INTERNET PROTECTION

The District provides its students and employees with access to the District's computer network system, including Internet access, in an effort to expand the informational and communication resources in furtherance of the District's goal of promoting educational excellence. It is hoped that the expanded use of these resources will enhance students' research capabilities, increase faculty and staff productivity, and result in better communication between the District and its patrons.

The Internet has often been described as the information super-highway and over time has expanded worldwide, permitting access and communication with a vast number of resources and individuals. Through the Internet, the District will provide students, faculty, and staff access to:

- electronic mail providing communication with people throughout the world;
- information and news, including the opportunity to correspond with scientists at research institutions in the public and private sector, including NASA;
- public domain software and shareware of all types;
- news groups, or discussion groups, covering a wide range of topics appropriate to the educational purposes of the District;
- access to university libraries, the Library of Congress, and other repositories of information;
- World Wide Web access to information containing text, graphics, and photographs, as well as sound on literally millions of topics

With access to such vast storehouses of information and instant communication with millions of people from all over the world, material will be available that may not be considered to be of educational value by the District or which is inappropriate for distribution to students. The District has taken available precautions including, but not limited to, enforcing the use of filters that block access to obscenity, child pornography, and other materials harmful to minors. However, on a global network, it is impossible to control all material, and an industrious user may obtain access to inappropriate information or material. The District firmly believes that the value of the information and interaction available on the Internet far outweighs the possibility that students and employees may procure material which is not consistent with our educational goals.

Internet access is coordinated through a complex association of government agencies and regional and state networks. The smooth operation of these networks relies upon the proper conduct of the end users and the users' adherence to generally accepted guidelines. The guidelines provided in this policy are designed to promote the efficient, ethical, and legal utilization of network resources. If a District user violates any of these provisions, his or her account may be terminated, and future access could be denied.

Students' use of the District's system will also be governed by the School Behavior Response Plan.

Internet Access - Terms and Conditions.

Acceptable Use. The use of the District’s system, whether by students, faculty, or staff, must be in support of education and consistent with the educational objectives of the District. The use of any other organizations' network or computing resources must comply with the rules and regulations appropriate for that network. The transmission or receipt of any material in violation of any United States or state law or regulation and the transmission or receipt of any material inconsistent with the educational objectives of the District is prohibited. This includes, but is not limited to: copyrighted material, threatening, indecent, lewd, or obscene material, or material protected by trade secret. Use of the District system for commercial activities is not acceptable. Use for product advertisement or political lobbying is also prohibited.

Parental Oversight. In order for a student to gain access to the District system, the student's parent or guardian must be provided a copy of the Internet Protection and Safety Policy. There is a wide range of information available through the Internet which is not appropriate for access by minors, has no educational value or does not meet with the particular values of the families of the student. The District system and Internet Protection and Safety Policy contain devices and restrictions on use intended to prevent access to inappropriate material or information. However, it is impossible for the District to guarantee that students will not be exposed to inappropriate material through their use of the Internet. The District believes that parents bear primary responsibility for communicating acceptable behavior and family values to their children. The District encourages parents to discuss with their children what material is and is not acceptable for their children to access through the District system.

Privilege of Use. The District system and its Internet access is a privilege afforded to students and staff of the District. Use of these resources is not a right, and inappropriate use may result in a cancellation of those privileges. Inappropriate use is any use prohibited by the terms of this policy or use determined by the District's system administrators to be inappropriate under particular facts and circumstances. Prior to receiving Internet access, all users will be required to successfully complete an Internet training program administered by the District.

Inappropriate Use. Each system user is expected to comply with all District policies governing Internet access and to abide by generally-accepted rules of network etiquette. These general rules include, but are not limited to, the following:

a. Appropriate language - Do not use abusive language in messages to others. Be polite. Do not use obscene, indecent, lewd or profane language, vulgarities, rude or disrespectful language. Do not engage in personal attacks or activities intended to distress, harass, or annoy another user.

b. Safety - Do not reveal personal contact information about yourself or any other person. This information includes telephone numbers and addresses. Do not use the Internet access to arrange meetings with persons you have met on-line.
Users will promptly disclose to the teacher, District system administrator, or to some other member of the faculty or staff any message they consider to be inappropriate or which makes them feel uncomfortable.

c. Electronic mail - Users should be aware that electronic mail (E-Mail) may not be assumed or expected to be a private communication. The District and system administrators do have access to E-Mail. Messages relating to, in support of, or in furtherance of illegal activities will be reported to the authorities. System users should not post any message which is intended to be private.

d. Network resources - System users should not use the network in a way that will disrupt the use of the network by other users. The network should be used for educational, professional, and career development activities only. System users should refrain from downloading large files unless absolutely necessary, and then only when the system is not being heavily used. Such files should be removed from the system when no longer needed.

e. Intellectual property - Do not plagiarize works obtained from the Internet. Users must respect the rights of copyright owners and comply with all limitations imposed upon use of copyrighted material.

