

RESCIND BOARD REPORT 02-0626-PO03
CHICAGO PUBLIC SCHOOLS' POLICY ON THE USE OF THE INTERNET, THE CPS
INTRANET, ELECTRONIC MAIL, AND COMPUTER ACCESS BY AUTHORIZED USERS
AND ADOPT NEW MEMBER ACCEPTABLE USE OF THE CPS NETWORK POLICY

THE CHIEF EXECUTIVE OFFICER RECOMMENDS THE FOLLOWING:

That the Chicago Board of Education ("Board") rescind Board Report 02-0626-PO03, "Chicago Public Schools' Policy on the Use of the Internet, the CPS Intranet, Electronic Mail, and Computer Access by Authorized Users," and adopt new "Member Acceptable Use of the CPS Network Policy."

SUBJECT:

Chicago Public Schools ("CPS") employees', consultants', parent- or community-volunteers' working under the supervision of a school principal or non-Board employees such as interns' use of CPS computers and the CPS Network.

POLICY TEXT:

I. PURPOSE

This policy, also referred to as the "Member Acceptable Use for Electronic Network Related Technologies and Access Policy" ("AUP") sets forth the standards governing Chicago Public Schools ("CPS") members' use of the CPS Electronic Network Related Technologies and Access ("CPS Network") system. This policy also sets forth the rules under which Member Authorized Users ("Members") may continue their access to and use of these resources. This policy promotes the ethical and legal business-related use of the CPS Network, and ensures CPS compliance with the Children's Internet Protection Act. Personal electronic devices will be governed under this policy when such devices are attached to the CPS network.

Member use of information resources must be consistent with the educational and business purposes for which these resources have been provided. Use of the CPS Network is a privilege that is provided to help Members complete and deliver educational and business obligations. The CPS Network provides Members with the means for communicating effectively with schools, central office departments, area offices, the public, other government entities, and the business sectors. The authorized uses of these resources shall include, but not be limited to, work-related inquiries, researching CPS-related information, and informing the public about district programs and services. Member use must not violate the public trust or disregard applicable policies and regulations established by the Chicago Board of Education ("Board").

II. DEFINITIONS

- A. Chicago Public Schools' Electronic Network Related Technologies and Access ("CPS Network")** is the system of computers, terminals, servers, databases, routers, hubs, switches, and distance learning equipment connected to the CPS Network. These components may function in conjunction with established hardwire or wireless LAN running over outside lines, such as T-1, BRI, PRI, VPN, Dialup, Distance Learning Equipment, owned or leased by CPS.
- B. Distance Learning Equipment** is a means for providing meetings, educational or professional courseware, and workshops utilizing media management systems.

- C. **Electronic Mail ("e-mail")** consists of all electronically transmitted information including any combinations of text, graphics, audio, pictorial, or other information created on or received by a computer application system and includes the transmission data, message text, and all attachments.
- D. **Internet** is a worldwide telecommunications system that provides connectivity for thousands of other smaller networks.
- E. **Other Electronic Devices** include, but are not limited to, cellular telecommunication devices such as cellular phones, pagers, text communication pagers, two-way text pagers, and personal digital assistants that may or may not be physically connected to the network infrastructure.
- F. **Password** is a secret word or series of letters and numbers that must be used to gain access to an online service or the Internet or to modify certain software (such as parental controls).
- G. **Member Authorized Users ("Members")** are Chicago Public Schools' employees, consultants, parent- or community- volunteers working under the supervision of a school principal, and non-Board employees such as interns.
- H. **Website** is a collection of "pages" or files on the Internet that are linked together and managed by a company, institution, or individual. In the case of the CPS Network, it is recommended that the hosting of websites be executed by the Office of Technology Services ("OTS").

III. GENERAL PROVISIONS

A. MEMBER AUTHORIZED USERS ("Members")

All Members shall adhere to the provisions of this policy as a condition for continued use of the CPS Network. This policy applies anytime there is a connection to the Board's hardwired or wireless network via outside lines such as T-1, BRI, PRI, VPN, Dialup, DSL, Distance Learning Equipment, Personal Digital Assistants, and other personal electronic devices.

The Internet, Intranet, computer access, and e-mail resources are to be used only for business pertaining to the Chicago Public Schools, with allowance made for modest amounts of incidental personal use that does not violate this policy.

Department supervisors, the principals of attendance centers, the Area Instructional Officers ("AIOs"), and the Chief Information or Technology Officer of the Chicago Public Schools have the authority to enroll and terminate Member access of the Internet, Intranet, network resources, and e-mail.

