

August 22, 2018

**RESCIND 03-0326-PO03
AND ADOPT A NEW STUDENT ACCEPTABLE USE POLICY**

THE CHIEF EXECUTIVE OFFICER RECOMMENDS: That the Board rescind Board Report 03-0326-PO03 and adopt a new Student Acceptable Use Policy.

PURPOSE: Chicago Public Schools (CPS) provides access to technology devices, internet, and network systems to students for educational purposes. This Student Acceptable Use Policy (AUP) establishes the standards for acceptable electronic activity of students accessing or using the district or school technology, internet and network systems regardless of physical location and also the electronic communications between students and CPS staff and other adults who work in schools.

GUIDING PRINCIPLES:

1. CPS is responsible for providing reliable and secure technology resources necessary to foster the educational development and success of our students.
2. CPS provides a baseline set of policies and structures to allow schools to implement technology in ways that meet the needs of their student and parent communities.
3. CPS provides a secure framework that will allow students to use online tools, including social media, in our classrooms and schools, to increase student engagement, collaboration and learning.
4. CPS is responsible for instructing students about digital citizenship, including appropriate and safe online behavior, interactions with individuals on social media and cyberbullying awareness.

POLICY TEXT:

I. Applicability. This policy applies to all students who use CPS Computer Resources and/or access the CPS Network ("Students"). Personal electronic devices (e.g. personal laptop) are subject to this policy when such devices are connected to the CPS Network or Computer Resources.

II. Delegated Authority. This policy is subject to periodic review by the Chief Information Officer (CIO) to consider amendments based on technological advances, educational priorities or changes to the organizational vision.

III. Definitions.

Children's Internet Protection Act (CIPA) refers to the federal law that requires schools that receive federal funding through the E-Rate program to protect students from content deemed harmful or inappropriate and shall filter internet access accordingly. For more information, visit <https://www.fcc.gov/consumers/guides/childrens-internet-protection-act>

Collaboration Tools refers to systems which support synchronous and asynchronous communication through a variety of devices, tools and channels. Examples of collaboration systems include, but are not limited to: calendaring, message/conference boards, blogs, group messaging apps, video conferencing, websites and podcasting.

Computer Resources refers to all computers and information technology, whether stationary or portable, used by students, including but not limited to all related peripherals, components, disk space, storage devices, servers, telecommunication devices and output devices such as printers, scanners, facsimile machines and copiers whether owned or leased by the Board.

CPS Network or Network refers to the infrastructure used to communicate and to transmit, store and review data over an electronic medium and includes, but is not limited to, CPS email system(s), bulk communication tools, collaboration tools, databases, internet service, intranet and systems for student information, financials, and personnel data and any school-based system authorized for use by ITS.

Social Media refers to online platforms, networks or websites through which users post or share information, ideas, messages and other content (such as photos or videos) and includes, but is not limited to, media sharing sites and social networking sites such as Twitter, Facebook, Instagram, Snapchat, YouTube and LinkedIn.

“CPS Social Media” refers to authorized CPS-related social media that is either school-based (e.g. principal establishes a social media page for the school, or a teacher establishes a social media page for his/her class) or district-based, network-based or department-based (e.g. a department establishes a social media page to communicate with the larger CPS community).

“Personal Social Media” refers to non-CPS-related Social Media page(s) established by a user for his/her personal or private endeavors.

“Non-CPS Social Media” refers to Social Media established by or for a third party or non-CPS group or organization (e.g. Social Media page(s) established by or for a public or private organization, for-profit or not-for-profit company, etc.)

Unauthorized Software refers to any software product or tool that is explicitly listed as ‘prohibited for use’ on the CPS network. The complete list of prohibited technology platforms is located on the district’s AUP Guidance website: www.cps.edu/aupguidelines.

IV. Privacy and Monitoring.

A. Privacy. Students have no expectation of privacy in their use of the CPS Network and Computer Resources. By authorizing student use of technology resources, CPS does not relinquish control over materials on the systems or contained in files on the systems. There is no expectation of privacy related to information stored or transmitted over the CPS Network or in school systems. CPS reserves the right to access, review, copy, store, or delete any files stored on Computer Resources and any student communication using the CPS Network or school system. Electronic messages and files stored on CPS computers or transmitted using CPS systems may be treated like any other school property. District administrators may review files and messages to maintain system integrity and, if necessary, to ensure that students are acting responsibly. CPS may choose to deploy location tracking software on Computer Resources for the sole purpose of locating devices identified as lost or stolen.

B. Monitoring. The Department of Information & Technology Services (ITS) has the right to access, search, read, inspect, copy, monitor, log or otherwise use data and information stored, transmitted and processed on the CPS Network and Computer Resources in order to execute the requirements of this policy. CPS Network including but not limited to internet and email usage may be monitored and audited by the school management and ITS for in appropriate activity or oversight purposes. ITS reserves the right to: (1) access and make changes to any system connected to the CPS Network and Computer Resources to address security concerns, (2) deny student access to any system to address security concerns, and (3) determine what constitutes appropriate use of these resources and to report illegal activities. ITS may intercept and/or quarantine email messages and other messaging services for business, legal or security purposes.

