DISTRICT OF COLUMBIA
PUBLIC SCHOOLS

DCPS Student and Staff Technology and Network Acceptable Use Policy

I. PURPOSE AND SCOPE

DC Public Schools (DCPS) provides students and staff with access to internet, data and network systems (DCPS network). DCPS also provides students with access to computers, tablets, devices, and other technology such as printers (DCPS devices or technology). The DCPS network and DCPS technology are provided to staff for planning, instructional, and administrative purposes; and provided to students for educational, research, and career development purposes. The purpose of this DCPS Student and Staff Safety and Acceptable Use Policy for Internet and Technology is to:

1) To establish standards for the acceptable uses of the DCPS network and DCPS technology;
2) To prevent unauthorized and unlawful uses of the DCPS network and DCPS technology; and
3) To comply with the Children's Internet Protection Act of 2000 (CIPA), the Children's Online Privacy Protection Act (COPPA), the Protecting Students Digital Privacy Act, and all other applicable laws, regulations, policies and procedures.

This policy is applicable to all DCPS students and staff (collectively, users) and rescinds the DCPS Student Safety and Use Policy for Internet and Technology (2009).

II. AUTHORITY AND APPLICABLE LAW[1]

Source	Citation
Federal Law (USC)	- Children's Internet Protection Act (CIPA), codified at 47 U.S.C. § 254(h)(5) - Children's Online Privacy Protection Act of 1998 (COPPA), codified at 15 U.S.C. § 6501 *et seq*. - Neighborhood Children's Internet Protection Act, codified at 47 U.S.C. § 254(l)
Federal Regulations (CFR)	- Children's Online Privacy Protection Rule, 16 CFR Part 312
District of Columbia Law (DC Code)	- Protecting Students Digital Privacy Act of 2016, D.C. Law 21-218, codified at D.C. Code 38-831.01 *et seq*.
District of Columbia Municipal Regulations (DCMR)	- 5-B DCMR § 2500 *et seq*. – Student Discipline - 6-B DCMR § 1610 – Employee Progressive Discipline

III. KEY TERMS AND DEFINITIONS

[1] Nothing in this policy shall supersede federal, state, or local law.

DCPS Staff means all DCPS employees (full or part-time), contractors, agents, representative or volunteers, or any other individual acting on behalf of DCPS, who have access to the DCPS network and DCPS technology.

DCPS Network means internet, data, and network systems provided by DCPS to all DCPS students and staff.

DCPS Technology means computers, tablets, devices, and other technology provided by DCPS to all DCPS students and staff.

Personal Information means information that, when used alone or in combination with other relevant data, can identify an individual. Personal information includes, but is not limited to, full name, home or other physical address, screen name or username where it functions as online contact information, and a photo, audio, or video file containing an individual's image or voice.

Suspension means the temporary removal of a student from the student's regular class schedule as a disciplinary consequence, during which time the student either remains on school grounds under the supervision of school personnel or the student is not allowed on school grounds.

Expulsion means the removal of a student from the student's school of enrollment for disciplinary reasons for the remainder of the school year or longer.

Progressive Discipline means an employee disciplinary system that provides a graduated range of responses to employee performance or conduct problems. DCPS' progressive discipline steps include verbal counseling, reprimand, corrective action, and adverse action.

IV. REQUIREMENTS

A. General

DCPS provides and authorizes the use of the DCPS network and DCPS technology to staff and students. By providing and authorizing use of technology resources, DCPS does not relinquish control over materials on the systems or contained in files on the systems. Except as described below, there is no expectation of privacy related to information stored or transmitted over the DCPS network or in DCPS systems and DCPS reserves the right to access, review, copy, store, or delete any files stored on DCPS technology or in DCPS network accounts; and all communication using the DCPS network. Electronic messages and files stored on DCPS computers or transmitted using DCPS systems may be treated like any other school property. DCPS staff may review files and messages to maintain system integrity and, if necessary, to ensure that users are acting responsibly. All student accounts created by DCPS for students or created by students at DCPS request may be monitored by DCPS staff.

