DISTRICT POLICY

POLICY SERIES: Technology & Communication
SUBJECT:
BOARD APPROVED: February 2012
REVISION DATE: February 2015

TC120 Technology Responsible Use and Safety Policy

I. PURPOSE

The purpose of this policy is to set forth guidelines for the safe and responsible use of the District's technology. The District's technology includes but is not limited to desktop computers, laptops, netbooks, telephones, voicemail, mobile phones, other wireless devices, mobile computing devices and the applications they support and/or access.

II. GENERAL STATEMENT OF POLICY

In making decisions regarding student and employee access to the District's technology, the District considers its own stated educational mission, goals and objectives. Electronic information research skills are now fundamental to the preparation of citizens and future employees. The District expects instructional staff to integrate thoughtful use of the District's technology throughout the curriculum and to provide guidance and instruction to students to use these resources safely and wisely.

III. LIMITED EDUCATIONAL PURPOSE

The District provides students and employees with access to its technology for a limited educational purpose. This limited educational purpose includes use of the District's technology for classroom activities, educational research, and professional or career development activities consistent with the mission of the District and its policies. Use of the internet may include using electronic mail, creating Internet Web pages, and sending, receiving, storing and sharing documents. Students will receive information about safe and responsible use of the internet, including how to protect their personal information when communicating on the internet, cyberbullying and harassment. Uses, which might be responsible on a user's private personal account on another system, may not be responsible on this limited-purpose network.

IV. USE OF TECHNOLOGY IS A PRIVILEGE

A. The use of District technology is a privilege, not a right. When using District technology, students and staff shall not utilize language that is inappropriate in the educational setting or is disruptive to the educational process; engage in activities that are illegal; engage in plagiarism or copyright infringement or engage in actions that jeopardize the security of the technology. District technology shall not be used to: vandalize, damage or disable the property of another person or organization; deliberately degrade or disrupt equipment, software or system performance by spreading computer viruses or by any other means; tamper with, modify or change the District software, hardware or wiring or take any action

to violate the District's security system; or disrupt the use of the system by other users. District technology shall be used in a manner that protects the confidentiality of information about students and staff and is fully in accord with the student and staff confidentiality protection requirements of federal law, state law, and District policy. A complete list of irresponsible uses may be found in the District's procedure on Technology Responsible Use and Safety.

B. The District has the authority to impose consequences on and take disciplinary measures against any student or employee who engages in an act that has the effect of harassing, intimidating, or otherwise advocating violence or discrimination against other people that takes place through the use of District technology, use of a personal electronic device on District property, or any off-campus activities that cause or threaten to cause a substantial or material disruption at school or interference with the rights of students and employees to be secure. Depending on the nature and degree of the violation and the number of previous violations, irresponsible use of the District technology or the Internet may result in one or more of the following consequences: suspension or cancellation of use or access privileges; payments for damages and repairs; discipline under other appropriate District policies, including suspension, expulsion, exclusion or termination of employment; or civil or criminal liability under applicable laws.

V. FILTER

A. With respect to any of its technology, the District may at any time monitor the online activities of minors and employ technology protection measures during any use of such computers by minors and adults. The technology protection measures utilized will block or filter internet access to any visual depictions that are 1) obscene; 2) child pornography; or 3) harmful to minors.

B. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:
   1) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or
   2) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; or
   3) is intended to or could reasonably be expected to have the effect of promoting or inciting violence towards other people; and
   4) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

   Due to the nature of the internet, there can be no absolute guarantee that the technology protection measures implemented will fully protect students against access to material or people that may be considered inappropriate or potentially harmful. The District will not be responsible for any damage students may suffer if they accidentally or intentionally are exposed to such materials or people.

VI. LIMITED EXPECTATION OF PRIVACY

By authorizing use of its technology, the District does not relinquish control over materials on the District's system. Users should expect only limited privacy in the materials (including personal files) on the District's system.

CROSS REFERENCES:
Internet Filtering: A New Vision for Promoting Responsible Student Use of Information
Cellular Devices Procedure
Social Media Guidelines for Staff and Students
Staff E-mail Guidelines and Operating Procedures
Staff Security Guidelines and Procedures
Equipment Management Procedures

LEGAL REFERENCES:
15 U.S.C. § 6501 *et seq* (Children's Online Privacy Protection Act)
17 U.S.C. § 101 *et seq* (Copyrights)
20 U.S.C. § 6751 *et seq* (Enhancing Education through Technology Act of 2001)
17 U.S.C. § 1701 *et seq* (Children's Internet Protection Act of 2000 (CIPA))
47 C.F.R. 54.520 (FCC rules implementing CIPA)
Minn. Stat. § 125B.15 (Internet Access for Students)
Tinker v. Des Moines Indep. Sch. Dist., 393 U.S. 503, 89 S. Ct. 733, 21 L.Ed.2d 731 (1969)
United States v. American Library Association, 539 U.S. 194, 123 S. Ct. 2297, 56 L.Ed.2d 221 (2003)
Layshock v. Hermitage Sch. Dist., 412 F. Supp. 2d 502 (2006)
J.S. v. Bethlehem Area Sch. Dist., 807 A.2d 847 (Pa. 2002)