V. General Provisions.

A. Acceptable Use. CPS provides E-mail, bulk communication tools (e.g. BlackBoard Connect) and other collaboration tools (e.g. CPS Google Classroom), internet access and other CPS Network tools and Computer Resources to students for educational and school-related purposes only. When using the CPS Network, students must conduct themselves in a responsible and appropriate manner.

B. Unacceptable Use. Unacceptable use of the CPS Network and Computer Resources are prohibited. Students shall not use the CPS Network or Computer Resources including access to the internet, intranet, collaboration tools, bulk communication tools, social media or email to use, 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, defamatory or otherwise meant to bully or intimidate others;

2. is offensive or discriminatory to persons based on race, ethnicity, national origin, gender, gender identity, sexual orientation, age, physical or mental illness or disability, marital status, economic status, immigration status, religion, personal appearance or other visible characteristics;
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 computer or network or constitutes unauthorized access or attempts to circumvent any security measures;
9. obtains access to another individual's CPS Network account, files or data, or modifies their files, data or passwords;
10. impersonates any person living or dead, organization, business, or other entity;
11. degrades the performance of, causes a security risk or otherwise threatens the integrity or efficient operation of, the CPS Network or Computer Resources;
12. deprives an authorized individual from accessing CPS Network or Computer Resources.
13. obtains Computer Resources or CPS Network access beyond those authorized
14. engages in unauthorized or unlawful entry into a CPS Network system;
15. enables or constitutes wagering or gambling of any kind;
16. accesses, distributes, downloads or uses games except when an assigned educational activity;
17. promotes or participates in any way in unauthorized raffles or fundraisers;
18. plagiarizing any information gained on or through use of the CPS Network or Computer Resources;
19. engages in private business, commercial or other activities for personal financial gain;
20. accesses or distributes unauthorized information regarding user passwords or security systems;
21. falsifies, tampers with or makes unauthorized changes, additions or deletions to data located on the CPS Network or school systems;
22. installs, downloads or uses unauthorized or unlicensed software or third party system;
23. violates the terms of use specified for a particular Computer Resource, CPS Network system or school system;
24. violates any express prohibition noted in this policy or the Student Code of Conduct;
25. engages in hacking (intentionally gaining access by illegal means or without authorization) into the CPS Network or school system to access unauthorized information, or to otherwise circumvent information security systems;
26. engages in inappropriate sexual conduct, including unwelcomed sexual contact, indecent exposure, transmitting sexually suggestive images, or other sexual activities;
27. downloads unauthorized games, programs, files, electronic media, and/or stand-alone applications from the internet that may cause a threat to the CPS Network;
28. constitutes use that disrupts the proper and orderly operation of the school;
29. use of proxy servers or virtual private networks to bypass network security systems (firewalls, etc.);
or
30. accesses, distributes or downloads non-educational materials or inappropriate content or materials.

C. Software Installation. Students are not authorized to install software on CPS equipment unless supervised and approved as part of an educational program or task. ITS may remove student-installed software at any time in order to preserve or protect the CPS Network or Computer Resources or for any other reason deemed necessary by ITS.

D. Filtering and Blocking. CPS is required to protect students from online threats, block access to inappropriate content, and monitor internet use by minors on school networks in accordance with CIPA. ITS is responsible for managing the district's internet filter and will work with school administrators to ensure the filter meets the academic and operational needs of each school while protecting minors from inappropriate content per CIPA. The district's use of filtering software does not negate or reduce a student's obligation to abide by the terms of this policy and to refrain from disabling filters or accessing inappropriate content online. Parents should be aware that despite the district's good faith efforts at filtering, objectionable

content might be available either due to an individual using unauthorized means to bypass filtering or as a result of the creation of objectionable content that has not yet been identified by filtering software.

E. Passwords. Students are required to adhere to password requirements set forth by CPS when logging into school computers, networks, and online systems. Students are not authorized to share their password under any circumstance.

F. Access Privilege. Student use of the CPS Network and Computer Resources is a privilege, not a right. When a student uses the CPS Network or Computer Resources in a manner that violates this policy or the Student Code of Conduct, his/her access may be suspended or revoked.

VI. Communication with CPS Staff and other Adults Who Work in Schools.

A. Exclusive Use of CPS Network. Students must use authorized CPS Network systems (e.g. CPS email, Google Classroom) for all electronic communications with CPS staff and other adults who work in schools, except when the communications are specifically authorized as set out below.

B. Phone and Text Communications.

1. Students are prohibited from calling or leaving a voice message on the personal telephone or mobile device of a staff member or other adult who works in a school.

2. Elementary students are prohibited from communicating with CPS staff and other adults who work in schools via text messaging or IM, except when authorized under sections VI.B.5 and 6 below.