B. Network, Email, and Applications

1. Network

The DCPS network and DCPS technology are provided to staff for planning, instructional, and administrative purposes; and provided to students for educational, research, and career development purposes. The DCPS

network allows staff and students internal access to DCPS information and resources, DCPS-approved applications, and external access to the internet. Access to the DCPS network, including the internet is provided to students solely to support student education, research, and career development. Use of the DCPS network is a privilege, not a right. Staff and students who violate any part of this policy or related policies may be subject to cancellation of their privileges to use the DCPS network and possible disciplinary actions.

Network access and bandwidth is provided to schools for academic and operational services. DCPS reserves the right to prioritize network bandwidth and limit certain network activities that are negatively impacting academic and operational services. Network users are prohibited from using the DCPS network to access content deemed inappropriate or illegal, including but not limited to content that is pornographic, obscene, illegal, or promotes violence.

DCPS makes no guarantee that the functions or quality of the network services it provides will be free of errors or defects. DCPS is not responsible for any claims, loss, damages, costs, or other obligations arising from use of the network or accounts. Any charges an individual incurs due to network use will be borne solely by the individual. DCPS is not responsible for the accuracy or quality of the information obtained through use of the system, unless the information is obtained from the DCPS website or the District of Columbia Government website. Any statement accessible on the network or the Internet is understood to be the author's individual point of view and not that of DCPS, the District of Columbia Government, their affiliates, or employees.

2. Filters and Monitoring

As required by the Children's Internet Protection Act (CIPA), DCPS is required to protect students from and educate them about online threats, block access to inappropriate content, and monitor Internet use by minors on school networks.[2]

DCPS uses technology protection to block or filter internet access to visual depictions that are obscene, pornographic, or harmful to minors. Except as described in section IV.G below, DCPS reserves the right to supervise and monitor students' online activities and to access, review, copy and store or delete any electronic information or files and disclose them to others as it deems necessary. Students should have no expectation of privacy regarding use of DCPS property, the DCPS computer network or the use of the Internet, files, or email while within the network, except as established by the Protecting Students Digital Privacy Act (see Section IV.G below).

DCPS also uses a safety management system to analyze and review content found in online student file storage, inbound and outbound DCPS email, DCPS email attachments, and links to websites. This system blocks potentially harmful content and images and notifies DCPS personnel under emergency circumstances such as threat or violence to self or others.

3. Applications

The Children's Online Privacy Protection Act (COPPA) requires operators of websites or online services directed to children under 13 years of age, and operators of other website or online services that have actual

[2] 47 U.S.C. 254(h)(5)(B).

knowledge that they are collecting personal information online from a child under 13 years of age, to obtain verifiable parental consent before collecting, using, or disclosing personal information from children.[3]

When DCPS contracts with a website or online service to collect personal information for the use and benefit of DCPS, and for no other commercial purpose, the operator may obtain consent from DCPS and is not required to obtain consent directly from parents.[4] DCPS will provide parents notice of consent provided by DCPS through an electronic inventory on the DCPS website of all COPPA-compliant websites and online services DCPS contracts with and/or requires students under 13 to access, including a link to each operator's privacy policy, and a process through which parents may opt out. DCPS staff are not permitted to require students under 13 to access non-COPPA compliant sites and services, or any COPPA-compliant sites and services where parents have opted out of the collection of personal information.

4. Access Control

DCPS implements security access control measures to ensure appropriate network and technology access for all DCPS users and to lock out unauthorized access and potential threats. DCPS assigns student access to the DCPS network, DCPS email accounts, and DCPS authorized applications based on grade level and/or school or teacher request as follows:

- *Network*: While all students are provided with personalized credentials and passwords, All students **must** use their personalized credentials and passwords to log in.
- *Email*: Students in grade 9 and above are provided with DCPS email accounts after the successful completion of a Digital Citizenship course. Students in other grade levels may be provided with DCPS email accounts after the completion of a Digital Citizenship course at the discretion of DCPS staff. Students with certain disabilities should have access to the testing and classroom accommodations listed in their IEP to complete the digital citizenship course, which may include read aloud and repetition of directions, reduced readability of the text and simplification of content, and other accommodations.
- *Applications*: DCPS provides access to a standard set of approved applications for all DCPS staff and students. Staff access is provided based on job responsibility and for some applications based on principal request. Students are provided access to an approved suite of applications. Students may receive access to other applications beyond the approved suite by school and teacher request.

