**August 28, 2019**

**AMEND BOARD REPORT 18-0822-PO2**
**~~AND ADOPT A NEW~~ STAFF ACCEPTABLE USE POLICY**

**THE CHIEF EXECUTIVE OFFICER RECOMMENDS:**

That the Board ~~rescind~~ amend Board Report ~~09-0722-PO3~~ 18-0822-PO2 ~~adopt a new~~ Staff 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 that message retention rules will apply to approved usage for field trips.

**PURPOSE:** Chicago Public Schools (CPS) provides access to technology devices, internet, data and network systems to employees and other authorized users for educational and business purposes. This Staff Acceptable Use Policy (AUP) establishes the standards for acceptable electronic activity of employees and other authorized Users using and accessing the district or school technology, internet, data and network systems regardless of the User's physical location and also the electronic communication between students and CPS staff.

**GUIDING PRINCIPLES:**

1. CPS has a legal obligation to protect the personal data of our students, families, and staff.
2. CPS provides a baseline set of policies and standards to allow schools and district offices to implement technology in ways that meet the needs of their staff.
3. CPS recognizes that social media technology and online tools can provide a means to enhance education, communication, community engagement and staff and student learning.
4. CPS is obligated to ensure that staff use technology appropriately and in support for educational and business purposes.

**POLICY TEXT**:

**I. Applicability.** This policy applies to all Board employees serving in any capacity, interns, vendors, consultants, contractors and authorized agents and volunteers who use Board computer resources and/or access the CPS network ("Users"). Personal electronic devices (*e.g.* personal laptops) are subject to this policy when such devices are connected to the CPS Network or Computer Resources.

**II. Delegated Authority.** The 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.**

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).

Children's Internet Protection Act (CIPA) refers to the federal law that requires schools that receive federal funding through the E-Rate program to use internet access filtering to protect students from content deemed harmful or inappropriate. 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 (*e.g.* CPS Google Classroom), blogs, group messaging apps (*e.g.* CPS Google Hangouts), video conferencing, websites and podcasting.

Computer Resources refers to all computers, electronic devices and information technology, whether stationary or portable, used to conduct the day to day business of CPS and the Board, 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 hereunder.

Department/School Management refers to the supervisor, manager, director, officer, principal, Network Chief or other employee of the Board designated by his/her department or office or school to implement policy compliance requirements.

Family Educational Rights and Privacy Act (FERPA) refers to the federal law that protects the privacy, accuracy, and release of student information and records. For more information, visit http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

HIPAA refers to the Health Insurance Portability and Accountability Act of 1996, the federal law that provides data privacy and security provisions for safeguarding medical information. For more information, visit https://www.hhs.gov/hipaa/index.html.

ISSRA refers to Illinois School Student Records Act (105 ILCS 10/1 et seq.), the state law that protects the privacy, accuracy, and release of student information and records. For more information, visit http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=1006&ChapterID=17

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

Remote Access refers to the CPS virtual private network which allows for secure entry from a location outside the CPS Network to portions of the CPS Network or Computer Resources that are subject to two factor authorized access credential requirements.

Personally Identifiable Information (PII) refers to sensitive data and information that must be protected against unwarranted disclosure such as student information, private employee information and protected health information that can adversely affect the privacy or welfare of an individual.

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 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.

## IV. Duties.

A. Department of Information & Technology Services (ITS) Duties: ITS is responsible for designing, establishing and maintaining the CPS Network and Computing Resources, assisting Users in all CPS departments, offices and schools in implementing and maintaining electronic information management and security practices at their respective locations. ITS shall establish and issue procedures, standards, training requirements and guidelines as necessary to implement the requirements of this policy or to specify the terms of use for a particular CPS Network system or Computer Resource (collectively referred to as "ITS Guidelines").

