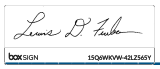
DISTRICT OF COLUMBIA
PUBLIC SCHOOLS

This *Student and Staff Technology and Network Acceptable Use Policy* rescinds and supersedes all previous policy, memoranda, and/or guidance promulgated by DCPS on this subject matter.

Chancellor Approval: 

Effective: August 26, 2024

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 and staff 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. This policy aims to:

- Establish standards for the acceptable uses of the DCPS network and DCPS technology;
- Set expectations around the responsible use of artificial intelligence;
- Prevent unauthorized and unlawful uses of the DCPS network and DCPS technology; and
- 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 applies to all DCPS students, staff, visitors, and others who use the DCPS network or devices, and rescinds the previous DCPS Student and Staff Technology and Network Acceptable Use Policy (2021).

II. AUTHORITY AND APPLICABLE LAW[1]

Source	Citation
Federal Law	- 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	- Children's Online Privacy Protection Rule, 16 C.F.R. Part 312
District of Columbia Law	- Protecting Students Digital Privacy Act of 2016, D.C. Law 21-218, codified at D.C. Official Code 38-831.01 *et seq*.
District of Columbia Municipal Regulations	- 5-B DCMR § 2500 *et seq*. – Student Discipline - 6-B DCMR § 1610 – Employee Progressive Discipline

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

III. KEY TERMS AND DEFINITIONS

Artificial Intelligence (AI) means a branch of computer science dealing with the simulation of intelligent behavior in computers.

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

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

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

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, in accordance with local education agency policy.

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.

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

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.

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 ownership or control over technology and materials on DCPS provided 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 conduct investigations, comply with legal requirements, maintain system integrity, and, if necessary, to ensure that technology and network users are acting responsibly and in alignment with this policy. All accounts created by DCPS for students or staff may be monitored by DCPS.

1. Students

DCPS will provide notice of this policy through the annual enrollment process, and all parents and adult students will be asked to acknowledge receipt. Students and parents may be required to sign a Student Technology and Network Responsible Use Agreement (Student Responsible Use Agreement), included in the Appendices and available on the DCPS website. 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.

DCPS provides students with annual lessons in digital citizenship and online safety. Students are required to complete the courses in the Digital Citizenship & Literacy Student Hub,[2] including the module on device use and care, and completion of a course may be required before a student is issued a DCPS device or account.

Failure to follow these rules will be addressed under DCPS discipline regulations and policies, including the Safe and Positive Students Policy,[3] and may result in loss of 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.

2. Staff

DCPS will provide notice of this policy to new staff through the onboarding process, and the Staff Technology Responsible Use Agreement (Staff Responsible Use Agreement) included in the Appendices, will be available on the DCPS website as an additional and ongoing reference. Staff who have been assigned a DCPS device may also be asked to sign or re-sign a Staff Technology Responsible Use Agreement Acknowledgement Form prior to or upon receipt of their device.

The DC Government, the DC Office of the Chief Technology Officer (OCTO), and/or DCPS may require staff to complete employee training related to cybersecurity or related topics. Staff who fail to complete those trainings in a timely manner or to follow this policy may be subject to progressive discipline.

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,

[2] *Available at* https://dcps.instructure.com/enroll/Y8Y7KY.
[3] *Available at* https://dcps.dc.gov/page/dcps-policies.

and career development. Use of the DCPS network is a privilege. 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 are 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 DCPS produced content. Any statement not produced by DCPS that is 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.[4]

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, store, or delete any electronic information or files as well as disclose them to others as it deems necessary. Students have no expectation of privacy regarding use of DCPS property, the DCPS computer network, or 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 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

[4] 47 U.S.C. 254(h)(5)(B).

from children.[5]

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.[6] 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 age 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 age 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 users and lock out unauthorized access and potential threats. DCPS assigns user access to the DCPS network, DCPS email accounts, and DCPS authorized applications based on grade level and/or school or teacher request as follows:

- **Access**: All students and staff must use their personalized credentials and passwords to log into DCPS systems and devices.
- **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 grades 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, 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 certain 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.
- **Graduation or Unenrollment:** Students who graduate or unenroll from DCPS will no longer have access to DCPS technology or systems including applications and stored materials.

5. Passwords

Password protection is required on all DCPS-issued technology to prevent use by anyone unauthorized by DCPS, and users are required to adhere to DCPS password requirements when logging into school computers, networks, and online systems. Users will be automatically prompted to meet these DCPS' password requirements as part of the process of regularly updating their password.

[5] *See* 16 C.F.R. 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.

[6] For additional information on complying with COPPA, please see https://www.ftc.gov/tipsadvice/business-center/guidance/complying-coppa-frequently-asked-questions.