5. Passwords

DCPS users are required to adhere to DCPS password requirements when logging into school computers, networks, and online systems. Users are not authorized to share their password or any other DCPS student or staff member password they may have learned, whether innocently or in violation of this policy, and must use extra caution to avoid email scams that request passwords or other personal information. Students in the designated grades are required to participate in a Digital Citizenship course to learn how to avoid these scams and other good cyber practices

[3] *See* 16 CFR Part 312.5. This requirement also applies to any material change in the collections, use, or disclosure practices to which a parent has previously consented. Operators must also give parents the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties.

[4] More information about complying with COPPA is available from the Federal Trade Commission here: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

Adults who support student with disabilities may require access to their passwords if the students is not able to physically input or recall the password.

Penalties for prohibited use of passwords may result in restrictions to network access or cancellation of accounts. Additionally, violations may result in disciplinary and/or legal action for students including suspension, expulsion, and criminal prosecution.

6. Online Safety, Digital Citizenship, and Cybersecurity

DCPS will provide students with annual lessons in digital citizenship and online safety. DC Government, the DC Office of the Chief Technology Officer and/or DCPS may require staff to complete employee trainings related to cybersecurity or related topics. Failure to timely complete those trainings may result in progressive discipline.

7. Access to Telehealth/Telemedicine

DCPS staff and students are permitted to access telehealth sessions on DCPS devices. Although the District has no intention of actively monitoring telehealth sessions, federal law requires that school districts scan data and monitor student activity on school-issued devices, which could include medical records or other documents saved to the devices' hard drives. **Live telehealth sessions will not be monitored.** If confidential data is stored on the devices' hard drives, it will be purged upon the devices' return to inventory.

8. Videoconferencing

Videoconferencing occurs when DCPS staff and students in different locations communicate with each other in real-time sound and vision using a videoconferencing application. Teachers and staff may record the videoconference and make it available to themselves and the student later.

Staff should not disclose personally identifiable information about students during videoconferencing sessions.

Teachers and students should report any inappropriate behavior or concerning behavior that may occur during a videoconference to the DCPS Office of Integrity.

Students and staff must continue to follow the DCPS Employee Rights and Responsibilities Policy, the DCPS Social Media Policy, and any other applicable policy regarding staff-student interactions.

C. Technology (Including Computers, Laptops, Tablets)

1. Device Support

DCPS provides basic installation, synchronization, and software support for DCPS-issued electronic devices. Devices must be connected to the DCPS network on a regular basis to receive software updates and/or for inventory purposes. Password protection is required on all DCPS-issued electronic devices to prevent unauthorized use in the event of loss or theft.

2. Damage, Loss and Theft

Staff are stewards of DCPS technology and may be held financially responsible for damage, loss or theft of property due to negligence. Examples of negligence include, but are not limited to:

- damage as a result of leaving DCPS technology in a vehicle or other location that is exposed to heat, cold, or moisture;
- damage due to spilled beverages or food; or
- theft as a result of leaving DCPS technology unattended or in an unsecure location.

Students must take reasonable measures to prevent a device from being damaged, lost or stolen. If a student device is damaged, DCPS staff at the student's school may investigate to determine if damage to devices resulted from negligence or intentional acts of vandalism. This investigation should take into factors that impact whether the student is able to understand proper device care including age and any disability. Examples of damage resulting from negligence or intentional acts of vandalism include but are not limited to:

- Drawing on devices using a permanent marker, etching words/graphics using a sharp object, or animal bite marks on the device;
- Damage in several locations due to devices being mishandled or not cared for (e.g., screen is cracked, keyboard is damaged, keys are missing and the outer laptop casing shows signs of impact in several locations or laptop/tablet is returned in several pieces;
- Forceful damage**,** damage caused by impact using sharp or hard object(s), or damage by object(s) being jammed into the laptop USB or power ports;
- Repeated pattern of damage if the student has caused damage to three or more devices in a school year; or
- The device was completely submerged in water or other liquids.

