Chicago Public Schools Policy Manual

Title: **STUDENT ACCEPTABLE USE OF THE CPS NETWORK**
Section: **604.2**
Board Report: 03-0326-PO03 **Date Adopted:** March 26, 2003

Policy:

I. PURPOSE

This policy, also referred to as the "Student Acceptable Use for Electronic Network Related Technologies and Access Policy" ("AUP") sets forth the standards governing Chicago Public Schools ("CPS") students' use of the CPS Electronic Network Related Technologies and Access ("CPS Network") system. This policy also sets forth the rules under which student authorized users may continue their access to and use of these resources. This policy promotes the ethical, legal, and school-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.

Authorized student use of information resources must be consistent with the educational purposes for which these resources have been provided. Use of the CPS Network is a privilege that is provided to help student authorized users complete and deliver educational obligations. The CPS Network provides student authorized users with the means for communicating effectively with schools, teachers, administrators, the public, other government entities, and educational experts. These resources should be used in a manner that both enhances students' educational experiences and complies with this policy and regulations established from time to time by the Chicago Board of Education ("Board"). CPS students, through their use of the CPS Network, will gain skills and expertise that prepare them for an increasingly technology-oriented society.

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 video and/or audio conferencing equipment, and/or media management systems to distribute video to individual classrooms and offices in schools**.**

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. **Student Authorized Users** are any students enrolled in any classes offered by CPS in a traditional classroom or virtual classroom setting.

H. **Website** is a collection of "pages" or files on the Internet that are linked together and managed by a company, institution or individual.

III. GENERAL PROVISIONS

A. STUDENT AUTHORIZED USERS

All student authorized users shall adhere to the provisions of this policy as a condition for continued use of the CPS Network. It is a general policy of CPS to promote the use of computers in a manner that is responsible, legal and appropriate. This policy is enacted 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.

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. Student authorized users 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 children and staff gain access to inappropriate and/or harmful material, the Board will not be liable. To minimize these risks, student use of the CPS Network is governed by this policy.

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

A. ACCEPTABLE USES

CPS students may use the various resources provided by the CPS Network to pursue educationally-related activities. Teachers and other staff should help guide students in their use of the CPS Network so that students will learn how Internet resources such as discussion boards, instant messaging and chat rooms can provide valuable educational information from classrooms, schools, and other national and international sources. In addition to using the CPS Network strictly for educational pursuits, students 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, addresses, and telephone numbers of students or colleagues confidential.

4. Use these resources so as not to disrupt service to other student authorized users.

5. Do not upload, post, e-mail, transmit, or otherwise make available any content that is unlawful, dangerous or may cause a security risk.

B. UNACCEPTABLE USES

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

1. Use of the CPS Network for, or in support of, any illegal purposes.

2. Use of 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 student authorized user inadvertently accesses such information, he or she should immediately disclose the inadvertent access to a teacher or to the school principal. This will protect the user against allegations of intentionally violating this policy.

3. Use of the CPS Network for soliciting or distributing information with the intent to incite violence, cause personal harm or bodily injury, or to harass or “stalk” another individual.

4. Non-educational uses of the CPS Network including, but not limited to games, wagering, gambling, junk mail, chain letters, jokes, private business activities, raffles, fundraisers, religious activities or political lobbying.

5. Making a statement of policy, either expressly or by implication, except for messages that quote policies, Board Rules, procedures, documents published by CPS, or other official sources.

6. Using Internet tools such as discussion boards, chat rooms, and instant messaging for personal rather than educational purposes.

7. Using profanity, obscenity or language that is generally considered offensive or threatening to persons of a particular race, gender, religion, sexual orientation, or to persons with disabilities.

8. Plagiarizing any information gained on or through use of the CPS Network or any other network access provider.

9. Using copyrighted materials, including commercial software, without permission of the copyright holder, and in violation of state, federal or international copyright laws. (If students are unsure whether or not they are using materials in violation of copyright provisions, they should ask their teachers or a school technology coordinator for assistance. School-based personnel are encouraged to contact the Office of Technology Services if they have questions regarding use of copyright materials found through the CPS Network.)

10. Violating of any provision of the Illinois School Student Records Act (105 ILCS 10/1*et seq*.), which governs students' rights to privacy and the confidential maintenance of certain information including, but not limited to, a student's grades and test scores is prohibited.

11. Using the CPS Network for financial gain or for the transaction of any business or commercial activities.

C. SECURITY

All student authorized users 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 their teacher or the school principal. Authorized personnel will report such breaches to the Area Instructional Officer or designee or the Chief Technology Officer or designee of the Chicago Public Schools. Failure to report any incident promptly may subject the student authorized user to corrective action consistent with the Uniform Discipline Code ("UDC"), Board's rules, and policies.

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

1. Connecting to a modem to dial into any online service provider, or Internet Service Provider ("ISP") or connect through a Digital Subscriber Line ("DSL") while physically being connected to the CPS Network where a T-1 line is functioning.

2. Intentionally 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 "hacking" of any kind, which is an illegal or unlawful entry into an electronic system to gain secret unauthorized information.

3. Intentionally spreading computer viruses or programs that loop repeatedly, or for the purpose of infiltrating a computer system without authorization or for damaging or altering without authorization the software components of a computer or computer system.

4. Disclosing the contents or existence of CPS computer files, confidential documents, e-mail correspondence, or other information to anyone other than authorized recipients. Student authorized users must not share logins or password(s) and unauthorized information regarding other users' passwords or security systems.

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

V. STUDENT WEBSITES

1. Educational Purposes

Student authorized users may create webpages as a part of a class activity. Material presented on a student's class activity website must meet the educational objectives of the class activity. CPS has the right to exercise control over the content and/or style of the student webpages.

Only those students whose parent(s) or guardian(s) have completed the attached Consent Form and Release (Attachment A) may post their work or picture on student or school websites. Students whose work, likeness (as captured by photograph, video or other media) or voices are presented on a student website shall be identified by first name only for confidentiality and safety purposes.

2. Website Development

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

VI. MONITORING

The CPS Network is routinely monitored to maintain the efficiency of the system. Student authorized users 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 state and federal laws. Any activities related to or in support of violations of this policy and/or the UDC may be reported and will subject the user to sanctions specified either in the UDC or in this policy.

VII. ASSUMPTION OF RISK

CPS will make a good faith effort to keep the CPS Network system and its available information accurate. However, student authorized users 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, student authorized users 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. Student authorized users further acknowledge that the information available through interconnecting networks may be inaccurate. CPS has no ability to maintain 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 student authorized user.

VIII. INDEMNIFICATION

The student authorized user 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.

IX. SANCTIONS

Failure to abide by this policy may subject the student authorized user to corrective action ranging from suspension of some or all access privileges up to and including expulsion and prosecutions according to the UDC. A violator must understand that if his or her privileges to use the CPS Network are revoked by a school faculty member that he or she has the right to appeal the revocation within thirty (30) days, in writing, to the principal of the school. The school principal's decision shall be FINAL.

If an student authorized user’s access to the CPS Network is suspended by CPS Network administrators as a result of violations of this policy, the student may appeal the suspension to the Chief Education Officer or designee.

A violator must understand that if he or she is removed from the CPS Network, there shall be no obligation to provide a subsequent opportunity to access the CPS Network.