B. Department/School Management Duties: Department/School Managers are responsible for designating Users authorized to access and use the CPS Network and Computer Resources and providing for their individualized access to specific CPS Network systems based on job duties. Department/School Management shall enroll and terminate User access to the CPS Network and Computer Resources in accordance with ITS Guidelines. Department/School Management will approve access to the CPS Network and Computer Resources by Users who are not Board employees, such as consultants or contractors, only when access is required to perform critical functions and services, and only upon the consultant's/contractor's successful completion of criminal background screening and execution of a confidentiality agreement regarding such access and use.

C. User Duties:

1. *Communications with Students.* Users who communicate with students electronically (a) must do so using ITS-authorized CPS Network systems (*e.g.* CPS email, CPS Google Classroom, BlackBoard Connect, etc.), except for any express exception noted in this policy or the ITS guidelines (*e.g.* see section VIII. and IX.); (b) shall communicate regarding classroom, school and school-related activities only; and (c) shall exercise best professional judgment, integrity and concern for student well-being. Communications with students for fraternization purposes are strictly prohibited, except communications between family members.
2. *Duty to Protect.* Users have a duty to protect the security, integrity and confidentiality of the CPS Network and Computer Resources including the obligation to protect and report any unauthorized access, use, abuse, misuse, injury, degradation, theft or destruction.
3. *Compliance.* Users shall complete all mandated AUP-related training and know their responsibilities outlined in this policy. Users shall comply with this policy and all ITS Guidelines when using the CPS Network or Computer Resources.

## V. Ownership and Privacy.

A. Board Property. All documents, data and information stored, transmitted and processed on CPS Network or Computer Resources are the property of, and subject to, the Board's policies, rules as well as ITS Guidelines and standards on usage. Users shall ensure that all access and use of such documents, data and information complies with applicable laws and Board rules and policies including those related to the Confidentiality of Student Records and Email Retention. When a User is no longer employed or under contract with the Board, all information stored by that User on CPS Network and Computer Resources remains the property of the Board.

B. Privacy. Users have no expectation of privacy in their use of the CPS Network and Computer Resources. By authorizing 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, Computer Resources or school systems. CPS reserves the right to access, review, copy, store, or delete any files stored on Computer Resources and all User communication using the CPS Network. Electronic messages and files stored on CPS computers or portable devices or transmitted using CPS systems are treated like any other school property. District administrators may review files and messages to maintain system integrity and, if necessary, to ensure that Users are acting responsibly and in compliance with this policy and related guidelines. CPS may choose to deploy location tracking software on devices for the sole purpose of locating Computer Resources identified as lost or stolen.

C. Data & Systems. A User's access to view, edit, or share student information, records or data located on the CPS Network or Computer Resources must abide by local, state, and federal regulations, including FERPA and ISSRA. Student information, records and data may only be shared with individuals deemed eligible to have access as set out in FERPA, ISSRA and Board Policy and guidelines regarding the confidentiality of student records.

D. Personally Identifiable Information (PII). When sensitive information, including student records, private employee information or protected health information is transmitted or shared electronically, Users are expected to exercise reasonable efforts to protect the privacy of the information and only use CPS-approved secure channels to transmit data. Use of portable storage media such as a USB/flash/thumb drive to share PII is strictly prohibited. Further, Users must ensure that PII record transmissions reach only to those individuals with a right to said records and must take reasonable measures to ensure that only the intended recipients are able to access the PII.

E. Monitoring. 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. The CPS Network including, but not limited to, internet and email usage may be monitored and audited by the Department/School Management, ITS and other authorized CPS oversight departments for inappropriate activity or for oversight and audit 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 User 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 other messaging services for business, legal or security purposes.

F. Manager Access. Department/School Management may access documents, data and information generated, stored, transmitted or processed by a User on the CPS Network and Computer Resources in accordance with ITS Guidelines. A User's manager may also access a User's CPS Network account for business purposes, including oversight purposes, regardless of whether the User is present or absent. In all cases, the Department/School Management shall contact the ITS Service Desk at 773-553-3925 to obtain access. Managers shall not ask Users to share their password for such purposes.

