

October 23, 2025

AMEND BOARD REPORT 19-0828-PO2
STUDENT ACCEPTABLE USE POLICY

THE CHIEF EXECUTIVE OFFICER RECOMMENDS:

That the Board of Education (“Board”) amend Board Report 19-0828-PO2 Student Acceptable Use Policy.

~~The purpose of these proposed amendments is to incorporate feedback from principals and administrators, Career and Community connections, the Student Outreach and Re-Engagement Centers (SOAR), Juvenile Justice (JJ) teams, the Office of Safety and Security, Student Protections/Title IX and the Law Department. The proposed amendments will:~~

- ~~1) permit the use of telephone communication between Staff and Students when necessitated by an educational or extra-curricular activity including field trips, for purposes of ensuring student safety, and~~
- ~~2) clarify message retention rules will apply to approved usage for field trips.~~
- 1) introduce artificial intelligence and media literacy responsibilities.
- 2) extend the policy to include recent graduates, and
- 3) align electronic communication standards with the district’s Reporting of Child Abuse, Neglect and Inappropriate Relations Between Adults and Students 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 (including recent graduates) 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.~~ This policy also governs the electronic communications between students and CPS staff and other adults who work in schools the District.

GUIDING PRINCIPLES:

1. CPS’ department of Information and Technology Services is responsible for providing the reliable and secure technology resources and updates/upgrades necessary to foster the educational development and success of our students.
2. CPS’ department of Information and Technology Services provides a baseline set of policies and structures to allow schools to implement technology in ways that meet the needs of their students and school/parent/guardian communities.
3. CPS’ department of Information and Technology Services and Office of Teaching and Learning provide a secure framework that will allow students to use online tools, including social media and artificial intelligence/machine learning (AI/ML), in our classrooms and schools, to increase student engagement, collaboration and learning.
4. CPS’ Office of Teaching and Learning is responsible for instructing students ~~about digital citizenship, including appropriate and safe online behavior, interactions with individuals on social media and cyberbullying awareness.~~ in computer literacy, internet safety and media literacy as mandated by Illinois

state law, including the development and implementation of a mandatory, grade-appropriate K–12 AI Literacy curriculum.

5. CPS' school leaders are responsible for supervising students' use of technology in accordance with this policy and ensuring students and parent/guardian communities receive this policy.

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.

Artificial Intelligence (AI) refers to leveraging computing power to mimic human cognitive functions such as problem solving and decision making. This technology encompasses several elements, including learning from data, human feedback and recognizing patterns through machine learning.

Artificial Intelligence (AI) Literacy refers to a comprehensive understanding of AI's capabilities, limitations, ethical implications and societal impact.

Generative Artificial Intelligence (GenAI) refers to a subset of artificial intelligence. GenAI generates new content—including text, audio, code, images, or videos—based on vast amounts of "training" data, typically derived from the internet. Users are able to request and refine specific content via prompts—inputs or queries submitted to the model. Such technology not only supports creative educational tools but also enhances internet search capabilities and word processing, offering students and faculty unique ways to engage with media. GenAI includes applications, software and models.

Machine Learning (ML) refers to a subset of AI where algorithms enable systems to enhance their performance over time without human guidance. AI systems also have the ability to perceive and interpret sensory data, using tools like cameras and microphones.

Broadcast Email refers to any email which contains the same content and is transmitted en masse to school(s), department(s), parents or students from a district-authorized bulk communication tool (e.g. BlackBoard Connect/Mass Notifications).

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, chats, text, group messaging apps, video conferencing, like Google Meet, websites and podcasting.

Computer Literacy Illinois Instructional Mandate requires that all school districts shall ensure students in K-12 receive developmentally appropriate opportunities to gain computer literacy skills embedded in the district's curriculum at each grade level.

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.

CPS' Protected Categories include sexual orientation, gender or sex (includes gender identity, gender expression, pregnancy, childbirth, breastfeeding, and pregnancy related medical conditions), race or ethnicity (includes hairstyles historically associated with race, ethnicity, or hair texture, including, but not limited to, protective hairstyles such as braids, locks, and twists), ethnic group identification, ancestry, nationality, national origin, religion, shared ancestry, color, mental or physical disability, age, immigration or citizenship status, marital status, registered domestic partner status, genetic information, political belief or affiliation (not union related), military status, unfavorable discharge from military service, and any other basis listed under CPS' Comprehensive Non-Discrimination, Harassment, and Retaliation Policy.

