12-0627-PO2 June 27, 2012

ADOPT AN INTERNET SAFETY POLICY

THE CHIEF EXECUTIVE OFFICER RECOMMENDS:

That the Board adopt an Internet Safety Policy.

PURPOSE: The Board intends to establish a separate stand-alone policy that enumerates internet safety measures that the District will continue to implement to protect students from accessing inappropriate material over the Chicago Public Schools' (CPS) computer network. This policy further identifies curricular measures the District will continue to implement to educate students about internet safety and appropriate online behavior. The requirements set out in this policy are intended to ensure CPS compliance with the Children's Internet Protection Act (CIPA) as well as state requirements for internet safety education.

HISTORY OF BOARD ACTION: On June 26, 2002, the Board adopted amendments to its Policy on Student Acceptable Use of the CPS Network to include new internet safety provisions in compliance with CIPA (Board Report 02-0626-PO04.) The Board subsequently adopted a modified Policy on Student Acceptable Use of the CPS Network (Board Report 03-0326-PO03), which superseded the previous policy yet maintained the internet safety provisions. On June 26, 2002, the Board adopted amendments to its Policy on Use of the Internet, CPS Intranet, Electronic Mail and Computer Access by Authorized Users to include internet safety provisions in compliance with CIPA (See Board Report 02-0626-PO03). This policy addresses the use of the CPS network by employees and other adult users. The Board modified this policy under Board Report 04-0428-PO2, which superseded the previous policy yet maintained the internet safety provisions. On July 22, 2009, the Board adopted a new policy on the Acceptable Use of the CPS Network and Computer Resources (See Board Report 09-0722-PO3) which rescinded Board Report 04-0428-PO2, but maintained the provisions pertaining to internet safety.

POLICY TEXT:

I. Introduction

It is the policy of the Chicago Board of Education: (a) to prevent use of the CPS computer network to access or transmit, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) to prevent unauthorized access to the CPS computer network and other unlawful online activity; (c) to prevent unauthorized online disclosure, use, or dissemination of student record information; and (d) to comply with the Children's Internet Protection Act also with federal and state requirements for internet safety education for students.

II. Access to Inappropriate Material

As required by law, CPS uses technology protection measures to block or filter internet sites for inappropriate material that is harmful to minors and prohibit access, to the extent possible, to such content found on the internet. In addition to the use of filtering technology, the Office of Information & Technology Services (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 computer network or otherwise disabling or modifying the district's technology protection measures. All blocking and unblocking decisions will be made by ITS in compliance with applicable laws and the requirements of this policy. Technology protection measures may be disabled for District administrators, supervisors or other authorized staff to access materials via the internet for bona fide research, legitimate educational purposes or other lawful purposes.

III. Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the CPS network and when using the CPS computer resources. The District takes reasonable precautions to prevent (a) the unauthorized access, including so-called 'hacking' and other unlawful activities, and (b) the unauthorized disclosure, use, and dissemination of student record information. These precautions include, but are not limited to: network provisioning protocols, confidential passwords, network firewalls, data encryption, electronic monitoring and physical data security.

IV. Student Internet Safety Education and Supervision

Each school shall incorporate into the school curriculum a component on internet safety to be taught at least once each school year to all students. The Chief Education Officer or designee shall determine the scope, age-appropriate components, duration and topics covered in this unit of instruction. At a minimum, the unit of instruction shall address: (a) safety on the Internet; (b) appropriate behavior while on online, on social networking Web sites, and in chat rooms; and (c) cyberbullying awareness and response. The unit of instruction may be incorporated into the current courses of study regularly taught.

Each school shall satisfy the documentation requirements established by the Chief Education Officer or designee to ensure compliance with this curricular requirement.

In addition, the school principal shall ensure that school personnel supervise students for appropriate usage of the CPS computer network and access to the internet in accordance with this policy and ensure the CPS computer network is used to support the school's educational program.

V. 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 computer network and computer resources in order to execute the requirements of this policy. CPS network including but not limited to internet and email 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 computer network or 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 or other electronic communication for business, legal or security purposes.

The CPS computer network and computer resources are for educational and business use only. Even with the technology protection measures and other mandates contained in this policy, the Board cannot guarantee that a student or staff member will not gain access to objectionable or inappropriate Internet material.

VI. Adoption

This Internet Safety Policy was adopted by the Chicago Board of Education at its regular monthly Board Meeting held on June 27, 2012, following standard public notice procedures and compliance with public participation requirements and other applicable statutory requirements for conducting its monthly meeting.

LEGAL REFERENCES: 105 ILCS 5/27-13.3; Protecting Children in the 21st Century Act, Pub. L. No. 110-385, Title II, 122 Stat. 4096 (2008); 47 C.F.R. 54.520; Children's Internet Protection Act, 47 USC 254(h); Federal Communications Commission Report and Order FCC 11-125.

Approved for Consideration:

Tim Cawley
Chief Administrative Officer

Respectfully submitted:

Jean-Claude Brizard
Chief Executive Officer

Noted:

David G. Watkins
Chief Financial Officer

Approved as to Legal Form:

Patrick J. Rocks
General Counsel