## VI. General Provisions.

A. Business Use. All Users must use the CPS Network and Computer Resources in a professional, ethical and lawful manner in compliance with all Board Rules and policies. Use of the CPS Network and Computer Resources is a privilege that is provided to help Users perform their job responsibilities.

B. Personal Use. Use of the CPS Network and Computer Resources is intended for Board business, with limited personal use permitted. Such personal use must in all circumstances comply with this policy, must not result in costs to the Board, cause legal action against the Board or cause any adverse consequence to the Board. Such use must also be appropriate as to duration and not interfere with the User's duties and the Board's business demands. Excessive use or abuse of these privileges can be deemed in violation of this policy and subject the User to discipline.

C. Unacceptable Use. Unacceptable use of the CPS Network and Computer Resources is prohibited. Users 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 or defamatory;
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 User'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 User of access to 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. discloses Board trade secrets, or confidential or proprietary information, including student record information, without authorization or without proper security measures;
16. discloses personally identifiable student information, videos and photographs without authorization or without proper security measures;
17. shares confidential information about students or CPS personnel in a manner that violates state law, federal law, Board rule, policy or guideline;
18. shares CPS email addresses or distribution lists for uses that violate this policy or any other Board policy;
19. enables or constitutes wagering or gambling of any kind;
20. accesses, distributes, downloads or uses games except when an assigned educational or training activity;
21. promotes or participates in any way in unauthorized raffles or fundraisers;
22. promotes or participates in any way in partisan political activities;
23. promotes or participates in any way in internal political or election activities related to a union or other organization representing employees;
24. engages in private business, commercial or other activities for personal financial gain;
25. distributes unauthorized information regarding other User's passwords or security systems;
26. transmits PII without appropriate security safeguards;
27. falsifies, tampers with or makes unauthorized changes, additions or deletions to data located on the CPS Network or school systems;
28. accesses or uses data located on a CPS 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. installs, downloads or uses unauthorized or unlicensed software or third party system;
31. violates the terms of use specified for a particular Computer Resource or CPS Network system;
32. constitutes use that disrupts the proper and orderly operation of a school or office;

33. engages in hacking (intentionally gaining access by illegal means or without authorization) into the CPS Network to access unauthorized information, or to otherwise circumvent information security systems;
34. engages in inappropriate sexual conduct, including unwelcomed sexual contact, indecent exposure, transmitting sexually suggestive images, or other sexual activities;
35. downloads unauthorized games, programs, files, electronic media, and/or stand-alone applications from the internet that may cause a threat to the CPS Network;
36. violates federal or state law or any Board rules, policies, standards or guidelines regarding the protection of employee or student privacy or the confidentiality of employee or student records; or
37. violates any prohibition noted in this policy or any other Board policy.

D. Intellectual Property Requirements. No User may transmit to, or disseminate from, the CPS Network any material that is protected by copyright, patent, trademark, service mark or trade secret unless such use or disclosure is properly authorized and bears the appropriate notations. No User may download, upload or share materials in violation of U.S. patent, trademark or copyright law.

E. Software Licenses. All software used by Users must have a valid license. Users shall use only authorized software in compliance with the licenses provided to or by the Board. Users may install authorized software that is deemed necessary for business use by Department/School Management. Such software must not compromise the security or integrity of the CPS Network or Computer Resources and must not interfere with the proper functioning of required CPS software. ITS may remove User 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.

F. Network Usage. CPS Network access and bandwidth is provided to schools for academic and operational services. CPS reserves the right to prioritize network bandwidth and limit certain Network activities that are negatively impacting academic and operational services. Use of proxy servers or virtual private networks to bypass Network security systems (firewalls, etc.) is strictly prohibited.

