

## **GUIDELINES FOR ACCEPTABLE USE OF DISTRICT TECHNOLOGY SYSTEM BY STUDENTS**

### **A. Acceptable Use.**

All users of the District Technology system must comply with the District Acceptable Use Guidelines, as amended from time to time.

The System shall include all computer hardware and software owned or operated by the District, the District electronic mail, the District web site, and the District on-line services and bulletin board systems. Use of the System shall include use of or obtaining access to the System from any computer terminal whether owned or operated by the District.

Students have no expectation of privacy in their use of the System. The District has the right to access, review, copy, delete, or disclose, as allowed by law, any message sent, received, or stored on the District's electronic mail system. The District has the right to and does monitor use of the System by students, including student's access of the Internet, as part of System maintenance and to determine whether the use is consistent with federal and state laws and District policies and guidelines.

Employees of the district are instructed to continuously monitor and supervise all students, in the classroom or in a lab setting, when they are participating in an Internet activity to ensure that they are not engaged in inappropriate activities such as trying to bypass district filters in order to access obscene web sites. They are also to monitor students to be sure they are not participating in other unlawful activities such as hacking into servers or administrative computers in order to change grades or obtain personal information on other students or staff. Employees are also instructed to limit student use of personal e-mails and participation in on-line chat rooms or other Internet sites where personal information could be disclosed.

## **B. Privileges.**

Access to the System is provided as a privilege by the District and may be revoked at any time. Inappropriate use may result in discipline, including loss of System use privileges.

The System, including all information and documentation contained therein is the property of the District except as otherwise provided by law.

The district technology coordinator periodically monitors and reviews the access logs generated by the filtering system (SonicWall Firewall and Internet Filter). This filtering system blocks the visual depiction of obscenity, child pornography, and materials harmful to minors.

## **C. Prohibited Use.**

The uses of the System listed below are prohibited and may result in discipline or other consequences as provided in section I of these Guidelines and the District's Student Discipline Code and rules. The System shall **not** be used to:

1. Engage in activities that are not related to District educational purposes or which are contrary to the instructions from supervising District employees as to the System's use.
2. Access, retrieve, or view obscene, profane or indecent materials. Indecent materials are those materials that, in context, depict or describe sexual activities or organs in terms patently offensive, as measured by contemporary community standards. Obscene materials are those materials which, taken as a whole, appeal to the prurient interest in sex, which portray sexual conduct in a patently offensive way in which, taken as a whole, do not have any serious literary, artistic, political or scientific value.
3. Access, retrieve, view or disseminate any material in violation of any federal or state laws or regulation or District policy or rules. This includes, but is not limited to, improper use of copyrighted material; improper use of the System to commit fraud or with the intent to commit fraud; improper use of passwords or access codes; or disclosing the full name, home address, or phone number of any student, District employee, or System user.

4. Transfer any software to or from the System without authorization from the System Administrator.
5. Engage in for-profit or non-school sponsored commercial activities, including advertising or sales.
6. Harass, threaten, intimidate, or demean an individual or group of individuals because of sex, color, race, religion, disability, national origin or sexual orientation.
7. Disrupt the educational process, including use that is reasonably foreseeable to result in a disruption, or interfere with the rights of others at any time, either during school days or after school hours.
8. Disrupt or interfere with the System.
9. Gain unauthorized access to (including hacking and other unlawful online activities by minors) or vandalize the data or files of another user.
10. Gain unauthorized access to (including hacking and other unlawful online activities by minors) or vandalize the System or the technology system of any other individual or organization.
11. Forge or improperly alter electronic mail messages, use an account owned by another user, or disclose the user's individual password or that of another user.
12. Invade the privacy of any individual, including violating federal or state laws regarding limitations on the disclosure of student records.
13. Download, copy, print or otherwise store or possess any data which violates federal or state copyright laws or these Guidelines.
14. Send nuisance electronic mail or other online messages such as chain letters, pyramid schemes, or obscene, harassing or other unwelcome messages.
15. Send mass electronic mail to multiple users without prior authorization by the appropriate District Administrator.

16. Conceal or misrepresent the user's identity while using the System.
17. Post material on the District's web site without the authorization of the appropriate District administrator.

**D. Discipline for off-site use of electronic technology that disrupts or can reasonably be expected to disrupt the school environment**

The District may discipline a student whose personal web site or other off-site activity involving electronic technology causes, or can reasonably be expected to cause, a substantial disruption of the school environment, without regard to whether that activity or disruption involved use of the District Technology System.

**E. Web sites.**

Unless otherwise allowed by law, District web sites shall not display information about or photographs or works of students without written parental permission.

Any web site created by a student using the System must be part of a District-sponsored activity, or otherwise be authorized by the appropriate District administrator. All content, including links, of any web site created by a student using the System must receive prior approval by the classroom teacher or an appropriate District administrator. All contents of a web site created by a student using the System must conform with these Acceptable Use Guidelines.

**F. Disclaimer.**

The District makes no warranties of any kind whether express or implied for the System. The District is not responsible for any damages incurred, including the loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions. Use of any information obtained via the System is at the user's own risk. The District is not responsible for the accuracy or quality of information obtained through the System. The District is not responsible for any user's intentional or unintentional access of material on the Internet that may be obscene, indecent, or of an inappropriate nature.

## **G. Security and User Reporting Duties.**

Security in the System is a high priority and must be a priority for all users. Students are prohibited from sharing their login IDs or passwords with any other individual. Any attempt to log in as another user will result in discipline.

A user who becomes aware of any security risk or misuse of the System must immediately notify a teacher, administrator or other staff member.

## **H. Vandalism.**

Vandalism or attempted vandalism to the System is prohibited and will result in discipline as set forth in section I of these Guidelines, and in potential legal action. Vandalism includes, but is not limited to, downloading, uploading, or creating computer viruses.

## **I. Consequences for Violations.**

Violations to the district's AUP/Internet Safety Policy are reported to the appropriate building principal. A student who engages in any of the prohibited acts listed above shall be subject to discipline, which may include: (1) suspension or revocation of System privileges, (2) other discipline including suspension or expulsion from school, and (3) referral to law enforcement. Misuse of the System by a student may be considered gross misconduct as that term is defined by the District Student Discipline Policy and rules, and a student may be subject to discipline pursuant to the Student Discipline Policy and rules. A student who believes that his/her System use privileges have been wrongfully limited may request a meeting with the building principal to review the limitation. The decision of the building principal shall be final.