Disciplinary responses for damage to devices that resulted from negligence or intentional acts of vandalism will be determined under the DCPS discipline regulations and policies and this Acceptable Use Policy. Students may not be penalized for damage resulting from normal wear and tear or unintentional accidents. Examples of damage resulting from normal wear and tear include but are not limited to:

- Missing key(s) on the keyboard.
- Cracked screen because of dropping the device.
- Damage isolated to a small portion of the device such as corner/sides of the screen which could have happened by dropping the device.
- Accidental liquid spills on the keyboard.
- Damage caused by a power surge.

In the event DCPS technology is lost, stolen, or damaged, users are required to immediately notify DCPS staff. DCPS will take all reasonable measures to recover the lost property and to ensure the security of any information contained on the device. DCPS may choose to deploy location tracking software on devices for the purpose of locating devices identified as lost or stolen or remotely disable devices that are not returned upon request

1. Overnight or At-Home Use by Students

DCPS school staff may provide students with DCPS devices for overnight or at-home use at the discretion of the school's principal or the IEP team where appropriate, and in accordance with this policy. DCPS students and a parent/guardian must sign the attached Student Acceptable Use Agreement prior to being assigned a device for overnight or at-home use. DCPS school staff must adhere to privacy requirements under the Protection of Student Digital Privacy Act and parents and students should be aware that these devices may be accessed by DCPS staff.[5]

Technology that is classified as assistive technology may go home with the student if the IEP team, not the Chancellor or their designee, determines that the student requires these supports to complete educational tasks at home (e.g. homework, communication). This is pertinent when students use assistive technology provided by the schools directly. The IEP team has a home use form for technology students and families can use for this purpose.

D. Conduct and Acceptable Use

By using the DCPS network and DCPS technology, staff and students agree to follow all relevant DC Government, DC Office of the Chief Technology Officer, and DCPS regulations, policies, and guidelines. Staff shall report misuse or breach of protocols to teachers, appropriate supervisors, administrators, or Central Office employees as soon as they are aware of the misuse or breach.[6]

Users shall not use the DCPS network or DCPS technology, including access to the internet, intranet, collaboration tools, bulk communication tools, social media, or email to use, record, share, upload, post, mail, display, store, or otherwise transmit in any manner, any content, communication or information that, among other unacceptable uses:

1. Is hateful, harassing, threatening, libelous or defamatory;
2. Is offensive or discriminatory to persons based on race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, gender identity or expression, familial status, family responsibilities, matriculation, political affiliation, genetic information, disability, source of income, status as a victim of an intrafamily offense, place of residence or business, or status as a victim or family member of a victim of domestic violence, a sexual offense, or stalking;
3. Constitutes or furthers any criminal offense, or gives rise to civil liability, under any applicable law, including, without limitation, U.S. export control laws or U.S. patent, trademark or copyright laws;
4. Constitutes use for, or in support of, any obscene or pornographic purpose including, but not limited to, the transmitting, retrieving or viewing of any profane, obscene, or sexually explicit material;
5. Constitutes use for soliciting or distributing information with the intent to incite violence, cause personal harm or bodily injury, or to harass, threaten or stalk another individual;
6. Contains a virus, trojan horse, ransomware or other harmful component or malicious code;
7. Constitutes junk mail, phishing, spam, or unauthorized broadcast email;
8. Violates the security of any other DCPS device or network, or constitutes unauthorized access to any DCPS device or network or attempts to circumvent any security measures;
9. Obtains access to or provides an unauthorized third party with access to another user's DCPS

[5] Specifically, DC Code § 38-831.03(a).