B. DISCLAIMER

Pursuant to the Children's Internet Protection Act, CPS uses filtering software to screen Internet sites for offensive material. The Internet is a collection of thousands of worldwide networks and organizations that contain millions of pages of information. Users are cautioned that many of these pages contain offensive, sexually explicit, and inappropriate material, including, but not limited to the following categories: Adult Content; Nudity; Sex; Gambling; Violence; Weapons; Hacking; Personals/Dating; Lingerie/Swimsuit; Racism/Hate; Tasteless; and Illegal/Questionable. In general it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content.

Members accessing the Internet do so at their own risk. No filtering software is one hundred percent effective and it is possible that the software could fail. In the event that the filtering software is unsuccessful and Members gain access to inappropriate and/or harmful material, the Board will not be liable. To minimize these risks, Member use of the CPS Network is governed by this policy.

C. E-MAIL AS A RECORD

The Local Records Act [50 ILCS 205/3] defines a "Public Record" as any book, paper, map, photograph, digitized electronic material, or other official documentary material regardless of physical form or characteristics, made, produced, executed or received by any agency or officer pursuant to the law or in connection with the transaction of public business and preserved or appropriate for preservation by such agency or officer, or any successor thereof, as evidence of the organization, function, policies, decisions, procedures, operations or other activities of the State or the State Government or because of the informational data contained therein. Pursuant to Board Report 01-0725-PO3 ("Retention and Management of Business Records"), e-mail is a transitory vehicle of communication and is not to be used by CPS employees as a Public Record as defined in the State Code.

In the event that e-mail meets the definition of a Public Record or contains information valuable for future reference for the user or CPS, e-mail should be saved outside of the e-mail system by printing and saving the e-mail as a paper document to protect and ensure retrievability over time.

The rules of record retention apply regardless of the physical form or characteristics of the record. In the event of questions regarding record retention, contact the CPS Enterprise Records Manager within the Law Department.

All e-mail, although not a Public Record as defined in the State Code, is subject to the rules of discovery.

IV. TERMS AND CONDITIONS FOR MEMBER USE OF THE CPS NETWORK

A. ACCEPTABLE USES

Members may use the various resources provided by the CPS Network to pursue educational and business-related activities. Members should use the network resources via Internet such as discussion boards, instant messaging, and chat rooms for educationally collaborated businesses to perform CPS educational or business objectives. When using the CPS Network, Members will be expected to follow generally accepted rules of network etiquette. These include, but are not limited to, the following:

1. Be polite. Do not become abusive in your messages to others.
2. Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.
3. Keep personal information, including the logins, passwords, social security, addresses, and telephone numbers of members or colleagues confidential.
4. Use these resources so as not to disrupt service to other Members.
5. Users who are provided with CPS e-mail account have the responsibilities to:
 - a. Maintain prescribed mailbox sizes.

- b. Use distribution lists only as allowed by their position and only as appropriate for business purposes.
- c. Only request Public Folders and electronic discussion groups (distribution lists, listservs, etc.) that are essential and appropriate for business purposes.
- d. If a Public Folder is not used for six (6) months or used inappropriately, OTS reserves the right to remove or delete the folder and the file content.

B. UNACCEPTABLE USES

Improper use of the CPS Network is prohibited. Actions that constitute unacceptable uses of the CPS Network and that are not specifically addressed elsewhere in this policy include, but are not limited to:

- 1. Using the CPS Network for, or in support of, any illegal purposes.
- 2. Using the CPS Network for, or in support of, any obscene or pornographic purposes including, but not limited to, the retrieving or viewing of any sexually explicit material. If a Member inadvertently accesses such information, he or she should immediately disclose the inadvertent access to a superior and follow the Internet filtering guidelines for blocking a site. This will protect the user against allegations of intentionally violating this policy.
- 3. Using the CPS Network 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.
- 4. Using the CPS Network for non-Board-related business purposes, including, but not limited to, games, wagering, gambling, junk mail, chain letters, jokes, private business activities, raffles, fundraisers, religious activities, or political lobbying.
- 5. Using the CPS Network to upload, post, e-mail, transmit, or otherwise make available any content that is unlawful, dangerous, or may cause a security risk.
- 6. Knowingly making a false, misleading, or unauthorized statement of Board policy, either expressly or by implication.
- 7. Using Internet tools such as discussion boards, chat rooms, and instant messaging for personal rather than educational and CPS business purposes.
- 8. Using profanity, obscenity, or language without a legitimate business purpose that is generally considered offensive or threatening to persons of a particular race, gender, religion, sexual orientation, or to persons with disabilities.
- 9. Knowingly plagiarizing any information gained on or through use of the CPS Network or any other network access provider.
- 10. Knowingly using copyrighted materials, including commercial software, without permission of the copyright holder, and/or in violation of state, federal, or international copyright laws. (If Members are unsure whether or not they are using materials in violation of copyright provisions, they

should contact the Area Office or Office of Technology Services if they have questions regarding use of copyright materials found through the CPS Network).