Internet Safety Education Illinois Instructional Mandate - Required for grades 3-12 at each grade level, may be provided for in grades K-2 - A school district must incorporate into the school curriculum a component on internet safety to be taught at least once each school year to students in Grades 3 through 12. The age-appropriate curriculum may begin with students in kindergarten.

Media Literacy Illinois Instructional Mandate requires that every high school shall include in its curriculum a unit of instruction on "media literacy," defined as the ability to access, analyze, evaluate, create, and communicate using a variety of objective forms, including, but not limited to, print, visual, audio, interactive, and digital texts.

Portable Device refers to movable devices including, but not limited to, laptops, desktop computers and like-devices, tablets, wireless communication devices (e.g. Smartphones).

Recent Graduate refers to a former student, of any age, up until one year after the student has graduated. Recent graduates maintain access to their CPS email account for two years post-graduation and are required to use it for communicating with adults who work in the District for one year post-graduation.

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 X (formerly Twitter), TikTok, Discord,

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~~ their 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~~ their 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: <https://www.cps.edu/AcceptableUsePolicy/Pages/aup.aspx>.

Unwelcome Conduct may include, but is not limited to, bullying, intimidation, offensive jokes, slurs, epithets or name calling, assaults or threats, touching, ridicule or mockery, insults or put-downs, offensive objects or pictures, messages sent via email, text or social media, sexual advances, requests for sexual favors, conduct of a sexual nature, sex-based conduct and any other persistent, pervasive or severe conduct that is objectively offensive and unreasonably interferes with, limits, or denies an individual’s educational or employment access, benefits, or opportunities.

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, including information stored or transmitted over the CPS Network or in school 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 inappropriate 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~~ email, bulk communication tools (e.g. BlackBoard Connect/Mass Notifications) 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. Students are highly encouraged to use CPS-provided resources when applicable. 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, result in:

1. Causing harm to others, damage to their property or CPS property, such as behaviors and actions that are:

- a. ~~is offensive,~~ hateful, harassing, threatening, libelous, defamatory ~~discriminatory, retaliatory,~~ bullying, or otherwise meant ~~to bully or~~ intimidate others or causing emotional harm;
- b. ~~is offensive or, discriminatory, harassing, retaliatory or discriminatory to protected categories of persons based on CPS' Comprehensive Non-Discrimination, Harassment, and Retaliation Policy; race, shared ancestry 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;~~
- c. ~~Constitutes use for, or in support of, any obscene or pornographic, purpose including, but not limited to, transmitting, retrieving, creating, possessing or viewing of any profane, obscene, or sexually explicit material; 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;~~
- d. ~~constitutes~~ used for soliciting or distribution information with the intent to incite violence, cause personal harm or bodily injury, or to harass, threaten or "stalk" another individual; ~~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;~~
- e. used to engage in inappropriate sexual conduct, including unwelcomed sexual contact, indecent exposure, transmitting sexually suggestive images, or other sexual activities; conduct as defined above;
- f. used to intentionally damage a CPS device or the device(s) of others; and
- g. used to impersonates any person, living or dead, organization, business or other entity; for the sake of reputable harm or embarrassment;
- h. Creating, using, or distributing synthetic media, including AI-generated 'deepfakes,' to impersonate, defame, harass, or otherwise cause harm to any member of the school community.

2. Gaining or attempting to gain unauthorized access to the CPS Network or Computer Resources, or to any third party's computer system, such as:

- a. ~~contains a~~ intentionally sending viruses, trojan horses, ransomware or other harmful components or malicious code through any format, including but not limited to, email, chat and text.
- b. ~~constitutes~~ sending junk mail, phishing, spam or unauthorized broadcast email;

- c. ~~taking an action that~~ violates the security of any other computer or network or constitutes unauthorized access or attempts to circumvent any security measures;
- d. ~~obtains~~ access to another individual's CPS Network account, files or data, or ~~modifying-es~~ their files, data or passwords;
- e. ~~impersonating-es~~ any person, living or dead, organization, business, or other entity;
- f. ~~degrading-es~~ the performance of, ~~causing-es~~ a security risk or otherwise ~~threatening-es~~ the integrity or efficient operation of, the CPS Network or Computer Resources;
- g. ~~depriving-es~~ an authorized individual from accessing CPS Network or Computer Resources;
- h. ~~obtaining-es~~ Computer Resources or CPS Network access beyond those authorized;
- i. ~~accessing-es~~ or ~~distributing-es~~ unauthorized information regarding user passwords or security systems;
- j. ~~falsifying-ies~~, ~~tampering-es~~ with or ~~making-es~~ unauthorized changes, additions or deletions to data located on the CPS Network or school systems;
- k. ~~installing-es~~, ~~downloading-es~~ or ~~using-es~~ unauthorized or unlicensed software or third party system;
- l. ~~violating-es~~ the terms of use specified for a particular Computer Resource, CPS Network system or school system;
- m. ~~engaging-es~~ 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;
- n. ~~downloading-es~~ unauthorized games, programs, files, electronic media, and/or stand-alone applications from the internet that may cause a threat to the CPS Network;
- o. Using technology in a way ~~constitutes use~~ that disrupts the proper and orderly operation of the school; and
- p. ~~using-es of a~~ proxy servers or virtual private networks to bypass network security systems (firewalls, etc.).