[6] More information about filing reports and complaints is available Section V.

network account, files or data, or modifies their files, data or passwords;
10. Impersonates any person living or dead, organization, business, or other entity with the intent to deceive;
11. Degrades the performance of, causes a security risk or otherwise threatens the integrity or efficient operation of, the DCPS network or technology;
12. Deprives an authorized user of access to the DCPS network or technology;
13. Obtains DCPS technology or DC network access beyond those authorized;
14. Engages in unauthorized or unlawful entry into a DCPS Network system;
15. Discloses confidential or proprietary information, including student record information, without authorization or without proper security measures;
16. Discloses or transmits personally identifiable student information, videos and photographs without authorization or without proper security measures;
17. Shares confidential information about students or DCPS personnel in a manner that violates DC law, federal law, regulations, policy or guideline;
18. Shares DCPS email addresses or distribution lists for uses that violate this policy or any other DCPS policy;
19. Enables or constitutes wagering or gambling of any kind;
20. Accesses, distributes, downloads or uses unauthorized games, programs, files, electronic media, and/or stand-alone applications from the internet that may cause a threat to the DCPS Network
21. Promotes or participates in any way in unauthorized raffles or fundraisers;
22. Promotes or participates in any way in partisan political activities;
23. Promotes or participates in any way in internal political or election activities related to a union or other organization representing employees;
24. Engages in private business, commercial or other activities for personal financial gain;
25. Distributes unauthorized information regarding other user's passwords or security systems;
26. Falsifies, tampers with or makes unauthorized changes, additions or deletions to data located on the DCPS network or any school systems;
27. Accesses or uses data located on a DCPS Network for personal uses;
28. Promotes or participates in any activity or relationship with a student that is not related to academics or school-sponsored extracurricular activities, unless authorized in advance in writing by the principal and the student's parent/guardian;
29. Installs, downloads or uses unauthorized or unlicensed software or third-party system;
30. Violates the terms of use specified for a particular technology, application or DCPS network system;
31. Constitutes use that disrupts the proper and orderly operation of a school or office;
32. Engages in hacking (intentionally gaining access by illegal means or without authorization) into the DCPS network to access unauthorized information, or to otherwise circumvent information security systems;
33. Engages in inappropriate sexual conduct, including unwelcomed sexual contact, indecent exposure, transmitting sexually suggestive images, or other sexual activities; or
34. Violates any prohibition noted in this policy or any other DCPS policy.

Users shall not share their DCPS-issued device, nor their DCPS-issued network log-in information, with any other individual. Using someone else's DCPS-issued device or DCPS-issued network log-in information, permitting unauthorized users to use one's DCPS-issued device or DCPS-issued network log-in information, or facilitating the unauthorized use of any other individual's DCPS-issued device or DCPS-issued network log-in information through sharing of log-in information or any other means is strictly prohibited.

E. Student Conduct and Responsible Use

All students and parents must annually sign a Student Technology and Network Responsible Use Agreement (Student Responsible Use Agreement), found in Appendix. The Student Responsible Use Agreement outlines responsible use and prohibited activities for students using DCPS technology or accessing the DCPS network. Schools may also require students and parents to sign school-specific agreements that detail technology check in/check out processes, identify school staff with specific technology-related roles, and establish school-specific rules.

Failure to follow these rules will be addressed under DCPS student discipline regulations and policies and may result in losing access to the DCPS network or DCPS technology for increasing periods of time, provided that students are able to participate in and complete classwork through alternative means and are able to receive all necessary special education and English Learner services. In some instances, misconduct may also constitute a criminal violation.

F. Personal Media Electronic Devices

Student use of personal electronic devices on the DCPS network is not permitted without the express written authorization from the Chancellor or the Chancellor's designee. DCPS is not responsible for the maintenance and security of student personal electronic devices and assumes no responsibility for loss or theft. DCPS and the Office of the Chief Technology Officer (OCTO) and their staff are not required to provide technical support to students seeking to use personal electronic devices at school or on the DCPS network or to access personal media accounts on DCPS devices other than support with web-based, DCPS-approved applications in use on those personal devices. Except as described below in this section, DCPS reserves the right to enforce security measures on personal devices when used to access the DCPS network and remove devices found to be in violation of DCPS policy.