Students and staff are not authorized to share their password or the password of any other DCPS student or staff member 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. DCPS requires students to participate in digital citizenship and online safety lessons to learn how to avoid these scams and other good practices for the safe use of technology.

Students with disabilities who are not able to master digital citizenship lessons are excluded from these password requirements.

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. Access to Telehealth/Telemedicine

DCPS staff and students are permitted to access telehealth sessions on DCPS devices. Although DCPS 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.

7. Videoconferencing

Videoconferencing occurs when DCPS staff and students 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.

Staff and students should report any inappropriate behavior or concerning behavior that may occur during a videoconference to the DCPS Office of Integrity.[7] Staff and students must continue to follow the DCPS Employee Rights and Responsibilities Policy,[8] Social Media Policy,[9] and any other applicable policy, regulation, and law regarding staff-student interactions.

8. Artificial Intelligence (AI)

As with all technology, students and staff are required to use AI in a responsible and ethical manner. AI tools should be used by students and staff as a supplement, not a substitute, for learning. DCPS will provide students with lessons on the benefits and risks of AI through Digital Citizenship and AI-specific courses.

[7] The Office of Integrity can be reached by completing the Online Referral Form, available at https://dcps.dc.gov/page/office-integrity or emailing dcps.cio@k12.dc.gov.
[8] *Available at* https://dcps.dc.gov/page/dcps-policies.
[9] *Available at* https://dcps.dc.gov/page/dcps-policies.

Though addressed in other parts of this policy, the below uses of AI are specifically prohibited and will be the subject of additional scrutiny:

- Bullying and Harassment: Students are prohibited from using AI in a way that could harm themselves or others. Using AI tools to manipulate media to impersonate others is prohibited.
- Plagiarism and Cheating: Students are prohibited from submitting AI-generated work as their original work or using AI to answer test, exam, or other assignment questions (unless directed to do so by their teacher).

Consistent with the DCPS Safe and Positive Schools Policy,[10] staff must implement disciplinary responses, beginning with the least severe appropriate response within the range of permissible disciplinary responses. This range could vary from providing an opportunity to re-submit the work, to grade reduction.

a. Additional Considerations for Staff Use of AI

DCPS maintains a list of approved AI-enhanced tools for student learning and will provide professional development to support the appropriate deployment of these tools. If teachers and school leaders wish to use an AI tool outside of the list curated by the DCPS EdTech team, it must meet the criteria set by the EdTech Team and they must submit the AI Tool Approval Form prior to purchase and use in a class or on an assignment. These criteria and the Form are available on the EdTech SharePoint website at https://dck12.sharepoint.com/sites/DCPSEdTechInformationResources.

Staff are required to verify the truthfulness of any AI-produced content using trusted sources as AI-generated content may contain errors or biases. When using AI for communications, such as drafting emails to parents, staff are responsible for ensuring that language is professional and free of inaccuracies and bias. Staff must review and critically reflect on all AI-generated content before use.

C. Technology (Including Computers, Laptops, Tablets)

1. Device Support

DCPS provides basic installation, synchronization, and software support for DCPS-technology. 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 technology to prevent unauthorized use in the event of loss or theft.

2. Damage, Loss, or 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.

[10] *Available at* https://dcps.dc.gov/publication/safe-and-positive-schools-policy.

A DCPS staff member should only use the device assigned to them by the DCPS IT team and is prohibited from taking or using devices assigned to other current or past employees.

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 relevant 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, or 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;
- The device was completely submerged in water or other liquids; or
- Repeated pattern of damage if the student has caused damage to three (3) or more devices in a school year.

Disciplinary responses for students for damage to devices that resulted from negligence or intentional acts of vandalism will be determined under the DCPS Safe and Positive Schools Policy[11] discipline regulations and law, and this Acceptable Use Policy.

Students may not be penalized for damage resulting from normal wear and tear or unintentional accidents. Examples of device damage resulting from *normal wear and tear* include but are not limited to:

- Missing key(s) on the keyboard;
- Cracked screen because of accidental drops;
- Damage isolated to a small portion of the device, such as corner/sides of the screen, which could be the result of accidental drops;
- Accidental liquid spills on the keyboard; or
- Damage caused by a power surge.

If DCPS technology is lost, stolen, or damaged, students must notify a teacher or school leader; staff must notify their supervisor and a DCPS Technology point of contact. 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 to locate devices identified as lost or stolen or remotely disable devices that are not returned upon request. Damaged devices must be returned to the DCPS IT team (AssetAdmin@k12.dc.gov) and must not be disposed of by students, families, or staff. The device must first be evaluated by the DCPS IT team and OCTO prior to replacement.

[11] *Available at* https://dcps.dc.gov/page/dcps-policies.