G. Network Security. The CPS Wide Area Network (WAN) infrastructure, as well as the building-based Local Area Networks (LANs) are implemented with performance planning and appropriate security measures in mind. Modifications to an individual building network infrastructure and/or use will affect LAN performance and will reduce the efficiency of the WAN. For this reason, any additional Network electronics including, but not limited to, switches, routers, and wireless access points must be approved, purchased, installed, and configured solely by ITS to ensure the safety and efficiency of the network. Users are prohibited from altering or bypassing security measures on electronic devices, Network equipment, and other software/online security measures without the written consent of the CIO. Anyone utilizing the CPS Network understands and acknowledges that CPS security systems may intercept and decrypt traffic in order to analyze traffic for security risks or content filtering purposes. Devices connected to the CPS Network may be disconnected if any security risk is identified that places the rest of the Users, Network systems, Computer Resources or data at risk. Situations would include but not limited to devices infected with malware, unauthorized network scanning systems and applications that bypass Network security.

H. 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 Management to ensure the filter meets the academic and operational needs of each school while protecting minors from inappropriate content. Additionally, under an ITS-managed program to allow schools limited controls over the web content filtering policies for their relevant schools, a school principal or their designee may be provided secure access to the web content filtering systems. School staff with access to manage the policies affecting the Internet must ensure the district does not violate CIPA or other compliance requirements. The principal will ensure the school remains in compliance with all requirements to participate in the program as set by ITS, otherwise access to the additional controls will be revoked and the school web content filtering policies will be reset to the current district-wide policy settings.

I. Remote Access. Remote access to the CPS Network is allowed only through ITS-authorized remote access solutions and will always require two factor authentication.

J. Third Party Systems. CPS provides Users with the means to communicate through a variety of district-owned or leased systems located on the CPS Network in order to effectively conduct district operations. Users may not circumvent the requirements of this policy or other Board policies by using a third party system to communicate when a similar system is otherwise available on the CPS Network. To the extent that a particular system is not available on the CPS Network, User's use of a third party system is subject to approval by the Chief Information Officer (CIO) or designee. If approved, such use is subject to the requirements of this policy and other applicable Board policies as well as any other requirements specified by the CIO. In such cases, the User is solely responsible for ensuring compliance with all such policies and requirements. Nothing herein is intended to limit prior Board mandates for Users to use only the Board's email system, student information system, remote access solution and any other mandates that may be established in the future by the CIO or the Board.

K. New Technologies. The requirements of this policy apply to all technologies currently in use on the CPS Network, those technologies authorized by ITS for use by a school, office or departments, and those technologies that may be used in the future on the CPS Network. ITS shall establish guidelines on the use of any new technology approved for use on the CPS Network or for use by a school, office or department.

L. Passwords. Users are required to adhere to password requirements set forth by CPS when logging onto the CPS Network or Computer Resources directly or via remote access. Users are not authorized to share their password under any circumstance.

M. Unauthorized Access and Data Tampering. Users are prohibited from (1) using their authorized access to a CPS Network system to falsify, misreport, misrepresent, make unauthorized changes or deletions or otherwise tamper with CPS data; and (2) entering, changing, moving or copying data in a CPS Network system that the User has no access or entry authorization rights to such system. Any entry, modification or deletion of CPS data by an unauthorized User is considered tampering and is prohibited. Users are subject to discipline for any unauthorized access to a CPS Network system or Computer Resources and for their acts or omissions that allow others to gain unauthorized access.

**VII. Email.**

A. Usage. Users are not allowed to use a personal, third-party email account (*e.g.* Hotmail, Yahoo, etc.) in their capacity as representatives of CPS. Email sent by Users in their capacity as representatives of the CPS must be sent from their CPS email account, with Board authorized return addresses. User emails are subject to retention by ITS in accordance with the Board's Email Retention Policy. If a User inadvertently sends or receives an email related to their work duties on their personal email account, the User shall forward the email(s) to their CPS email account.