3. Using the CPS Network or Computer Resources for commercial purposes, such as:

- a. ~~taking actions that~~ enables or constitutes wagering or gambling of any kind;
- b. ~~accessing-es~~, ~~distributing-es~~, ~~downloading-es~~ or ~~using-es~~ games except when ~~an~~ assigned as an educational activity;
- c. ~~promoting-es~~ or ~~participating-es~~ in any way in unauthorized raffles or fundraisers; and
- d. ~~engaging-es~~ in private business, commercial or other activities for personal financial gain.

4. Engaging in criminal, unlawful or other inappropriate activities, such as:

- a. using technology in a way that 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;
- b. using technology in a way that violates any express prohibition noted in this policy or the Student Code of Conduct;
- c. plagiarizing or misusing any information gained on or through use of the CPS Network or Computer Resources; and
- d. ~~accessing-es~~, ~~distributing-es~~ or ~~downloading-es~~ non-educational materials or inappropriate content or materials.

~~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 GPS 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 GPS Network or Computer Resources;
 12. deprives an authorized individual from accessing GPS Network or Computer Resources;
 13. obtains Computer Resources or GPS Network access beyond those authorized
 14. engages in unauthorized or unlawful entry into a GPS 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 GPS 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 GPS 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, GPS 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 GPS 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 GPS 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. CPS uses technology protection measures to block or filter internet sites for inappropriate material that is harmful to minors and prohibit access, to the extent possible, to such content found on the internet. 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.

In addition to the use of filtering technology, ITS may also block access to certain websites when required by law, when their use may interfere with the optimal functioning, or when among other things, the website may compromise the security of the CPS network or computer resources. ITS shall establish standards and procedures by which individual websites may be authorized for blocking or unblocking of access from the CPS computer network or otherwise disabling or modifying the district's technology protection measures. All blocking and unblocking decisions will be made by ITS in compliance with applicable laws and the requirements of this policy. Technology protection measures may be disabled for district administrators, supervisors or other authorized staff to access materials via the internet for bona fide research, legitimate educational purposes or other lawful purposes.

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 passwords under any circumstances.

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 their access may be suspended or revoked.

G. Artificial Intelligence. CPS is committed to equipping students with AI Literacy to ensure students have the tools and knowledge to thrive in the age of AI. ITS is responsible for ensuring AI systems are responsibly developed, human-centered, thoroughly tested, and continuously monitored to promote dynamic, forward-looking and continuous learning and innovation solutions for the classroom. Students must use CPS approved tools. For CPS guidance and ethical use of AI, review the AI Guidebook at cps.edu/aiuidebook.

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

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~~ the district, 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 the district, ~~a school~~, except when authorized under sections VI.B.5 and 6 below.

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

3. ~~All High Schools~~ students, and recent graduates within one year of graduation, are prohibited from communicating with CPS staff and other adults who work in the district schools via personal email, text messaging, instant messaging, social media or telephone, except when authorized under sections VI.B.5 and 6 below, and except for authorized pre-approved safety meet-up communications, including field trips where:

- a. The parent/guardian and principal both provide prior written permission to ~~the~~ text messaging, instant messaging, and telephone communications, and
- b. Communications are sent as group texts/messages with the parent/guardian on the text message or instant message, and also include the staff/adults' CPS email address as a recipient of the message for proper retention of communications.

4. Students may receive bulk text notifications and alerts on their ~~personal~~ mobile devices from their school when their parent/~~or~~ guardian provides written permission to enroll and receive these text notifications and alerts. Consent forms are available at <https://www.cps.edu/about/policies/acceptable-use-policy/resources/>.