3. 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 (see the Appendices) before they are assigned and issued 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 monitored and accessed by DCPS staff.[12]

Assistive technology may go home with the student if the student's IEP team, in collaboration with the DCPS Assistive Technology Team, determines that the student requires these supports to complete educational tasks at home (e.g., homework, communication). Students must follow all DCPS policies in using this technology at home, just as they would if or when using the technology at school. For additional information on assistive technology, please see the DCPS Assistive Technology website[13] or contact DCPS.AssistiveTech@k12.dc.gov or the student's IEP Team.

D. Conduct and Acceptable Use

By using the DCPS network and DCPS technology, staff and students agree to follow all relevant DC Government; OCTO; and DCPS regulations, policies, and guidelines. Staff and students must report misuse or breach of protocols to teachers, appropriate supervisors, administrators, or Central Services employees as soon as they are aware of the misuse or breach.[14]

Staff and students must 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:

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 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;

[12] *See* D.C. Official Code § 38-831.03(a).
[13] *Available at* https://dcps.dc.gov/page/assistive-technology%E2%80%AF.
[14] For additional information on filing reports and complaints, please see Section V.

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 network account, files, or data, or modifies their files, data, or passwords;
10. Impersonates any living or dead authorized person, 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. Installs, downloads, or uses unauthorized or unlicensed software or third-party system;
21. Accesses, distributes, downloads, or uses unauthorized games, programs, files, electronic media, or stand-alone applications from the internet that may cause a threat to the DCPS network;
22. Promotes or participates in any way in unauthorized raffles or fundraisers;
23. Promotes or participates in any way in partisan political activities;
24. Promotes or participates in any way in internal political or election activities related to a union or other organization representing employees;
25. Engages in private business, commercial, or other activities for personal financial gain;
26. Distributes unauthorized information regarding other user's passwords or security systems;
27. Falsifies, tampers with, or makes unauthorized changes, additions, or deletions to data located on the DCPS network or any school systems;
28. Accesses or uses data located on a DCPS network for personal uses;
29. 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;
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 (i.e., 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.

Students, staff, and other users must not share their DCPS-issued device or 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. Personal Media Technology

Student use of personal technology on the DCPS network is not permitted without the express written authorization from the Chancellor or their designee. DCPS is not responsible for the maintenance and security of student personal electronic devices and assumes no responsibility for loss or theft. DCPS, 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.

F. Privacy of Student Personal Media Accounts and Technology

1. School-Specific Student Personal Media Account and Technology Policies

Principals must notify students and parents in writing if their school has additional rules related to student personal media accounts and technological devices.

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

Other than those exceptions in Section IV.G.3, DCPS will not take or threaten to take action against a student or prospective student, including discipline, expulsion, unenrollment, refusal to admit, or prohibited 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.[15]

If DCPS 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 means, DCPS will:

[15] D.C. Official Code § 38-831.04(a).

- 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.[16]

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 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.[17]

3. Exceptions to Privacy of Personal Media Accounts and Student Technology

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 instances of policy violations or imminent threat to life or safety.

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 has a reasonable suspicion that the personal media account or personal technological device contains evidence of the suspected violation.[18]

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 components to be searched or that the student will be compelled to produce.[19]

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.[20]

[16] D.C. Official Code § 38-831.04(b).
[17] D.C. Official Code § 38-831.04(e).
[18] D.C. Official Code § 38-831.04(c)(1)(A).
[19] D.C. Official Code § 38-831.04(c)(1)(B).
[20] D.C. Official Code § 38-831.04(d).

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.[21]

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.[22]

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.[23]

V. POLICY IMPLEMENTATION REQUIREMENTS

All DCPS students and staff are required to comply with the requirements set forth in this policy. To support its implementation, principals are expected to make staff aware of required activities and timelines on an 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[24] or sending an email to dcps.cio@k12.dc.gov.

[21] D.C. Official Code § 38-831.04(c)(1)(C)-(D).
[22] D.C. Official Code § 38-831.04(c)(2)(A).
[23] D.C. Official Code § 38-831.04(c)(2)(B)-(C).
[24] *Available at* https://dcps.dc.gov/page/office-integrity.

APPENDICES

The following documents are included as appendices:

- Student Technology Responsible Use Agreement;
- Student Technology Responsible Use Agreement Acknowledgement Form; and
- Staff Technology Responsible Use Agreement Acknowledgement Form.

DISTRICT OF COLUMBIA
PUBLIC SCHOOLS

Student Technology Responsible Use Agreement

As a responsible user of technology:

A. I will treat my DCPS device with respect, taking care not to drop or damage it.

- ❑ I will follow school rules about checking out and returning my DCPS device.
- ❑ I will immediately report to a teacher or staff member if my DCPS device is damaged or not working properly.
- ❑ I will keep my device indoors in a secure location whenever I am not using it.

