

**RESCIND BOARD REPORT 04-0428-PO2
AND ADOPT A NEW POLICY ON THE ACCEPTABLE USE OF
THE CPS NETWORK AND COMPUTER RESOURCES**

THE CHIEF EXECUTIVE OFFICER RECOMMENDS:

That the Board rescind Board Report 04-0428-PO2 and adopt a new Policy on the Acceptable Use of the CPS Network and Computer Resources.

PURPOSE: This policy intends to (1) set forth the terms and conditions under which Chicago Public Schools ("CPS") Users may access and use CPS Network and Computer Resources; (2) state the requirements that shall govern the operation and management of all information technology used, operated and/or maintained by CPS; and (3) ensure the Board's information technology and information assets are managed so as to maximize their efficient and secure use.

POLICY TEXT:

I. APPLICABILITY

This policy applies to all Board employees, officers, temporary employees, interns, vendors, consultants, contractors and authorized agents and volunteers working under the supervision of a school principal, who use Board Computer Resources and/or access the CPS Network ("Users"). Students are subject to and must comply with the Board's Policy on Student Use of the CPS Network and Computer Resources. Personal electronic devices are subject to this policy when such devices are connected to the CPS Network or Computer Resources.

II. DEFINITIONS

Broadcast E-Mail refers to any e-mail which contains the same content and is mass emailed to a school(s) or department(s) from outside the school or department, or to all or a subset of Users. Intra-departmental or intra-school e-mails, even if identical in content, are not considered broadcast e-mails.

Computer Resources refers to all computers 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, system memory, servers, telecommunication devices and output devices such as telephones, hand held devices, printers, scanners, facsimile machines and copiers whether owned or leased by the Board.

Collaboration Systems refers to the hardware and software 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, text chat/instant messaging, video conferencing, websites and podcasting.

CPS Network refers to the infrastructure used to transmit, store and review data over an electronic medium and includes, but is not limited to, the CPS E-mail system(s), collaboration systems, databases, information systems such as IMPACT and CPS@Work, internet service, the CPS intranet system and CPS mainframe systems, whether the system is owned or contracted.

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

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

Unsolicited Bulk E-mail, also known as "spam," is any message sent over the CPS Network to multiple recipients that is (a) not authorized by the recipient, and (b) identical in content for all recipients.

III. DUTIES

A. ITS Duties. ITS is responsible for designing, establishing and maintaining the CPS Network and Computer Resources and for 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 and guidelines (collectively referred to as ITS 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.

B. Department/School Management Duties. Department/School Managers are responsible for designating Users authorized to 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 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 for the consultant or contractor to perform critical functions and services, and only upon the consultant's/contractor's execution of a confidentiality agreement regarding such access and use.

C. User Duties. All 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 or use, abuse, misuse, injury, degradation, theft or destruction. Users shall comply with all ITS Guidelines when using the CPS Network or Computer Resources. All employees communicating with students via electronic means must do so using CPS Network systems.

IV. 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, standards and guidelines 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 E-mail 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.

C. Monitoring. ITS has the right to access, search, read, inspect, copy, monitor, log or otherwise use data and information stored, transmitted and processed on CPS Network and Computer Resources in order to execute the requirements of this policy. CPS Network including but not limited to Internet and E-mail usage may be monitored and audited by Department/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 User access to any system to address security concerns, and (3) determine what constitutes appropriate use of these resources and to report any illegal activities. ITS may intercept and/or quarantine E-mail messages and related resources, such as Internet mail and other messaging services for business, legal or security purposes.

D. 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 3-EXCL Service Desk to obtain access. Managers shall not ask Users to share their password for such purposes.

V. GENERAL PROVISIONS REGARDING USE

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 CPS Network and Computer Resources is intended for Board business, with limited personal use permitted. Such personal use must in all circumstances comply with the unacceptable use and conduct provisions in this policy, and must not result in costs to the Board, cause legal action against or cause embarrassment 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.

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 Systems or E-mail 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 deemed offensive to persons based on race, ethnic heritage, national origin, sex, sexual orientation, age, physical or mental illness or disability, marital status, religion or other characteristics that may be protected by applicable civil rights laws;
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, logic bomb, worm or other harmful component or malicious code;
7. constitutes a chain letter, junk mail, phishing, spam or unauthorized broadcast e-mail;
8. violates the security of any 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, unless explicitly authorized to do so;
10. impersonates any person living or dead, organization, business, or other entity;
11. degrades the performance of the CPS Network or Computer Resources or causes a security risk;
12. deprives an authorized User of access to CPS Network or Computer Resources;
13. obtains 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. shares CPS e-mail addresses or distribution lists for uses that violate this policy or any other Board policy;
17. enables or constitutes gaming, wagering or gambling of any kind;
18. promotes or participates in any way in unauthorized raffles or fundraisers,
19. promotes or participates in any way in partisan political activities;
20. promotes or participates in any way in internal political or election activities related to a union or other organization representing employees;
21. engages in private business, commercial or other activities for personal financial gain;
22. distributes unauthorized information regarding other Users' passwords or security systems;
23. solicits or distributes information with the intent to cause personal harm or bodily injury;

24. transmits sensitive or confidential information without appropriate security safeguards;
25. falsifies, tampers with or makes unauthorized changes or deletions to data located on the CPS Network;
26. enters false data on to the CPS Network;
27. accesses or uses data located on a CPS Network system for personal uses;
28. promotes or participates in a relationship with a student or which 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;
29. installs, downloads or uses unauthorized or unlicensed software or third-party system;
30. violates the terms of use specified for a particular Computer Resource or CPS Network System;
31. 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
32. violates any express 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 laws.