B. Confidentiality. Users must exercise due care to ensure that email messages containing PII or confidential information conform to the confidential transmission requirements noted herein and are transmitted only to their intended recipients. Users are prohibited from transmitting Social Security Number (SSN) information via email without the prior written approval of ITS and when authorized must comply with ITS security standards established for SSN transmission. Users shall abide by the ITS Guidelines and standards on the classification, handling and email transmission of PII and other confidential information, including applicable encryption requirements.

When communicating with a student's parent/guardian, Users should use verified email addresses listed in the Board's student information system, unless steps have been taken to verify an alternate email address to ensure the communication is provided to the proper persons with authorization to receive information regarding the student.

C. Broadcast Emails. The Office of Communications shall establish guidelines by which broadcast emails may be authorized for distribution. Users may transmit broadcast emails only when authorized in accordance with such guidelines. Any links to attachments on broadcast emails must be hosted on a CPS-authorized source and vetted to ensure that the file does not contain PII or confidential information and must comply with ITS security standards established for the bulk communication tool.

D. Freedom of Information Act (FOIA). Any communication sent by or to a User using the CPS Network or Computer Resources could be subject to public access requests submitted through FOIA. Further, data and other materials and files maintained on the CPS Network or Computer Resources may be subject to review and disclosure under FOIA or discovery. Use of personal email accounts, personal social media and other personal electronic communication systems to conduct school business is prohibited and may cause a User's personal accounts to be subject to FOIA and other inquiries.

**VIII. Mobile Device Communication.**

A. Use of Mobile Devices for CPS Business. Use of a Board-Issued Mobile Device or Personal Mobile Device to conduct district business must comply with the mobile device use standards issued by the CIO. The standards shall, at a minimum, require a User to properly retain text and call records generated while using a mobile device for business purposes and comply with the Board's record retention policies and retention schedule established to comply with the Illinois Local Records Act.

B. Mobile Device Communications with Student(s). Users are prohibited from communicating with a student via (1) a student's mobile device, whether phone, text or ~~IM~~ instant message, (2) a student's personal email account (communications to the student's CPS email account is permitted), (3) any Personal Social Media account or non-CPS Social Media account, and (4) any group messaging app other than the CPS-provided or approved app (currently CPS-Google Hangouts), subject to the following exceptions:

1. Pre-Approved Safety Meet-Up Communications. Staff ~~Users~~ may communicate with students in grades 9-12 via phone, text messaging or ~~IM~~ instant message when necessitated by an educational or extra-curricular activity including field trips, for purposes of ensuring student safety, and:
   (a) the parent/guardian and principal both provide prior written permission to the phone text message or ~~IM~~ instant messaging communications using the CPS form established for such purpose, and
   (b) communications are sent as group texts/messages with the parent/guardian on the text message or ~~IM~~ instant message and also the ~~User's~~ Staff's CPS email address as a recipient of the message for proper retention of communications.

2. Approved Bulk Text Notifications and Alerts to Students. Schools may utilize a bulk text notification system that delivers group text notifications and alerts to a student's personal cell phone, provided that:
   (a) the notification system is authorized by the CIO or designee upon information security and records retention compliance review;
   (b) the parent/guardian provides prior written permission for their child to receive the text notifications/alerts; and
   (c) the parent/guardian receives the same text notifications/alerts sent to their child when the parent/guardian elects to receive these notifications/alerts.

3. CPS Programs for Re-Engagement of Out-of-School Youth, Chronic Truants, the Student Outreach and Re-Engagement Centers (SOAR), Juvenile Justice (JJ) teams and Students Exiting Juvenile Detention Facilities approved by the Chief Executive Officer (CEO-Approved Re-Engagement Programs). CPS staff members who are responsible for student outreach efforts under a CEO-Approved Re-Engagement Program may communicate with students in grades ~~7~~4-12 via phone, text messaging or ~~IM~~ instant messaging or email from a CPS staff member's CPS email account to a student's personal email account provided that the CPS staff member:

(a) complies with the parent/guardian permission requirements established by the CEO for staff/student text communications under the Program;

(b) complies with the group texts/messages requirements established by the CEO to include other staff member(s) or the parent/guardian on the staff/student text communications;

(c) complies with any other requirements established by the CEO for such text, ~~/IM~~ instant message and phone communications with a student for Program purposes, and

(d) includes the staff member's CPS email address, or other CPS email address, as a recipient on the message identified by the CEO, on all texts ~~/IMs~~ or instant messages for proper records retention.