11. Knowingly violating any federal or state statutes or any Board policies and/or procedures regarding the protection of employee or student privacy or the confidentiality of employee or student records.
12. Using the CPS Network for personal financial gain or for the transaction of any non-Board-related-business or commercial activities.
13. Downloading software from the Internet without prior approval from the OTS Department. Downloaded software can introduce computer viruses onto the CPS network. In addition, anti-virus download software is not to be disabled. All computers are configured to automatically scan any material downloaded from the Internet.

C. SUBSCRIPTION AND USAGE FEES

The Internet provides access to sites that charge a subscription or usage fee to access and use the information on such sites. If Members incur costs for appropriate use of such sites in accordance with this policy, the user may submit the charges for reimbursement on expense reports, subject to CPS review. Users will be responsible for paying any unapproved costs associated with using the information on such sites.

V. SECURITY

All Members are to report promptly any breaches of security violations of acceptable use and the transmission of web addresses or e-mail information containing inappropriate material (as outlined in Section III B of this policy) to department supervisors, the principals of attendance centers, AIOs or their designees, or the Chief Information or Technology Officer of the Chicago Public Schools. Department supervisors or school principals shall report security breaches to AIOs or their designees or to the Chief Technology Officer or designee. Failure to report any incident promptly may subject the Member to corrective action consistent with the Board's rules and policies.

In order to maintain the security of the CPS System, Members are prohibited from engaging in the following actions:

- A. Connecting to a modem to dial into any online service provider or Internet Service Provider ("ISP") or connecting through a Digital Subscriber Line ("DSL") while physically being connected to the CPS Network where a T-1 line is functioning.
- B. Knowingly disrupting the use of the CPS Network for other users, including, but not limited to, disruptive use of any processes or programs, sharing logins and passwords or utilizing tools for ascertaining passwords, or engaging in unauthorized or unlawful entry into an electronic system to gain information (i.e. "hacking").
- C. Knowingly spreading computer viruses or programs that loop repeatedly, infiltrating a computer system without authorization, or damaging or altering without authorization the software components of a computer or computer system.
- D. Disclosing the contents or existence of CPS computer files, confidential documents, e-mail correspondence, or other information to anyone other than authorized recipients. Members must not share logins or password(s) and unauthorized information regarding other users' passwords or security systems.

- E. Downloading unauthorized games, programs, files, electronic media, and/or stand-alone applications from the Internet that may cause a threat to the CPS Network.

VI. MEMBER WEBSITES

A. Educational Purposes

Members may create web pages as a part of an educational or business pursuit. CPS has the right to exercise control over the content and/or style of the member web pages.

Members are required to obtain permission from parent(s) or guardian(s) on the attached Consent Form and Release (Attachment A) if student work or pictures will be posted on CPS websites. Members who place students' work, likeness (as captured by photograph, video or other media), or voices on a CPS website, or who refer to students on a CPS website, should identify these students by first name only due to safety and confidentiality considerations.

B. Website Development

Members designing websites should go to www.schoolhosting.cps.k12.il.us for the directions and procedures they need to follow in developing their websites.

VII. MONITORING

The CPS Network is routinely monitored to maintain the efficiency of the system. Members should be aware that use of the CPS Network, including their use of e-mail, is subject to reasonable and appropriate monitoring by OTS that abides by the requirements of all applicable federal and state laws. Any activities related to or in support of violations of this policy and/or other Board policies and rules may be reported and will subject the Member to appropriate sanctions.

VIII. ASSUMPTION OF RISK

CPS will make a good faith effort to keep the CPS Network system and its available information accurate. However, Members acknowledge that there is no warranty of any kind, either express or implied, regarding the accuracy, quality, or validity of any of the data or information available. For example, and without limitation, CPS does not warrant that the CPS Network will be error free or free of computer viruses. In making use of these resources, Members agree to release the Board from all claims of any kind, including claims for direct or indirect, incidental, or consequential damages of any nature, arising from any use or inability to use the network, and from any claim for negligence in connection with the operation of the CPS Network. Members further acknowledge that the information available through interconnecting networks may be inaccurate. CPS has no ability to maintain the accuracy of such information and has no authority over these materials. CPS makes no warranty of any kind, either express or implied, regarding the accuracy, quality, or validity of the data and/or information residing on or passing through the CPS Network from outside networks. Use of the CPS Network is at the risk of the Member.