3. High Schools students are prohibited from communicating with CPS staff and other adults who work in schools via text messaging or IM, except when authorized under sections VI.B.5 and 6 below, and except for authorized pre-approved safety meet-up communications where:

a. The parent/guardian and principal both provide prior written permission to the text messaging communications, and

b. Communications are sent as group texts/messages with the parent/guardian on the text message or IM and also the staff/adults CPS email address for proper retention of communications.

4. Students may receive bulk text notifications and alerts on their personal mobile device from their school when their parent/guardian provides written permission to enroll and receive these text notifications and alerts.

5. Students in grades 7-11 enrolled in a CPS Program for Re-Engagement of Out-of-School Youth, Chronic Truants or Students Exiting Juvenile Detention Facilities ("Program") may communicate via text/IM with the CPS staff member(s) assigned to the student when authorized in writing by the Program manager. The requirements for a student to text/IM with a CPS staff member shall be listed in the student's Program enrollment materials and the student must follow all listed requirements.

6. The Chief Executive Officer for CPS may authorize additional programs under which a student may have text/IM communications with a CPS staff or other adult who works in a school. In such cases, a student must: (a) receive written authorization from the manager of the CEO-authorized program to engage in text/IM communication with a CPS staff or other adult who works in a school, and (b) abide by the text/IM communication requirements listed in the student's program enrollment materials.

C. Personal Email. Students are prohibited from communicating with CPS staff and other adults who work in schools via the personal email of a staff member or other adult who works in a school. Students must use their CPS email account to engage in email communications to CPS staff or other adult who works in a school.

D. Social Media. Students shall not communicate with CPS staff and other adults who work in the school via the staff/adult's Personal Social Media or otherwise through non-CPS Social Media. Students shall not add, invite, follow or accept the request of any CPS staff member or other adult who works in a school to be a 'friend' or contact on any Personal Social Media or non-CPS Social Media account. Students may use CPS Social Media communicate with CPS staff members or other adults who works in a school.

E. Other Electronic Communications. Students are prohibited from communicating with CPS staff and other adults who work in schools via any group messaging application or other electronic or online tool except via tools provided on the CPS Network or otherwise authorized by ITS (e.g. CPS Google Classroom, BlackBoard Direct).

F. Exceptions. Nothing in this section shall restrict:

1. Communications between a student and their parent/guardian or other family members;
2. Emergency Communications involving the health and safety of a student in which case the student should include more than one CPS staff member on the contact.

G. Reporting Improper Contact. Any student who receives a communication from a staff member or other adult who works in a school via the student's mobile device, personal email or personal social media or non-CPS social media or is asked to provide contact information for this purpose should (except when authorized above) should:

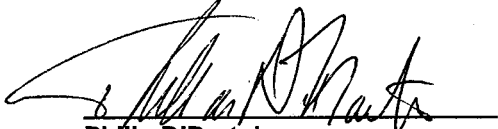
1. Immediately notify their parent/guardian and principal or school administrator;
2. Show or provide a copy of the communication to their parent/guardian and also the principal or school administrator; or
3. Call the CPS Student Protections Hotline at 773-535-4400.

VII. Notification of Misuse. Students have a duty to protect the security, integrity and confidentiality of the CPS Network and Computer Resources. Students must immediately notify a teacher or other school staff if they have identified a security problem or are aware of any unauthorized access, use, abuse, misuse, injury, degradation, theft or destruction of the CPS Network or Computer Resources.


VIII. Discipline. Failure to abide by this policy may subject a student to discipline in accordance with Student Code of Conduct.


IX. Student Protections. Students should promptly report to a teacher or other school staff member any communication they receive that is inappropriate or makes them feel uncomfortable. If a student is harassed, intimidated, bullied or threatened through the CPS Network, Computer Resources or otherwise, he/she should contact their principal or the Office of Student Protections & Title IX, or call the CPS Student Protections Hotline at 773-535-4400.

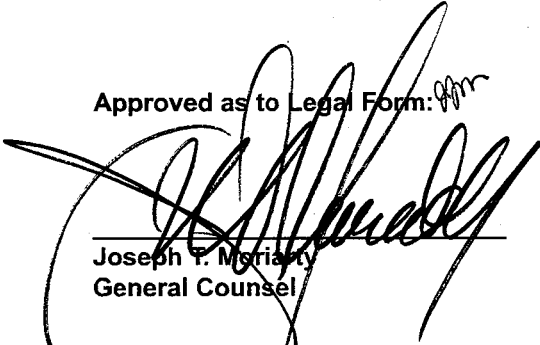
Approved for Consideration:


Philip DiBartolo
Chief Information Officer

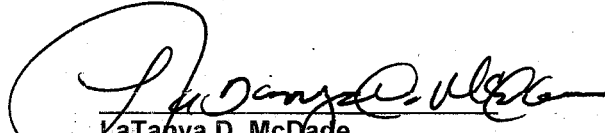
Approved:


Janice K. Jackson, EdD
Chief Executive Officer

Approved as to Legal Form: 


Joseph T. Moriarty
General Counsel

Approved for Consideration:


LaTanya D. McDade
Chief Education Officer