Note: For Board member use of District technology resources, see BBI. For student use of personal electronic devices, see FNCE.

For purposes of this policy, "technology resources" means electronic communication systems and electronic equipment.

Availability of Access

Access to the District's technology resources, including the Internet, shall be made available to students and employees primarily for instructional and administrative purposes and in accordance with administrative regulations.

Limited Personal Use

Limited personal use of the District's technology resources shall be permitted if the use:

1. Imposes no tangible cost on the District;
2. Does not unduly burden the District's technology resources; and
3. Has no adverse effect on an employee's job performance or on a student's academic performance.

Use by Members of the Public

Access to the District's technology resources, including the Internet, shall be made available to members of the public, in accordance with administrative regulations. Such use shall be permitted so long as the use:

1. Imposes no tangible cost on the District;
2. Does not unduly burden the District's technology resources; and
3. Is for participation in the District's education-related activities.

Acceptable Use

The Superintendent or designee shall develop and implement administrative regulations, guidelines, and user agreements consistent with the purposes and mission of the District and with law and policy.

Access to the District's technology resources is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the District's technology resources and shall agree to allow monitoring of their use and to comply with such regulations and guidelines.

Noncompliance

Noncompliance with this policy and applicable regulations shall result in:

1. Verbal or written warning by network administrator or designee;

2. Temporary reduction or suspension of computer system privileges;
3. Referral to immediate supervisor;
4. Permanent access revocation;
5. Termination of employment; or
6. Referral to appropriate law enforcement agencies for misuse amounting to criminal behavior.

Alleged violations shall be reviewed on a case-by-case basis. Violations of law may result in criminal prosecution as well as disciplinary action by the District. Disciplinary action shall be consistent with District policies. [See DH, CQ(REGULATION), FN series, FO series, and the Student Code of Conduct]

Improper Personal Internet Use

A student's home and personal Internet use can have an impact on the school and other students. If a student's personal Internet expression—such as a threatening message to another student, a District employee, or a violent website—creates a likelihood of material disruption of the school's operations, the student may face school discipline and criminal penalties.

Cyber Harassment

The District takes bullying, stalking, and harassment by computer very seriously. A student shall not use any Internet or other communication device to intimidate, bully, harass, stalk, or embarrass other students or staff members. A student who engages in such activity on school grounds or who engages in such activity off campus and creates a material disruption of school operations shall be subject to penalties for bullying and harassment contained in the student handbook, as well as possible criminal penalties.

Monitored Use

Internet use, file transfers (FTP), electronic mail transmissions, and other uses of the District's electronic communications system by students, employees, and the public, are not private and may be monitored at any time by designated District staff to ensure appropriate use.

Standards for Personal Expression on the Internet

The following restrictions against inappropriate speech and messages apply to all speech communicated and accessed through the District's Internet system, including all e-mail, instant messages, webpages, and web logs. Students and employees shall not send obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful messages. Students and employees shall not post information that could cause damage, danger, or disruption, or engage in personal attacks, including prejudicial or discriminatory attacks. Students shall not harass another person, or

knowingly or recklessly post false or defamatory information about a person or organization.

Internet Safety and Filtering

The Superintendent or designee shall develop and implement an Internet safety plan to:

1. Control students' access to inappropriate materials, as well as to materials that are harmful to minors;
2. Ensure student safety and security when using electronic communications;
3. Prevent unauthorized access, including hacking and other unlawful activities;
4. Restrict unauthorized disclosure, use, and dissemination of personally identifiable information regarding students; and
5. Educate students about cyberbullying awareness and response and about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms.

Each District computer with Internet access and the District's network systems shall have filtering devices or software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act and as determined by the Superintendent or designee.

Filter Disabling

Students and staff may not disable the District's filtering software at any time when students are using the Internet system if such disabling will cease to protect against access to inappropriate materials. Authorized staff may temporarily or permanently unblock access to sites containing appropriate material if the filtering software has inappropriately blocked access to such sites.

Student Due Process

In the event of a claim that a student has violated this policy, the District shall provide the student with notice and an opportunity for a hearing in the manner set forth in the student handbook. [See also Student Code of Conduct]

Disclaimer of Liability

The District shall not be liable for users' inappropriate use of the District's technology resources, violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. The District shall not be responsible for ensuring the availability of the District's technology resources or the accuracy, age appropriateness, or usability of any information found on the Internet.

Record Retention

A District employee shall retain electronic records, whether created or maintained using the District's technology resources or using

personal technology resources, in accordance with the District's record management program. [See CPC]

Security Breach Notification

Upon discovering or receiving notification of a breach of system security, the District shall disclose the breach to affected persons or entities in accordance with the time frames established by law.

The District shall give notice by using one or more of the following methods:

1. Written notice.
2. Electronic mail, if the District has electronic mail addresses for the affected persons.
3. Conspicuous posting on the District's website.
4. Publication through broadcast media.