

AND ADOPT A NEW STAFF ACCEPTABLE USE POLICY

THE CHIEF EXECUTIVE OFFICER RECOMMENDS: That the Board rescind Board Report 09-0722-P03 and adopt a new Staff Acceptable Use Policy.

PURPOSE: Chicago Public Schools (CPS) provides access to technology devices, internet, data and

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/elseq/elseq/ferpa/ferpa.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/ilcs2.asp?actID=10008&ChapterID=17>

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, etc.) and (b) must not disclose any confidential information to the ITS

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.

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 773-552-3025 to

16. disclose 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

performance and will reduce the efficiency of the MIAM. 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 ITC to ensure the safety and efficiency of the network. These are

of the CPS must be sent from their CPS email account with Board authorized return addresses. Users

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

(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 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 7-12 via text messaging or IM provided that the CPS staff member:

(a) complies with the parent/guardian permission requirements established by the CEO for

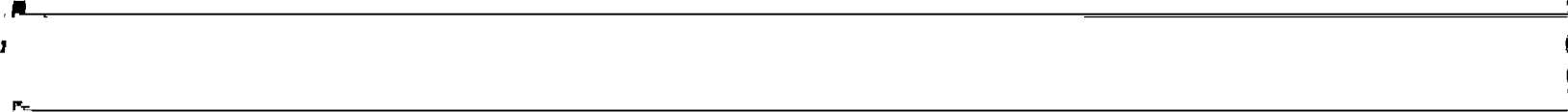
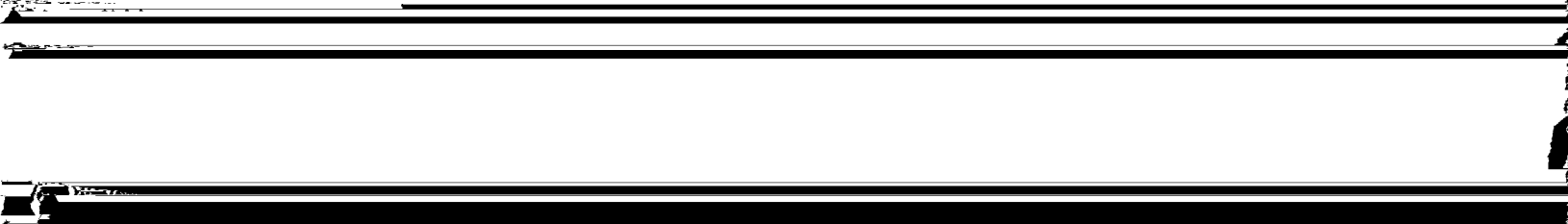
staff/student text communications under the Program;

(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 communications with a student for Program purposes, and

(d) includes the staff member's CPS email address, or other CPS email address identified by the

operations of the Chicago Public Schools may be subject to discipline. Users who are managers are also



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~~

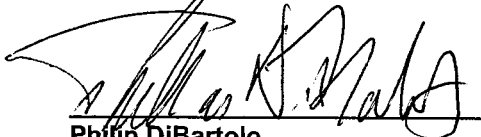
program, sports team or club and shall include, at a minimum, the following:

for loss or theft. The district reserves the right to enforce security measures on personal electronic devices
when used to access the CDC Network and system tools, and remove devices found to be in violation of

this policy.

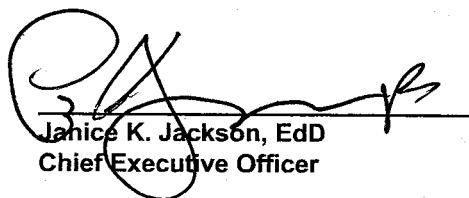
XI. Protected Storage. Hard drives that contain PII must be securely protected with a password and/or
encrypted to ensure the safety of the data contained therein. A list of approved services for storage or

Approved for Consideration:



Philip DiBartolo
Chief Information Officer

Approved:



Janice K. Jackson, EdD
Chief Executive Officer