G. Privacy of Student Personal Media Accounts and Electronic Devices

1. School Specific Student Personal Electronic Device and Media Accounts Policies

Principals must notify students and parents in writing as to a school's student personal electronic device and media accounts policy.

2. General Privacy of Personal Media Accounts and Student Electronic Devices

Unless an exception described in section IV.G.3 is met, DCPS will not take or threaten to take action against a student or prospective student, including discipline, expulsion, unenrollment, refusal to admit, or prohibiting participation in a curricular or extracurricular activity, because the student or prospective student refused to:

- Disclose a username, password, or other means of account authentication used to access the student's personal media account or personal technological device;
- Access the student's personal media account or personal technological device in the presence of school-based personnel in a manner that enables the school-based personnel to observe data on the account or device;
- Add a person to the list of users who may view the student's personal media account or access a student's personal technological device; or

- Change the privacy settings associated with the student's personal media account or personal technological device.[7]

If DCPS or DCPS staff inadvertently receives the username, password, or other means of account authentication for the personal media account or personal technological device of a student or prospective student through otherwise lawful mean, DCPS and or DCPS staff will:

- Not use the information to access the personal media account or personal technological device of the student or prospective student;
- Not share the information with anyone; and
- Delete the information immediately or as soon as is reasonably practicable.[8]

Nothing in this section prevents DCPS from:

- Accessing information about a student or prospective student that is publicly available;
- Requesting a student or prospective student to voluntarily share specific content accessible from a personal media account or personal technological device for the purpose of ensuring compliance with applicable laws or DCPS policies, provided the request complies with requirements of this policy;
- Prohibiting a student or prospective student from accessing or operating a personal media account or personal technological device during school hours or while on school property;
- Monitoring the usage of the DCPS network; or
- Revoking a student's access, in whole or in part, to the DCPS network or DCPS technology.[9]

3. Exceptions to Privacy of Personal Media Accounts and Student Electronic Devices

DCPS staff may search a student's personal media account or personal technological device or compel a

student to produce data accessible from the student's personal media account or personal technological device under the following two circumstances.

a. Policy Violations

DCPS staff may search a student's personal media account or personal technological device or compel a student to produce data accessible from the student's personal media account or personal technological device if DCPS staff has a reasonable suspicion that the student has used or is using the student's personal media account or personal technological device in furtherance of a violation of DCPS policy **and** a reasonable suspicion that the personal media account or personal technological device contains evidence of the suspected violation.[10]

Before conducting such a search or compelling the student to produce such data, DCPS staff must:

- Document the reasonable suspicion giving rise to the need for the search or production; and
- Notify the student and the student's parent/guardian of the suspected violation and the data or

[7] DC Code § 38-831.04(a).
[8] DC Code § 38-831.04(b).
[9] DC Code § 38-831.04(e).
[10] DC Code § 38-831.04(c)(1)(A).

components to be searched or that the student will be compelled to produce.[11]

DCPS may seize a student's personal technological device to prevent data deletion pending this required notification only if the pre-notification seizure period is no greater than 48 hours and the personal technological device is stored securely on DCPS property and not accessed during the pre-notification seizure period.[12]

The search or compelled production must be limited to data accessible from the account or device or components of the device reasonably likely to yield evidence of the suspected violation and no person may be permitted to copy, share, or transfer data obtained pursuant to a search or compelled production that is unrelated to the suspected violation that prompted the search.[13]

b. Imminent Threat to Life or Safety

DCPS staff may search a student's personal media account or personal technological device or compel a student to produce data accessible from the student's personal media account or personal technological device if doing so is necessary in response to an imminent threat to life or safety.[14]

The scope of any search or compelled production must be limited to this purpose and DCPS must, within 72 hours of the search or compelled production, provide the student and the student's parent with a written description of the precise threat that prompted the search and the data that was accessed.[15]

1. POLICY IMPLEMENTATION REQUIREMENTS

All DCPS students and staff are required to comply with the requirements set forth in this policy. In order to

support its implementation, principals are expected to make staff aware of required activities and timelines on annual basis. Implementation of this policy will be reinforced through a central oversight process which includes regular data reviews, record sampling, reviews of underlying documentation, and site visits (as needed). This framework will ensure that together we build a system of continuous improvement and prevent noncompliance. For key guidance and support with questions, training, or implementation, please visit dcps.dc.gov.

