SECTION 11 — COMPUTER/INTERNET ACCEPTABLE USE POLICY

The District provides students with access to the District's computers, electronic communication systems and network, which includes Internet access, whether wired or wireless, or by any other means. However, a student's use of the District's computers and Internet resources is a privilege, not a right. Student-users of the District's computer network and Internet access are expected to use this technology as an educational resource.

Student computer network/Internet users are expected to behave responsibly in accessing and viewing information that is pertinent to the educational mission of the District. Students are required to abide by the generally accepted rules of network etiquette and rules as outlined in this Acceptable Use Policy.

Definitions

The term **child pornography** is defined under both federal and state law.

Child pornography - under federal law, is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
2. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Child pornography - under state law, is any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited sexual act or in the simulation of such act.

The term **harmful to minors** is defined under both federal and state law.

Harmful to minors - under federal law, is any picture, image, graphic image file or other visual depiction that:

1. Taken as a whole, with respect to minors, appeals to a prurient interest in nudity, sex or excretion;
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 lewd exhibition of the genitals; and
3. Taken as a whole lacks serious literary, artistic, political or scientific value as to minors.

Harmful to minors - under state law, is any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:

1. Predominantly appeals to the prurient, shameful, or morbid interest of minors;

2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and

3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value for minors.

Obscene - any material or performance, if:

1. The average person applying contemporary community standards would find that the subject matter taken as a whole appeals to the prurient interest;

2. The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene; and

3. The subject matter, taken as a whole, lacks serious literary, artistic, political, educational or scientific value.

Technology protection measure - a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.

Policy:

The availability of access to electronic information does not imply endorsement by the District of the content, nor does the District guarantee the accuracy of information received. The District shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.

The District shall not be responsible for any unauthorized charges or fees resulting from access to the Internet or other network resources.

Student use of the District's computers and network is a privilege, not a right. The District's computer and network resources are the property of the District. Student users shall have no expectation of privacy in anything they create, store, send, delete, receive or display on or over the District's Internet, computers or network resources, including personal files or any use of the District's Internet, computers or network resources. The District reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization by District users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. The District shall cooperate to the extent legally required with the Internet Service Provider (ISP), local, state and federal officials in any investigation concerning or related to the misuse of the District's Internet, computers and network resources.

Students must fully comply with this Acceptable Use Policy and must immediately report any violations or suspicious activities to the Superintendent or Building Principal/Administrative staff.

The following materials, in addition to those stated in law and defined in this Policy, are inappropriate for access by students generally and minors specifically:

1. Defamatory.

2. Lewd, vulgar, or profane.

3. Threatening.

4. Harassing or discriminatory.

5. Bullying.

6. Terroristic.

The District reserves the right to restrict access to any Internet sites or functions it deems inappropriate through established Board policy, or the use of software and/or online server blocking. Specifically, the District operates and enforces a

technology protection measure(s) that blocks or filters access to inappropriate matter by minors on its computers used and accessible to adults and students. The technology protection measure shall be enforced during use of computers with Internet access.

Upon request by students or staff, the Superintendent or designee shall expedite a review and may authorize the disabling of Internet blocking/filtering software to enable access to material that is blocked through technology protection measures but is not prohibited by this policy.

Upon request by students or staff, building administrators may authorize the temporary disabling of Internet blocking/filtering software to enable access for bona fide research or for other lawful purposes. Written permission from the parent/guardian is required prior to disabling Internet blocking/filtering software for a student's use. If a request for temporary disabling of Internet blocking/filtering software is denied, the requesting student or staff member may appeal the denial to the Superintendent or designee for expedited review.

Guidelines:

Network accounts shall be used only by the authorized owner of the account for its approved purpose. Student network users shall respect the privacy of other users on the system.

Safety

It is the District's goal to protect student (and other) users of the network from harassment and unwanted or unsolicited electronic communications. Any network user who receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site shall report such immediately to a teacher or District administrator. Network users shall not reveal personal information to other users on the network, including chat rooms, email, social networking websites, etc.

The District imposes internet safety measures which address the following:

1. Control of access by minors and students to inappropriate matter on the Internet and World Wide Web.
2. Safety and security of minors students when using electronic mail, chat rooms, and other forms of direct electronic communications.
3. Prevention of unauthorized online access by minors and students, including "hacking" and other unlawful activities.
4. Unauthorized disclosure, use, and dissemination of personal information regarding minors and all other students.
5. Restriction of minors' and all other students' access to materials harmful to them.

Prohibitions

Users of the District's computers and network are expected to act in a responsible, ethical and legal manner in accordance with District policy, accepted rules of network etiquette, and federal and state law. Specifically, the following uses are prohibited:

1. Facilitating illegal activity.
2. Commercial or for-profit purposes.
3. Nonwork or nonschool related work.
4. Product advertisement or political lobbying.
5. Bullying/Cyberbullying.

6. Hate mail, discriminatory remarks, and offensive or inflammatory communication.

7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.

8. Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal materials, images or photographs.

9. Access by students and minors to material that is harmful to minors and students or is determined inappropriate for minors and students in accordance with Board policy.

10. Inappropriate language or profanity.

11. Transmission of material likely to be offensive or objectionable to recipients.

12. Intentional obtaining or modifying of files, passwords, and data belonging to other users.

13. Impersonation of another user, anonymity, and pseudonyms.

14. Fraudulent copying, communications, or modification of materials in violation of copyright laws.

15. Loading or using of unauthorized games, programs, files, or other electronic media.

16. Disruption of the work of other users.

17. Destruction, modification, abuse or unauthorized access to network hardware, software and files.

18. Accessing the Internet, District computers or other network resources without authorization.

19. Disabling or bypassing the Internet blocking/filtering software without authorization.

20. Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization.

Security

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or District files. To protect the integrity of the system, these guidelines shall be followed:

1. Students shall not reveal their passwords to another individual.

2. Users are not to use a computer that has been logged in under another student's or employee's name.

3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

Copyright

The illegal use of copyrighted materials is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines and applicable laws and regulations.

District Website

The District shall establish and maintain a website and shall develop and modify its web pages to present information about the District under the direction of the Superintendent or designee. All users publishing content on the District website shall comply with this and other applicable District policies.

Users shall not copy or download information from the District website and disseminate such information on unauthorized web pages without authorization from the building principal.

Consequences for Inappropriate Use

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

Illegal use of the network; intentional deletion or damage to files or data belonging to others; copyright violations; and theft of services shall be reported to the appropriate legal authorities for possible prosecution.

General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this Acceptable Use Policy.

Vandalism shall result in loss of access privileges, disciplinary action, and/or legal proceedings. **Vandalism** is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses.

Failure to comply with this policy or inappropriate use of the Internet, District network or computers shall result in usage restrictions, loss of access privileges, disciplinary action which include consequences up to and including expulsion from the District, and/or legal proceedings.

3.