5. Students ages 15-21 in grades 4—12 enrolled in a CPS Program for Re-Engagement to High School of Out-of-School Youth, Attendance and Truancy (Chronic Truants), the Student Outreach and Re-Engagement Centers (SOAR), Juvenile Justice (JJ) teams, or Juvenile Justice Re-Entry Program Students Exiting Juvenile Detention Facilities ("Program") may communicate via text, instant message with the CPS staff member(s) assigned to the student when authorized in writing by the Program manager. The requirements for a student to phone, text, or instant message 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, or instant message communications with a CPS staff member 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, or instant message communication with a CPS staff or other adult who works in a school, and (b) abide by the text, or instant message 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 the district 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 adults who work in a school.

D. Social Media. Students shall not communicate with CPS staff and other adults who work in the ~~district 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 to communicate with CPS staff members or other adults who works in ~~the district a school~~.

E. Other Electronic Communications. Students are prohibited from communicating with CPS staff and other adults who work in ~~the district 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~~ Connect/Mass Notifications).

F. Exceptions.

1. Nothing in this section shall restrict communications between a student and their parent/guardian or other family members;

2. Nothing in this section shall restrict 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.

3. Out of school youth, vulnerable or highly mobile youth that do not have an active CPS email accounts or if the contact is of urgent nature and it is not possible to arrange a CPS email account in time to address the situation may communicate via their personal email account to CPS staff's CPS issued email account.

G. Reporting Improper Contact. Any student or parent/guardian who believes a CPS-affiliated adult (including staff, administrators, contractors, and volunteers) has engaged in conduct that violates standards for professional staff/student boundaries outlined in the district's Reporting of Child Abuse, Neglect and Inappropriate Relations Between Adults and Students policy (Section I.G), including by sending a communication to ~~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 by asking~~ is asking the student to provide contact information for this purpose should (except when authorized above) should:

1. Immediately notify ~~their parent/guardian and principal or school administrator~~ their

~~parent/guardian and principal or school administrator;~~ with "a trusted staff member at the student's school, such as a principal, teacher, or counselor; or

2. If a student or parent/guardian experiences barriers to notifying a trusted staff member at the student's school, the student or parent/guardian should directly notify the Office of Student Protections and Title IX (OSP) by filing an online complaint form at www.cps.edu/osp, calling (773) 535-4400, or emailing osp@cps.edu; and

3. Show or provide a copy or details of the communication to their parent/guardian and also the principal or school administrator suspected professional staff/student boundary violation communication to the trusted staff member of OSP.


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 the Student Code of Conduct.


IX. Student Protections. Every student has the right to a safe and supportive environment free of discrimination, harassment, abuse and retaliation. Title IX is a federal civil rights law that does not allow discrimination on the basis of sex in schools and school activities including all of Chicago Public Schools. Title VI is a federal civil right law that does not allow discrimination on the basis of race, color, and national origin. Additionally, the Office of Student Protections and Title IX works to ensure students are safe from all sexual misconduct, bias-based harm and abuse. If a student is harassed, intimidated, or bullied based on a CPS protected category or threatened through the CPS Network, Computer Resources or otherwise, they should contact their principal or the Office of Student Protections & Title IX, via email at osp@cps.edu, Online Complaint, phone: 773-535-4400, by mail or in-person at 110 N Paulina St. Chicago, IL 60612.

Amends/Rescinds	Amends 18-0822-PO4 <u>19-0828-PO2</u>
Cross References	03-0326-PO03; 02-0626-PO04; 97-0326-PO2; <u>22-0622-PO2</u>
Legal References	<u>105 ILCS 5/27-13.3: Protecting Children in the 21st Century Act, Pub. L. No. 110-385, Title II, 122 Stat. 4096 (2008); 47 C.F.R. 54.520; Children's Internet Protection Act, 47 USC 254(h); Federal Communications Commission Report and Order FCC 11-125. 105 ILCS 5/10-20.79; 10-20.74, 105 ILCS 5/27-13.3 and 105 ILCS 5/27-20.08</u>


Approved for Consideration:

DocuSigned by:

393B2FEE544446B
Edward Wagner
Deputy Chief Information Officer

Approved:


Signed by:

B0E10BAC8D764AF...
Macquiline King, Ed.D
Interim Superintendent/Chief Executive Officer

Approved for Consideration:

Signed by:

C10AFFB2AB0749E...
Nicole Milberg
Chief Teaching and Learning Officer

Approved as to Legal Form:

^{Initial}
LB

Signed by:

974F0DEB7385497...
Elizabeth Barton
Acting General Counsel