The Superintendent or designee shall implement, monitor, and evaluate electronic media resources for instructional and administrative purposes.

AVAILABILITY OF ACCESS

Access to the District's electronic communications system, 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 of the system shall be permitted if the use:

LIMITED PERSONAL USE

1. Imposes no tangible cost to the District;
2. Does not unduly burden the District's computer or network 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 electronic communications system, including the Internet, shall be made available to members of the public, in accordance with administrative regulations. Such use may be permitted so long as the use:

1. Imposes no measurable cost on the District;
2. Does not unduly burden the District's computer or network resources; and
3. Is for participation in the District's educational related activities.

Members of the public who are granted access shall be required to:

1. Comply with all District rules, regulations, and policies governing appropriate use of the system;
2. Attend training on the District's acceptable use policies; and
3. Submit a signed copy of the Exhibit D form prior to accessing the District's electronic communications system. [See CQ(EXHIBIT)]

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 laws and policies.

Access to the District's electronic communications system is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree in writing to allow monitoring of

their use and to comply with such regulations and guidelines. [See CQ Regulations]

NONCOMPLIANCE

Noncompliance with applicable regulations may 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, FN series, FO series, and the Student Code of Conduct]

IMPROPER PERSONAL INTERNET USE

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

CYBER HARASSMENT

The District takes bullying, stalking, and harassment by computer very seriously. Students shall not use any Internet or other communication device to intimidate, bully, harass, stalk, or embarrass other students or staff members. Students who engage in such activity on school grounds or who engage in such activity off campus and create 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, Web pages, 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 Web sites and in chat rooms.

Each District computer with Internet access shall have a filtering device 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.

INTELLECTUAL PROPERTY RIGHTS

Students shall retain all rights to work they create using the District's electronic communications system.

As agents of the District, employees shall have limited rights to work they create using the District's electronic communications

system. The District shall retain the right to use any product created for its use by an employee even when the author is no longer an employee of the District.

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 to be heard in the manner set forth in the student handbook.

DISCLAIMER OF LIABILITY

The District shall not be liable for users' inappropriate use of electronic communication resources or 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 accuracy, age appropriateness, or usability of any information found on the Internet.