4. CEO-Approved Exceptions. The CEO may authorize exceptions to this policy to permit User/student text ~~/IM~~ or instant message communication where the CEO determines it is in the best interest of the student to authorize User/student electronic communications outside the CPS Network. In such instances, the CEO shall establish the parent consent, group text and other requirements necessary to ensure student safety and proper records retention. A User must (a) receive written authorization from the manager of the CEO-authorized program to engage in text~~/IM~~ instant message communication with a student, and (b) abide by the terms and conditions established by the CEO for text~~/IM~~ or instant message communication with students under the authorized program. The User shall include their CPS email address, or other CPS email address identified by the CEO, as a recipient of the message on their text ~~/IM~~ or instant message communication with students to ensure proper records retention.

## IX. Social Media / Online Communication.

A. General.

1. Communication with Students. Users are prohibited from communicating with current CPS students on Personal Social Media and Non-CPS Social Media except as expressly described herein. Users are permitted to communicate with current CPS students on CPS Social Media as described herein.

2. Confidential Information. Posting, sharing or other disclosure of personally identifiable student information (including information that can be traced back to a specific student or could allow a student to be publicly identified), private employee information or other CPS confidential information on Social Media is prohibited, provided, however, that student work, images and accomplishments may be posted on CPS Social Media with prior written parent/guardian consent.

3. Modeling Civil Online Behavior. Users serve as role models for students and as such are responsible for the information they post, share or respond to online. Users are responsible for modeling and actively practicing positive digital citizenship. Users are prohibited from using Social Media, in a manner that:

(a) disparages or demeans any student, parent/guardian or family member, User or school community member (e.g., LSC member, community member, alumni); or

(b) is offensive or discriminatory based on race, ethnicity, national origin, gender, gender identity, sexual orientation, age, physical or mental illness, disability, marital status, economic status, immigration status, religion or personal appearance or other visible characteristics.

4. Disruption. While Users may comment on matters of public concern, Users should be aware that their online activity has the potential to result in disruption at school and/or the workplace and such disruption can be a violation of this policy, other Board policies or laws and subject a User to discipline. Any User whose online activity is excessively disruptive to, or detracts from, the efficient or effective operations of the Chicago Public Schools, may be subject to discipline. Users who are managers are also subject to discipline if their online activity is critical of CPS, the Board, district leadership, policies, mandates, strategies or directives.

5. Concerted Activity. Nothing herein shall restrict Users with bargaining unit membership or Users eligible for bargaining unit membership from engaging in concerted activity regarding their working terms and conditions.

6. Any User who inappropriately uses Social Media during school/work hours or outside of school/work hours is subject to discipline.

B. Personal Social Media.

1. Users shall not use Personal Social Media to conduct CPS business, act in their capacity as a CPS employee or agent or otherwise express viewpoints as an employee or agent of CPS.

2. Users may not use their CPS email address for Personal Social Media activities.

3. In order to maintain a professional and appropriate relationships with students, Users shall not communicate with current CPS students via Personal Social Media or Non-CPS Social Media. Users shall not add any current CPS student, regardless of age, as 'friends', followers or contacts on a Personal Social Media account. This provision is subject to the following exceptions: (a) communication with the User's family members, and (b) if an emergency situation requires such communication, in which case the User shall notify his/her supervisor of the contact within 24 hours and send a copy of the communication to the User's and supervisor's CPS email account so that it can be retained in accordance with CPS records retention requirements.

