INSTRUCTIONAL SERVICES **Policy 6320**
(Regulation 6320)

Libraries, Media and Technology Services

Internet Safety Policy

A. Introduction

It is the policy of the District to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

B. Access to Inappropriate Material

To the extent practical, technology protection measures shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

C. Internet Safety Training

In compliance with the Children's Internet Protection Act, each year, all District students will receive internet safety training which will educate students about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, and cyberbullying awareness and response. Such training will include Internet, cell phones, text messages, chat rooms, email and instant messaging programs. (See also Policy 6116 – State Mandated Curriculum – Human Sexuality).

D. Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the District's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

E. Supervision and Monitoring

It shall be the responsibility of all District employees to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet protection Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of Technology Coordinator or designated representatives.

****

Approved 11/19/2015