E. Software Licenses. All software used by Users must have a valid license. Users shall use authorized software in compliance with the licenses provided to or by the Board. Users may install software that is deemed necessary for business use by Departmental/School Management. Such software must not compromise the security or integrity of the CPS Network and 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. Filtering and Blocking. As required by law, CPS uses filtering technology to screen internet sites for offensive material and prohibit access, to the extent possible, to objectionable, offensive or unsuitable content found on the internet. 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 Network. All blocking and unblocking decisions will be made by ITS in compliance with applicable laws and the requirements of this policy.

H. Remote Access. Remote access to the CPS Network is allowed only through ITS-authorized remote access solutions.

I. Third-Party Systems. The Board 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 Board 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 written approval by the Office of the Chief Executive Officer (CEO). 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 CEO. 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 e-mail systems, IMPACT system, remote access solution and any other mandates that may be established in the future by the CEO or the Board.

J. New Technologies. New network technologies are being invented constantly, and it is impossible to predict what systems or applications will be available for use in the future. The requirements of this policy apply to all technologies currently in use on the CPS Network 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.

K. Passwords. Users shall comply with ITS standards and guidelines on password set up, usage and security. Users must never disclose passwords or other access or authorization codes to any person.

L. Unauthorized Access and Data Tampering. A User is prohibited from using their authorized access to a CPS Network system to falsify, misreport, misrepresent, make unauthorized changes or deletions or otherwise tamper with CPS data. A User is prohibited from 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 in accordance with Section X of this Policy for any unauthorized access to a CPS Network system and for their acts or omissions that allow others to gain unauthorized access to a CPS Network system.

VI. E-MAIL

A. Usage. Users are not allowed to use third party e-mail systems (such as Yahoo or AOL) in their capacity as representatives of Chicago Public Schools. All e-mail sent by Users in their capacity as representatives of the Chicago Public Schools must be sent from Board authorized e-mail systems, with Board authorized return addresses. User e-mails are subject to retention by ITS in accordance with the Board's E-mail Retention Policy.

B. Confidentiality. Users must exercise due care to ensure that e-mail messages containing 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 information via e-mail without the prior written approval of ITS.

Users shall abide by ITS-issued standards and guidelines on the classification, handling and e-mail transmission of confidential information, including applicable encryption requirements.

C. Broadcast E-mails. The Office of Communications shall establish guidelines by which a broadcast e-mails may be authorized for distribution. Users may transmit broadcast e-mails only when authorized in accordance with such guidelines.

VII. PORTABLE DEVICES

All Computer Resources that are considered portable devices are subject to additional security requirements as set out in the ITS guidelines. Users shall abide by all requirements established by ITS for such portable devices, including but not limited to those related to laptops, cell phones, smart phones, USB memory sticks, and portable hard drives. Users are prohibited from housing Social Security Number information on a portable device without the prior approval of ITS.

VIII. CONFIDENTIALITY

Users shall maintain and protect the confidentiality of student records when using the CPS Network and Computer Resources. Further, Users shall maintain and protect the confidentiality of other confidential information that is housed, processed or maintained on the CPS Network or Computer Resources. Examples of such confidential information include, but are not limited to, information exempt from disclosure under Illinois Freedom of Information Act, information protected from disclosure under the federal Health Insurance Portability and Accountability Act, other personnel information, financial information, strategic plans, vendors' proprietary information and information protected by intergovernmental non-disclosure agreements or other non-disclosure agreements.

IX. REPORTING

Users shall immediately report to the 3-EXCL Service Desk and Department/School Management any actual or suspected:

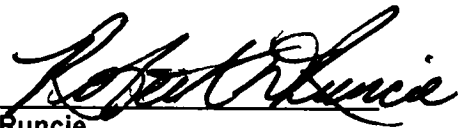
- a. security violations or breaches, including, but not limited to:
 - i. improper transmission of confidential information;
 - ii. compromised passwords or access codes
 - iii. receipt of messages containing suspected virus content;
- b. theft or loss of Computer Resources including portable devices
- c. unacceptable use of the CPS Network or Computer Resources; and
- d. any other violation of this Policy.

Receipt of inappropriate spam or suspicious electronic messages, including suspected phishing messages, should be reported immediately to ReportSpam@cps.k12.il.us. User access privileges may be suspended at any time if ITS determines that a security threat exists.

X. VIOLATIONS AND ENFORCEMENT OF THIS POLICY

Employees who fail to abide by this policy are subject to discipline in accordance with the Board's Employee Discipline and Due Process Policy with corrective action ranging from suspension or permanent revocation of CPS Network access privileges to termination of employment. Violations of certain provisions in this policy may also subject a User to civil and criminal liability according to applicable federal and state laws. Any Board contractor, consultant, volunteer or other business partner who violates this policy may have their system access privileges suspended and may further be subject to contract termination or any other remedy or action deemed appropriate by the Board.

Approved For Consideration:



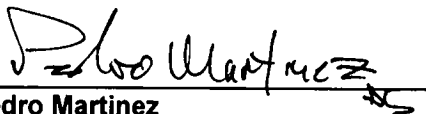
Robert Runcie
Chief Administrative Officer

Respectfully Submitted:



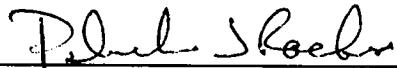
Ron Huberman
Chief Executive Officer

Noted:



Pedro Martinez
Chief Financial Officer

Approved as to Legal Form: *gam*



Patrick J. Rocks
General Counsel