4. Nothing herein prohibits communication with CPS graduates or former CPS students who are over the age of 18.

C. CPS Social Media.

1. CPS Social Media may be established to notify the school community of important matters, cover school events, recognize employees who are making a difference, recognize student accomplishments and to convey school announcements and messages of interest to the school community. To create a CPS social media presence, schools and departments should contact the Communications Department at digital@cps.edu for assistance to set up their site or to modify previously established sites to conform with this policy.

2. Users shall comply with the requirements set out in CPS Social Media Guidelines established by the Chief Communications Officer which govern the establishment, use and maintenance of any district, department or school-based Social Media site and shall include:

(a) Requirements to ensure school-based social media sites are approved by the principal and requirements for district and departmental social media sites to be approved by the requisite officer;

(b) Standards and requirements for preferred site platforms, site set-up, administrator access, regular monitoring, removal of inappropriate content, use of district logos, content restrictions, privacy controls, follower, friends and re-share standards, trusted source restrictions and standards to identify the site as a CPS site;

(c) Requirements to ensure that before posting any student image, work or accomplishment, the User must verify that the student has a current signed CPS Media Consent Form on file with the school. Posts musts be deleted and reported to the principal if a signed media consent form is not on file with the school;

(d) Requirements to ensure that Users utilize a CPS Social Media account (not a Personal Social Media account) when commenting or conveying information on behalf of CPS on a non-CPS Social Media Site and only when authorized to do so by the User's supervisor;

(e) Requirements regarding User communication with parents/guardians using Social Media; and

(f) Requirements for use of future Social Media platforms and features as developed.

3. The CPS Social Media Guidelines shall also establish the terms and conditions upon which a User may create a social media site for the purpose of communicating with students in his/her class, program, sports team or club and shall include, at a minimum, the following:

(a) The principal must approve in writing the establishment of a social media site for a class, program, sports team, club or other student group and approval shall be valid only for one school year.

(b) Approved CPS Social Media shall be used to address reasonable instructional, educational or extra-curricular program goals.

(c) The site shall be visibly identified as a school/CPS site and shall utilize and maintain appropriate privacy controls.

(d) The principal or designee shall regularly monitor the site(s) for questionable or inappropriate communications or behavior and shall have account administration rights to remove any posting or disable a page, or any other action necessary to ensure a safe and suitable school and learning environment.

(e) The principal or designee is responsible for maintaining a current list of all school-based social media accounts that have been approved for their school.

(f) The principal shall ensure that parents/guardians are notified of the school-based Social Media activities their child will be invited to participate in and of the purpose and nature of such access and activities.

(g) The User(s) responsible for the site shall educate students about responsible digital citizenship, which includes appropriate and safe online behavior, interactions with individuals on social media and also cyberbullying awareness and reporting.

4. Users who utilize CPS Social Media are expected to maintain professionalism at all times.

5. Notwithstanding anything in this policy to the contrary, ITS and the Office of Communications are authorized to identify appropriate Social Media platforms and related standards to enable classroom to classroom communications between CPS students and students from another city, state or country for educational purposes. These standards shall specify appropriate privacy, monitoring and other controls.

## X. Management of Computer Resources.

A. Device Support. CPS provides basic installation, synchronization and software support for CPS-issued electronic devices. Devices must be connected to the CPS Network on a regular basis to receive an up-to-date software and antivirus updates and for inventory purposes. Password protection is required on all CPS-issued electronic devices to prevent unauthorized use in the event of loss or theft. Users are responsible for making periodic backups of data files stored locally on their devices.

B. Damage/Loss/Theft. Users must take reasonable measures to prevent a device from being damaged, lost or stolen. In the event an electronic device is lost or stolen, the User is required to immediately notify their direct supervisor, and the ITS Service Desk (773-553-3925). The User must file a police report and document the event in the district's incident reporting system. CPS will take all reasonable measures to recover the lost property and to ensure the security of any information contained on the device.

C. Return of Electronic Devices. All technology purchased or donated to CPS is considered district property and any and all equipment assigned to employees must be returned prior to leaving their position in the same working condition. All equipment containing PII or other confidential information must be returned directly to ITS, the Department/School Manager or designee before it can be redeployed.