IX. INDEMNIFICATION

The Member indemnifies and holds the Board harmless from any claims, including attorney's fees, resulting from the user's activities while utilizing the CPS Network that cause direct or indirect damage to the user, CPS, or third parties.

X. SANCTIONS

Failure to abide by this policy may subject employee Members to the Employee Discipline Code for corrective action ranging from suspension or permanent revocation of Network access

privileges to termination of employment. Violations of certain provisions in this policy may subject a Member to possible civil and criminal liability according to applicable federal and state laws.

When inappropriate use is determined by a Member's supervisor, the supervisor will notify, in writing, the Chief Technology Officer of the Chicago Public Schools, who is authorized to terminate the user's access privileges. An employee may appeal this decision through discipline procedures for employees in Board Reports 95-1025-PO1 ("Personnel Policy Teachers and Administrators: Discipline") and 95-1025-PO2 (Personnel Policy Educational Support Personnel: Discipline and Discharge"); a consultant may appeal this decision directly to his or her supervisor; and the parent- or community-volunteer may appeal this decision directly to the school principal.

If a Member's access to the CPS Network is suspended by CPS Network administrators as a result of violations of this policy, the member may appeal the suspension to the Chief Education Officer or designee.

For full details, instructions, and guidelines for network related tools, please visit:

http://ots.cps.k12.il.us/pdfs/Instructions_DLs.pdf.

http://ots.cps.k12.il.us/pdfs/EMail_ServicesProcedures.pdf

<http://ots.cps.k12.il.us/pdfs/PasswordGuidelines.pdf>

http://ots.cps.k12.il.us/pdfs/Mailbox_SizeLimits.pdf

<http://ots.cps.k12.il.us/pdfs/PublicFolders.pdf>

<http://ots.cps.k12.il.us/pdfs/AcquiringAccountInfo.pdf>

<http://ots.cps.k12.il.us/pdfs/PSTFILES.pdf>

LEGAL REFERENCES:

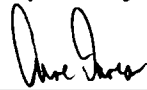
105 ILCS 10/1 *et seq.* (Illinois Member Records Act); Pub. L. No. 106-554 (Children's Internet Protection Act).

Reviewed for Consideration:



Barbara Eason-Watkins
Chief Education Officer

Respectfully submitted:



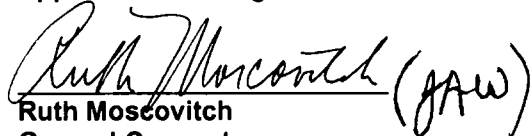
Arne Duncan
Chief Executive Officer

Noted:



John Maiorca
Chief Finance Officer

Approved as to Legal Form:



Ruth Moscovitch
General Counsel

**ATTACHMENT A
CONSENT FORM AND RELEASE**

School _____

Date _____

Board of Education
City of Chicago
125 South Clark Street
Chicago, Illinois 60603

I hereby consent to have _____
(full name and relation)

photographed, video taped, audio taped and/or interviewed by the Board of Education of the City of Chicago (the "Board") or the news media on the school premises when school is in session or when my child is under the supervision of the Board. Additionally, I hereby give the Board consent to use creative work(s) generated and/or authored by my child on the Internet, or on an educational CD, or any other electronic/digital media. I understand that my child will be identified by first name only, for confidentiality purposes, as the author of said work.

I also consent to the Board's use of my child's photograph or likeness or voice on the Internet or on an Educational CD or any other electronic/digital media. As the child's parent or legal guardian, I agree to release and hold harmless the Board, its members, trustees, agents, officers, contractors, volunteers and employees from and against any and all claims, demands, actions, complaints, suits or other forms of liability that shall arise out of or by reason of, or be caused by the use of my child's creative work(s), photograph, likeness or voice on television, radio or motion pictures, or in the print medium, or on the Internet or any other electronic/digital medium.

It is further understood and I do agree that no monies or other consideration in any form, including reimbursement for any expenses incurred by me or my child, will become due to me, my child, our heirs, agents, or assigns at any time because of my child's participation in any of the above activities or the above-described use of my child's creative work(s), photograph, likeness or voice.

Child's Name _____

Address _____

Signature of Parent or Guardian

Principal's Signature