



## **DCPS STUDENT SAFETY AND USE POLICY FOR INTERNET AND TECHNOLOGY**

**Purpose:** 1) To establish standards for the acceptable uses of internet and electronic mail (email) services within the computer network maintained and operated by the District of Columbia Public Schools (DCPS computer network); 2) To prevent unauthorized and unlawful uses of email and internet within the DCPS computer network; 3) To establish procedures for the use of computer equipment that is maintained and operated by the by District of Columbia Public Schools (DCPS); and 4) To comply with the Children’s Internet Protection Act of 2000 (CIPA). This policy is applicable to all current DCPS students who use computers within the DCPS network.

### **Policy**

DCPS will use technology protection to block or filter internet access to visual depictions that are obscene, pornographic, or harmful to minors. 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.

Penalties for prohibited use 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.

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 a student incurs due to network use will be borne solely by the student. DCPS is not responsible for the accuracy or quality of the information obtained by the student 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.

## **1. Acceptable and Prohibited Internet Use**

### **A. Acceptable uses of email and internet on the DCPS computer network**

1) Use of network email and internet that is directly related to the mission, business, and educational goals and policies of the D.C. Public Schools.

### **B. Prohibited uses of email and internet on the DCPS computer network**

All DCPS students are prohibited from the following when using the DCPS computer network:

- i. Accessing DCPS network and email accounts outside of school without a parent or guardian supervising the usage, unless the student is 18 or older.
- ii. Revealing personal information about themselves on the internet, including name, address, telephone number, and uploading photographs.
- iii. Personally meeting anyone with whom they have only had prior contact with on the internet.
- iv. Using profane, vulgar, or abusive language.

## **2. Procedures and Guidelines: Content and Conduct**

A. Students are prohibited from using the DCPS computer network to transmit fraudulent, harassing or obscene, or otherwise inappropriate email messages. Examples of such messages include but are not limited to:

1. Messages sent under an assumed name, modified email address, or with the intent to obscure the origin of the message.
2. Messages that harass an individual or group because of race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, gender identity or expression, family responsibilities, genetic information, disability, matriculation, or political affiliation.
3. Messages that are obscene, contain pornography, or are harmful to minors.
4. Messages containing indecent speech or hate speech.

- B. All contents of all files located on computer equipment owned or maintained by DCPS are considered property of DCPS and are subject to search by DCPS at any time and for any reason.
- C. Students shall not display or transmit any images, sounds, or messages, or other material that could be considered pornographic in nature.
- D. Students shall not display or transmit any images, sounds, or messages, or other material that could create an atmosphere of harassment or hate.
- E. Students are prohibited from online game playing and gambling, unless these activities are legitimately related to school curriculum and coursework a teacher or other appropriate school personnel is supervising the activity.
- F. Students are prohibited from accessing internet chat rooms, unless the chat rooms are related to school coursework and access is made under the supervision of a teacher, parent or guardian.
- G. Students are prohibited from accessing social networking sites, including, but not limited to, My Space, Facebook, and Twitter.
- H. Students shall not download or spread computer viruses on DCPS network computers or engage in any other deliberate conduct that disrupts, obstructs, or burdens the resources of the DCPS computer network.
- I. Students shall not use the DCPS computer network to engage in any illegal or criminal acts, including, but not limited to, criminal gang activity, threatening the physical safety of another person, or computer hacking.
- J. Students shall not install or run any type of software on a DCPS network computer without the consent of the Office of the Chief Technology Officer.
- H. Students may not use network computers for personal financial gain by posting messages that advertise the student's own personal business or any business or venture in which the student has a financial interest.
- K. Students shall not read, modify, or remove files owned by other students.

**3. Procedures and Guidelines: Network Security and Equipment Maintenance**

- A. Students are prohibited from sharing their password or login identification with any other person.

- B. Students are prohibited from logging into the network by using account information belonging to another student, teacher, or network administrator.
- C. If a student discovers or has reason to believe that another student has obtained unauthorized access of his/her account, the student shall contact a teacher or other school personnel, as well as immediately change his/her password. The teacher or school personnel shall immediately contact the Office of the Chief Technology Officer or a network administrator.
- D. Students are prohibited from modifying or rearranging technology equipment belonging to DCPS, including keyboards, monitor, printers, and computers.
- E. Students shall report any cases of malfunctioning equipment or other network issues to a teacher, or other school personnel. The teacher or other school personnel shall contact a network administrator.
- F. When using public workstations, students shall log off of the network before leaving the work station. Students shall further ensure that the workstation is in suitable condition for the next student.
- G. When using private or individual workstations, students shall lock their computer or log off of the network if they will be away from the workstation for an extended period of time.

**District of Columbia Public Schools**

**Student Safety and Use Policy For Internet and Technology**

**ACKNOWLEDGMENT FORM**



**For the Student**

I have read the DCPS Student Safety and Use Policy For Internet and Technology. I agree to follow all of the rules that are stated in the policy. I understand that if I violate any of these rules my school internet and technology access may be terminated, and I may face other disciplinary or legal consequences.

Date: \_\_\_\_\_

Name of School: \_\_\_\_\_

Name of Student (print): \_\_\_\_\_

Signature of Student: \_\_\_\_\_

**For the Parent/Guardian**

I have read the DCPS Student Safety and Use Policy For Internet and Technology and reviewed it with my child(ren). I recognize and understand that if my child does not abide by the terms of the policy that his/her school internet and technology access may be terminated and he/she may face other disciplinary or legal consequences.

Name of parent/guardian (print): \_\_\_\_\_

Signature of parent/guardian: \_\_\_\_\_