D. Energy Management. CPS strives to reduce its environmental footprint by pursuing energy conservation efforts and practices. The district reserves the right to adjust power-saving settings on electronics to reduce the energy consumption.

E. BYOD (Bring Your Own Device) & Personal Electronic Devices. The use of personal electronic devices (i.e. personal laptop) on the CPS Network is permitted at the discretion of the Department/School Manager. CPS is not responsible for the maintenance and security of personal electronic devices and assumes no responsibility for loss or theft. The district reserves the right to enforce security measures on personal electronic devices when used to access the CPS Network and system tools and remove devices found to be in violation of this policy.

**XI. Protected Storage.** Hard drives that contain PII must be securely protected with a password and/or encrypted to ensure the safety of the data contained therein. A list of approved services for storage or transmission of files containing sensitive information is available on a guidance website at www.cps.edu/aupguidelines. Users shall use ITS-approved data/information systems for the storage and transmission of sensitive data whenever possible and avoid storage on local hardware that cannot be secured.

**XII. Drones.** Federal and state laws refer to the flying objects commonly known as drones as unmanned aircraft systems (UAS) or unmanned aerial vehicles (UAV). These terms generally mean a small aircraft that can be flown remotely by an operator on the ground. School-owned drones must be reported on the school's asset registry in accordance with the Asset and Inventory Management Policy along with the drone's the Federal Aviation Administration registration documents.

**XIII. Reporting.** Users shall immediately report to the ITS Service Desk 773-553-3925 and their Department/School Management any actual or suspected:

A. Security violations or breaches, including, but not limited to:
   1. improper transmission of PII or other confidential information;
   2. compromised passwords or access codes;
   3. receipt of messages containing suspected virus content;

B. Theft or loss of Computer Resources including Portable Devices;
C. Misuse or abuse of CPS technology;
D. Unacceptable use of the CPS Network or Computer Resources; and
E. Any other violation of this policy.

**XIV. Policy Violations.** The district believes that technology devices, internet, and data systems, when used appropriately, provide a critical part of the district's mission of educating all of its students. When these same technology devices, internet, and data systems are used inappropriately, however, harm to the district, Users and students may result. Further, when personal devices, social media and other online tools and sites are used inappropriately, harm to the district, Users and students may result. Accordingly, any User that violates this Policy shall be subject to consequences which include, but are not limited to, the following:

A. Suspension or cancellation of use or access privileges;
B. Payments for damages or repairs;
C. Discipline under appropriate district discipline rules, policies and guidelines, up to and including termination of employment;
D. Contract penalties in accordance with the contractor/vendor/consultant's contract with the Board;

E. Exclusion of an intern, volunteer, or employee of a vendor, consultant or contractor from serving CPS in any capacity;
F. Exclusion from Board premises; and
G. Civil or criminal penalties.

Whenever a violation of this Policy results in physical or psychological harm or injury to a student or minor, or the potential thereof, then the district shall not hesitate in seeking the most severe discipline and penalties allowed under the law. Use of the CPS Network and Computer Resources is a privilege, not a right. By using CPS technology systems and devices, the User agrees to follow all CPS regulations, policies and guidelines. Abuse of these privileges may result in one or more of the following consequences set forth above.

**XV. Policy Guidance and Support.** ITS will provide platform specific guidance and best practice process guidance via website at www.cps.edu/aupguidelines. Schools will be provided materials to promote staff awareness on both practice and policy before the start of each school year in the ITS School Preparedness Guide, updated annually.

**Approved for Consideration:**

**Phillip B. DiBartolo**
**Chief Information Officer**

**Approved:**

**Janice K. Jackson**
**Chief Executive Officer**

**Approved for Consideration:**

**LaTanya D. McDade**
**Chief Education Officer**

**Approved as to Legal Form:**

**Joseph T. Moriarty**
**General Counsel**