Staff and Student Acceptable Use Policy Updates

August 22, 2018

Chicago Public Schools

Overview

- **Vision for Change**
- **Current Policies and Opportunities for Improvement**
- **Highlights: General Changes**
- **Staff Policy Updates**
- **Student Policy Updates**
- **Socializing the Change**
- **Communications Calendar**
- **Student/Parent Outreach**
- **Security Certification Program**

Vision for Change

The primary drivers for the proposed changes to both the staff and student acceptable use policies support each of the three core components of the larger organizational mission.

Academic Progress: Existing policies have not kept pace with the proliferation of online educational tools and, absent action, the gap will continue to increase. The lack of guidance inherently undermines our ability to leverage new technologies in the classroom and puts our teachers at a disadvantage.

Integrity: The proposed policies are geared to address a significant gap in explicit guidance to students and staff for general use of the CPS network. Moreover, the proposed changes support our increased focus on information security, as the policies touch on key elements related to data privacy and acceptable online behavior.

Financial Stability: These policies establish a foundation upon which we can begin to inventory the different platforms in use at a school level, allowing us to identify ‘safe’ tools and subsequently use the size of the district to obtain more competitive pricing.

Current Policies and Opportunities for Improvement

Staff Acceptable Use Policy

Last Updated = 2009

Policy Reference = 09-0722-P03

Improvement Targets

- No mention of social media, cell phone guidelines or related rules of engagement.
- Technical language required updating.
- Lack of delegated authority provision undermines the district's ability to be nimble in providing guidance in support of the policy.

Student Acceptable Use Policy

Last Updated = 2003

Policy Reference = 03-0326-PO03

Improvement Targets

- No mention of social media, cell phone guidelines or related rules of engagement.
- Technical language required updating.
- Lack of language providing student with a formal outlet to report unauthorized online behaviors by staff or other students.

Highlights: General Changes

Delegated Authority: The addition of the delegated authority clause provides structural support for the periodic issuance of policy guidance based on technological advances. Allows for increased agility.

Refresh of Definitions: New definitions include updates to Personally Identifiable Information (PII), Collaboration Tools and Social Media.

Refresh of Unacceptable Uses list: The former policies contained dated technical references and did not go far enough to explicitly outline unacceptable behavior.

Management of CPS Computing Assets: Lack of language around general asset mgmt. responsibilities and protocol.

Staff Policy Updates

Domain	Current Policy	Proposed Policy
Cell Phone Usage	***Undefined***	New policy sets parameters for the following mobile device communications: ✓ Use of Board and Personal mobile devices for Board Business. ✓ Use of Mobile Devices for Communications with Students.
Social Media Usage	***Undefined***	New policy sets parameters for the following social media interactions: ✓ Non-CPS Personal Social Media Accounts ✓ Non-CPS Third-Party Social Media Accounts ✓ Class or Team Social Media Accounts ✓ Creating District, Dept. and/or School Social Media Accounts

Student Policy Updates

Domain	Current Policy	Proposed Policy
Cell Phone Usage	***Undefined***	The proposed policy sets baseline around the use of cell phones for voice and text communications with staff members.
Social Media Usage	***Undefined***	The proposed policy establishes baseline parameters around social media interactions between students and staff from both CPS and Personal Social Media Accounts.
Guidance on Office of Student Supports	***Undefined***	The proposed policy includes instructions for engaging the new Office of Student Protections and Title IX in the event inappropriate communications take place.

Socializing the Change

These policies will require regular attention; therefore strong and consistent engagement with schools is essential to ensuring the policies are rooted to what is happening in the classroom. Pending policy approval, the ITS team is preparing a multi-channel campaign to ensure that all staff have a suitable level of awareness.

Delivery Channels	Key Artifacts
Policy Guidance Website **(8/24)**	▪ Full policy documents, one-page policy 'cheat sheets' ▪ Guidelines and best practices, list of approved/acceptable technology tools ▪ FAQs and toolkits
Email	▪ Message 1**:** *(Formal Announcement)* General announcement on new policies with a link to the new policy guidance website. **(8/23)** ▪ Message 2: *(Reinforce)* Disseminate one-page, relatable, policy summary that includes condensed policy changes and their implications. **(8/30)** ▪ ITS Monthly Communications: Topics will cover data security awareness and best practices. **(Recurring)**
Training Webinars	▪ Review Student and Staff policy changes ▪ Review approved/acceptable technology platforms ▪ Outline best practices to share with students, teachers and parents

Communications Calendar

This calendar provides the framework for our communications strategy: additional components forthcoming. Success is adopting these policies will require strong partnership with school leaders and the Office of Teaching and Learning. Policy updates are strongly related the notion of building a higher level of understanding in both staff and students as to what it means to be a good digital citizen.

SY19 ITS Monthly Communications Calendar

Sept.

Student Password Policy Reminder

Oct.

Updated Approved Platform List ***(Social Media)***

Nov.

Phishing & Ransomware Awareness

Dec.

Digital Citizenship Awareness

Jan.

-Reminder on Proper Process for External Document Sharing

Feb.

-Best Practices for Student Data Sharing

Mar.

Best Practices for Information Security

Apr.

Best Practices for Email Security

May

Securing your School's Devices for Summer

Student/Parent Outreach

Maintenance of the policies over time requires a **two way dialog,** this is vitally important for our student and parent stakeholders.

Audience	Channels	Date
Students	▪ CPS AUP Guidance Website – Updated throughout the year, provides FAQs, policy language and detail on the platforms that have been through the security certification process. ▪ Student Portal – Provide a link to the AUP Guidance website on the Student Portal. ▪ Establish a Student Voice Committee – Work with Teaching and Learning to establish a committee that provides students an opportunity to help drive guidance directly. ▪ CEO Student Advisory Council – Present policy and practical implications for students to the existing CEO student advisory board.	8/24 9/28 TBD
Parents	▪ CPS AUP Guidance Website – Updated throughout the year, provides FAQs, policy language and detail on the platforms that have been through the security certification process. ▪ LSC Roadshow – Meet with a diverse cadre of LSC's to walk them through the finer points of the policy to solicit for input on both practice and guidance.	8/24 10/1 - 11/30

Security Certification Program

If the proposed policies are adopted ITS will undertake the following steps to establish a certification program to register existing tools and inform subsequent guidance in order to establish better connections with schools and ensure increased supports and protection students.

Activity		Date
School Survey: ITS will survey schools to identify any/all non-CPS sponsored messaging tools in use. Once identified, we will take all solutions through an information security audit.	▪ Platforms that pass the audit will be noted as 'Approved' for use on the district's website. ▪ Platforms that fail the audit will be identified for Procurement to prevent additional purchases and the IT team will work with the location to transition to an approved platform.	9/5 – 10/5
Procurement and Legal Processes: ITS will ensure coordination between stake-holding departments post audit activity.	▪ Platforms that pass the audit will be identified for all Procurement Buyers and will be included on the Acceptable Platforms list. ITS will work with Law to establish contract language consistent with currently acceptable CPS platforms to ensure consistency in approach. ▪ Platforms that fail the audit will be flagged for all Procurement buyers so as to ensure there is a front line control over subsequent purchasing.	10/15