may include, but are not limited to, maintaining system integrity, security, or functionality, ensuring compliance with board policy and applicable laws and regulations, protecting the school system from liability, and complying with public records requests. School system personnel shall monitor online activities of individuals who access the Internet via a school-owned device.

By using the school system's network, Internet access, email system, devices, or other technological resources, individuals consent to have that use monitored by authorized school system personnel as described in this policy.

E. Use of Personal Technology on School System Property

Each principal may establish rules for his or her school site as to whether and how personal technology devices (including, but not limited to smart phones, tablets, laptops, etc.) may be used on campus. Students' devices are governed also by policy 4318, Use of Wireless Communication Devices. The school system assumes no responsibility for personal technology devices brought to school.

F. Personal Websites

The superintendent may use any means available to request the removal of personal websites that substantially disrupt the school environment or that utilize school system or individual school names, logos, or trademarks without permission.

1. Students

Though school personnel generally do not monitor students' Internet activity conducted on non-school system devices during non-school hours, when the student's online behavior has a direct and immediate effect on school safety or maintaining order and discipline in the schools, the student may be disciplined in accordance with board policy (see the student behavior policies in the 4300 series).

2. Employees

Employees' personal websites are subject to policy 7335, Employee Use of Social Media.

3. Volunteers

Volunteers are to maintain an appropriate relationship with students at all times. Volunteers are encouraged to block students from viewing personal information on volunteer personal websites or online networking profiles in order to prevent the possibility that students could view materials that are not age-appropriate. An individual volunteer's relationship with the school system may be terminated if the volunteer engages in inappropriate online interaction with students.

G. No Warranties

The school system makes no warranties of any kind, whether express or implied, for the electronic information resources it is providing. The board will not be responsible for any damages suffered by users, including loss of data resulting from delays, non-delivery, service interruptions, or any other cause. The board will not be responsible for any claims, losses, damages, costs, or other obligations arising from the unauthorized use of school system electronic information resources. Use of any information obtained via the Internet is at the user's risk. The board specifically denies any responsibility for the accuracy or quality of information obtained through its service.

Legal References: U.S. Const. amend. I; Children's Internet Protection Act, 47 U.S.C. 254(h)(5); Electronic Communications Privacy Act, 18 U.S.C. 2510-2522; Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; 17 U.S.C. 101 *et seq.*; 20 U.S.C. 7131; G.S. 115C-325(e) (applicable to career status teachers), -325.4 (applicable to non-career status teachers)

Cross References: Curriculum and Instructional Guides (policy 3115), Technology in the Educational Program (policy 3220), Internet Safety (policy 3226/4205), Web Page Development (policy 3227/7322), Use of Personal Technology to Conduct School Business (policy 3228/7323), Copyright Compliance (policy 3230/7330), Student Behavior Policies (all policies in the 4300 series), Student Records (policy 4700), Confidentiality of Personal Identifying Information (policy 4705/7825), Public Records – Retention, Release, and Disposition (policy 5070/7350), Use of Equipment, Materials, and Supplies (policy 6520), Network Security (policy 6524), Staff Responsibilities (policy 7300), Employee Use of Social Media (policy 7335)

Adopted: May 24, 2017

Revised: April 23, 2020

GUIDELINES FOR USAGE

Liability

Devices and/or hotspots are issued to students who, with his or her parents or legal guardians, are authorized users of those devices. Although each student accepts responsibility for the care and use of the device, the device remains the sole property of Durham Public Schools (DPS). DPS owns the licenses for the software installed on the device and under no circumstance may any software be transferred to any other device. Device damages, vandalism, or negligence must be reported to school administration and DPS Information Technology (ITSupport@dpsnc.net) the next school day. Parent/Guardians should report device theft/loss to local police to obtain a report. Official police report must be reported to school administration and DPS Information Technology (ITSupport@dpsnc.net) the next school day.

Daily Use

DPS IT recommends the following best practices for optimum performance of Chromebooks:

- Restart the computer daily.
- Close programs when you are done.
- Don't open a lot of tabs in browser.
- Allow computer to run and install updates.

DPS IT recommends the following habits for classroom use:

- 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.

Power Adapters

DPS IT provides one power adapter with each issued device. School administrators/Tech Champions may provide loaner batteries, power adapters and/or charging stations for students who forget their issued power adapter.

Care At Home

Devices should not be left in temperatures below 35 degrees or above 90 degrees. Food, drinks, or pets should not be near devices to avoid damage. Rain, wet hands, and high humidity are risky to devices and should be avoided. Devices should be charged fully each night and should be stored on a desk or table – never on the floor. Devices are not to be left in a vehicle; this

encourages theft and exposes the device to temperature changes outside of their operating limits.

Students may not personalize the device or peripherals in any way. This constitutes vandalism and will be subjected to appropriate disciplinary action.

Troubleshooting

Students or Parent/Guardian should report all problems or issues relating to the functionality of a DPS issued device (i.e., printing, software issues, syncing, etc.) to ITSupport@dpsnc.net. Students are prohibited from trying to troubleshoot any hardware problem. Under no circumstances shall a DPS owned device be taken to a third party for repair or troubleshooting.

Loaner Devices

In the event a DPS-issued device becomes inoperable, the student, parent/guardian, or teacher should submit a service request to ITSupport@dpsnc.net or call call 919-560-3837 (Monday – Friday 7AM to 5PM). The student will be issued a loaner device while their device is being repaired. The loaner device assumes all aspects and policies of the student's orginally issued device.

FREQUENTLY ASKED QUESTIONS

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, DPS needs to provide a learning environment that integrates today's digital tools, accommodates mobile lifestyles, and encourages students to work collaboratively in team environments. DPS' 1:1 technology program is designed to allow students to manage their own learning at any time and any location, while enhancing 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 week of school, barring any manufacturing delays that are out of the District's control.

Q: May I decorate the District provided device?

No. you may not decorate a DPS Chromebook/hotspot. Devices that have pencil/pen/magic marker writing on them, stickers or any other marks on them will be viewed as vandalism.

Q: Who owns the District issued device?

Durham Public Schools owns the device; however, it is very important that students take good care of it, leave the tags in place, and not damage or write on it, for as it is assigned to them.

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. While there is a filter installed, parents should not rely on the filter as an alternative to monitoring for inappropriate content. If you become aware of an inappropriate site(s) that is accessed using a district issued device, please submit a request to ITSupport@dpsnc.net to block inappropriate content. 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 Technology Responsible 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 device. Students are prohibited from having administrative rights to district devices.

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

Please report to ITSupport@dpsnc.net or call 919-560-3837 (Monday – Friday 7AM to 5PM) as soon as possible. If your computer is damaged, we will evaluate the damage and determine if repair is necessary for proper operation. If it needs to be repaired, we will loan you a device to use until it's returned. Under no circumstances should the device be taken to a third party for repairs.

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

Games or other software must be installed by DPS IT personnel only. Software shall not be installed unless it is in support of the curricular goals and objectives of DPS. DPS 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. Unlicensed/ illegally obtained media is prohibited and may result in legal action for copyright infringement and/or software piracy by the licensed owners of such.