B. I will protect my personal information.

- ❑ I will not share my DCPS device, username, or password with anyone (unless I am an early childhood learner or student who requires support to use my account).
- ❑ I will save my work in my DCPS Office365 OneDrive and log out of my accounts and programs when I finish working.
- ❑ I will inform a teacher immediately if I think or know someone has used my account.

C. I will use my device only for schoolwork.

- ❑ I will only download, install, or use software, apps, browser extensions, or media files, if my teacher gives me permission to do so.
- ❑ I will avoid resources that are inappropriate, offensive, or illegal. If I see inappropriate material online, I will immediately report it to a teacher or staff member.

D. I will use my digital citizenship skills and treat people with kindness.

- ❑ I will use respectful and appropriate language.
- ❑ I will properly reference others' work and will not plagiarize.
- ❑ I will fact check information before I share it online.
- ❑ I will use AI in a responsible and ethnical manner that respects the privacy of all, does not bully or harass others, and does not plagiarize or cheat on schoolwork.

Outcomes for Irresponsible Technology Use

You will lose access to the DCPS network or DCPS technology for increasing periods of time under DCPS student discipline regulations and policies. 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. Under certain circumstances, DCPS staff may be authorized to search your personal media account or device or require you to produce data from my personal media account or device.

Protocol for Stolen or Accidently Damaged Devices

If your device was stolen or damaged, you must immediately notify a teacher or staff member as soon as possible because DCPS must file a police report within five calendar days of a suspected theft in order for the device to be tracked. You will not be held responsible for costs associated with the stolen or accidentally damaged device. Your partnership with DCPS is greatly appreciated in this scenario.

Examples of Unacceptable Technology Use:

- Eating or drinking near a DCPS device;
- Writing, drawing, or attaching stickers on a DCPS device;

- Downloading, installing, or running any type of files, including music and video files, websites, software, apps, browser extensions, or media, unless a teacher grants permission;
- Using applications or plug-ins to try to change security settings or internet content filters;
- Inserting USB drives (i.e., flash drives) into a device unless approved to do so by a teacher;
- Searching for, saving, circulating, or displaying resources that are hate-based, lewd, vulgar, etc.;
- Using the DCPS network to engage in any illegal or criminal acts;
- Accessing online games, social media, messaging apps, or group chats unless these activities are related to schoolwork and a teacher or staff member is supervising the activity;
- Bullying, harassing, threatening, or intimidating other people;
- Using another person's login name or password; and
- Creating or posting pictures, audio, or video recordings of others without their permission.

DISTRICT OF COLUMBIA
PUBLIC SCHOOLS

Student Technology Responsible Use Agreement Acknowledgement Form

Students: I have read the DCPS Student and Staff Technology and Network Acceptable Use Policy and Student Technology Use Responsible Use Agreement, or someone has read and explained it to me.

Parents/Guardians: I have read and discussed the DCPS Student and Staff Technology and Network Acceptable Use Policy and Student Technology Responsible Use Agreement with my student.

1. I agree to use all DCPS devices and the DCPS network responsibly under the rules listed in the Agreement and the Acceptable Use Policy. I understand that if I do not follow these rules, I may receive consequences under DCPS discipline rules and policies and my ability to use DCPS devices and the DCPS network may be restricted.

2. 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 will 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.

3. If I am issued a device, I understand that it is loaned to me to be 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.

4. If I lose or intentionally or negligently damage a DCPS device, I may face appropriate disciplinary action from DCPS. I will be required to meet with DCPS to determine the reason for the loss or damage and learn responsible device care practices.

5. If I am issued a device, I understand that it must be returned to my school Technology Point of Contact or the DCPS IT team (AssetAdmin@k12.dc.gov) upon request. If I do not return the device as requested, the device may be disabled remotely, and a fee may be charged to my family.

6. I understand that I will no longer have access to DCPS technology or network once I graduate or unenroll from DCPS.

Staff Technology Responsible Use Agreement Acknowledgement Form

I have read the DCPS Student and Staff Technology and Network Acceptable Use Policy.

1. I agree to use the DCPS network and any DCPS device issued to me responsibly under the rules listed in the Acceptable Use Policy. I understand that if I do not follow these rules, I may receive consequences under DCPS discipline rules and policies and DC law and regulations.

2. If I am issued a laptop by DCPS, I acknowledge that the laptop is owned by DCPS. The laptop is loaned to me to be used for work purposes only and in accordance with the DCPS Student and Staff Technology and Network Acceptable Use Policy.

3. If I am issued a laptop by DCPS, I am responsible for any costs associated with repairing damage caused by my negligence or intentional actions while the laptop is on loan.

4. If I am issued a laptop by DCPS, the laptop must be returned to the DCPS IT team (AssetAdmin@k12.dc.gov) if I leave the organization or upon request. Failure to return this device when requested by DCPS may result in a fee being charged to me.