DCPS is committed to serving every student with equity, excellence, transparency, and accountability. For any concerns about, or to report potential violations of, this directive, contact the Chief Integrity Officer by completing the Online Referral Form[16] or sending an email to dcps.cio@dc.gov.

2. APPENDIX

See next page: Student Technology Responsible Use Agreement

[11] DC Code § 38-831.04(c)(1)(B).
[12] DC Code § 38-831.04(d).
[13] DC Code § 38-831.04(c)(1)(C)-(D).
[14] DC Code § 38-831.04(c)(2)(A).
[15] DC Code § 38-831.04(c)(2)(B)-(C).
[16] *Available at* https://dcps.dc.gov/page/office-integrity.

Student Technology Responsible Use Agreement
School Year _____

All DCPS students must use DCPS computers and other DCPS technology ("DCPS devices") and the DCPS network responsibly, under the guidance of teachers and DCPS staff, as follows:

A. I am responsible for keeping DCPS devices in good condition.

- I will treat my DCPS device with pride and respect, taking care not to drop it.
- I will follow school rules about checking out and returning my DCPS device.
- I will not eat or drink near my DCPS device.
- I will not write, draw, or put stickers on my DCPS device.
- I will protect my DCPS device's screen by closing it when carrying it from place to place.
- I will not lean on or place anything heavy on top of my DCPS device that could damage the screen.
- I will not damage accessories such as headphones, stylus pens, and keyboards.
- I will immediately report to a teacher or staff member if my DCPS device is damaged or not working properly.
- I will not share my DCPS device or my DCPS network log-in information with any other individual.

B. I am responsible for my DCPS accounts.

- I will not share my username or password with anyone unless I am an early childhood learner or student with certain disabilities who requires parental or staffing support to use my account.
- I will save my work and log out of all of my accounts and programs when I am finished working.
- I am responsible for all activities done through my accounts.
- I will tell a teacher if I think or know someone has used my account.

C. I am responsible for helping to protect the security of the DCPS network.

- I will not download, install, or run any type of files, including music and video files, websites, software, apps, browser extensions, or media, unless a teacher gives me permission.
- I will not download or install applications or browser plug-ins to bypass the internet content filter, try to change security settings or internet content filters, or interfere with the network in any way.
- I will not insert USB drives (also known as flash drives, thumb drives, jump drives, data sticks, or other names) into my device unless specifically approved to do so by my teachers.

D. I am responsible for my use of the DCPS network.

- I will not search for, retrieve, save, circulate or display hate-based, lewd, vulgar, or sexually explicit material.
- I will not search for, retrieve, save, circulate or display images or information about weapons or illegal drugs unless a teacher gives me permission as part of a school assignment.
- I will not use the DCPS network to engage in any illegal or criminal acts, including, but not limited to, gang or crew activity, threatening the physical safety of another person, or computer hacking.
- I will not access online games unless these activities are related to a school lesson or coursework and a teacher or staff member is supervising the activity.
- I will not access social media, messaging apps, or group chats unless it is related to schoolwork and a teacher gives me permission. This includes, but is not limited to, Facebook, Twitter, Instagram, TikTok, Snapchat, WhatsApp, Kik, Telegram, and Tumblr.

E. I am responsible for my language and how I treat other people online.

- I will not create, display or transmit any images, sounds, or messages, or other material that are sexually explicit, pornographic, obscene, or use profane language.
- I will not bully, harass, threaten, or intimidate other people by sending, sharing or posting hateful, harassing, derogatory, or discriminatory messages.

F. I am responsible for being honest while I am online.

- I will not pretend to be any specific other person with the intent to deceive. This means I will not send an email, create an account, or post any words, pictures, or sounds using someone else's account, name, or picture in order to make anyone believe I am that person.
- I will not use another person's login name or password.

G. I am responsible for respecting other people's property online.

- I will not plagiarize or use others' work without properly referencing it.
- I will not download materials that are owned by other people without permission (e.g. protected by copyright), including books, music and movies.
- I will not read, modify, or remove files owned by teachers or other students without permission.
- If I see another person's work on a computer screen or see that another student is logged into the computer, I will notify a teacher or staff member and wait to use the computer until the other student has been logged off.

H. I am responsible for following school rules whenever I post anything online using a DCPS device or the DCPS network.

- I will not post any material on a school website, wiki, blog, podcast, social media account, or discussion group without permission from a teacher or staff member.
- I will not post pictures or recordings, including my picture or videos of me, with my name or any other identifying information.
- I will not create or post pictures, audio recordings, or video recordings of anyone else without permission.

I. I understand that DCPS may be able to access my DCPS Device, files, and accounts.

- I understand that under certain circumstances, DCPS staff may be allowed to search and access all files located on the DCPS network or saved on DCPS devices at any time.
- I also understand that under certain circumstances, DCPS staff may be authorized to search my personal media account or device, or require me to produce data from my personal media account or device if:
    - DCPS staff has a reasonable suspicion that I am or have been using the account or device to violate DCPS policy (e.g., Bullying Prevention Policy) and a reasonable suspicion that my account or device contains evidence of the suspected violation; or
    - It is necessary to do so in response to an imminent threat to life or safety.

Student Technology Responsible Use Agreement Acknowledgement Form

STUDENTS:

I have read the Student Technology Use Agreement, or someone has read and explained it to me. I agree to use all DCPS devices and the DCPS network responsibly under the rules listed in the Agreement. I understand that if I do not follow these rules, I may receive consequences under DCPS discipline rules and policies, that are aligned to DCMR Chapter 25 policy, and my ability to use DCPS devices and the DCPS network may be restricted. I understand that if I see or otherwise become aware of anyone using a DCPS device or the DCPS network to bully, intimidate, threaten, harass, or hurt someone else, I am encouraged to report this to a teacher or staff member. I understand that my report will be kept confidential, and that DCPS will not tolerate any retaliation against me for making a report.

1. The laptop is owned by DCPS and is loaned to me to be used for instructional and academic purposes only and in accordance with the DCPS Student and Staff Technology and Network Acceptable Use Policy. DCPS collects data and monitors usage of the laptop in compliance with the Protecting Students Digital Privacy Act of 2016.

2. I am responsible for any costs associated with repairing damages caused by my negligence or intentional actions while the laptop is on loan.

3. The laptop must be returned to DCPS upon request. Failure to return this device when requested by DCPS may result in a fee being charged to my family.

Device Type/DCPS Asset Tag Number_____

Student Name (Print)_____

Student Signature_____Date_____

DCPS Representative Name (Print)_____

DCPS Representative Signature_____Date_____

PARENTS/GUARDIANS:

I have read and discussed the Student Technology Use Agreement with my student or, if I am an adult student, I have read the Student Technology Use Agreement or had someone read it for me. I understand that if I/my student fails to follow any of the rules outlined in the Agreement, I/my student may face consequences under DCPS discipline rules and policies, including Chapter 25, and their access to DCPS devices and the DCPS network may be restricted.

I also acknowledge, and agree to, the following with respect to DCPS technology issued to me/my student:

1. The device is owned by DCPS and is being loaned to me/my student to be used for instructional and academic purposes only and in accordance with the DCPS Student and Staff Technology and Network Acceptable Use Policy. DCPS collects data and monitors usage of the device in compliance with the Protecting Students Digital Privacy Act of 2016.
2. In the event that I/my student loses and/or DCPS determines I/my student has intentionally or negligently damaged the device, I/my student will be subject to appropriate DCPS discipline, and I will be required to meet with DCPS to determine the reason for the loss/damage and discuss best practices for the responsible care of the device.

3. I further understand that the device must be returned to DCPS upon request. If I fail to return the device as requested, the device may be disabled remotely.

Parent/Guardian Name (Print) _____

Parent/Guardian Signature_____Date_____