Limitation of Liability. The District makes no warranties of any kind, whether express or implied, for the services provided and will not be responsible for any damages which you may suffer through use of the District system or the Internet, including, but not limited to, the loss of information or files or the interruption of service. The District is not responsible for the accuracy or quality of information obtained through use of the District system or the Internet. The District is not responsible for any financial obligations which may be incurred through use of the District system.

Security. Security on any computer system is a high priority, especially when the system involves multiple users. Users are responsible for their individual account and should take precautions to prevent others from accessing that account. Under no conditions should a user provide their personal password to another person. If you identify a potential security problem on the District system or the Internet, you must notify the Information Systems Services department immediately. You should not demonstrate the problem to others, nor should you intentionally attempt to identify potential security problems. In either instance, your actions may be misinterpreted as an illegal attempt to gain unauthorized access. Any attempt to log on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with the District system or any other computer system may be denied further access.

Vandalism. Vandalism of District hardware, software, or the system itself will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy the property or data of the District, of another user, or of any other network connected to the Internet or all or any portion of the District's computer network system or any other network or system connected to the Internet. This includes, but is not limited to, the uploading or creation of computer viruses or any actions that disrupt, "crash," or otherwise interfere with the operation of all or any portion of the District's computer system. All system users shall avoid the accidental spread of computer viruses by strict adherence to District policies governing the downloading of software. No system user may use the system to "hack" or attempt to gain unauthorized access to any other computer system, network, or site, or any unauthorized portion of the District's system.

Inappropriate Material. Access to information shall not be restricted or denied solely because of the political, religious, or philosophical content of the material. However, system users must realize that rights go hand-in-hand with responsibilities and agree not to use the District system to access information or to distribute information or material which is:

a. Obscene to minors, meaning material which, taken as a whole, lacks serious literary, artistic, political, or scientific value for minors and, when an average person, applying contemporary community standards, would find that the written material, taken as a whole, appeals to an obsessive interest in sex by minors.

b. Libelous, meaning a false and unprivileged statement about a specific individual which tends to harm the individual's reputation.

c. Vulgar, lewd, or indecent, meaning material which, taken as a whole, an average person would deem improper for access by or distribution to minors because of sexual connotations or profane language.

d. Displaying or promoting unlawful products or services, meaning material which advertises or advocates the use of products or services prohibited by law from being sold or provided to minors.

e. Group defamation or hate literature, meaning material which disparages a group or a member of a group on the basis of race, color, sex, gender expression, gender identity, national origin, religion, disability, veteran status, sexual orientation, age, or genetic information or advocates illegal conduct or violence or discrimination toward any particular group of people. This includes racial and religious epithets, "slurs," insults, and abuse.

f. Disruptive to school operations, meaning material which, on the basis of past experience or based upon specific instances of actual or threatened disruptions relating to the information or material in question, is likely to cause a material and substantial disruption of the proper and orderly operation of school activities or school discipline.

Employee Access. In order for any employee of the District to gain access to the District system, the employee must sign the *Employee Internet and Computer Network Usage Agreement*.

Application and Enforceability. The terms and conditions set forth in this policy shall be deemed to be incorporated in their entirety in the Employee Internet and Computer Network Usage Agreement executed by each system user. By executing the Employee Internet and Computer Network Usage Agreement, the system user agrees to abide by the terms and conditions contained in this policy. The system user acknowledges that any violation of this policy may result in access privileges being revoked, disciplinary action being taken, including, as to students, disciplinary action under the District's Student Discipline Policy and, as to employees, any such discipline as may be allowed by law, including termination of employment.

Education of Students Regarding Appropriate On-Line Behavior. In compliance with the Protecting Children in the 21st Century Act, Section 254(h)(5), the District is educating minors about appropriate on-line behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. Faculty and staff are required to monitor the on-line activities of minors. As part of this education, the following information on cyberbullying and Internet Safety is distributed with this Policy to all students and parents.

Cyberbullying and Internet Safety

As young people embrace the Internet and other mobile communication technologies, bullying has manifested itself in a new and potentially more dangerous way – through cyberbullying. Cyberbullying can generally be defined as sending or posting harmful, harassing, intimidating, threatening, or malicious messages or images through e-mail, instant messages, cell phones, and websites. It is emerging as one of the more challenging issues facing educators since it has a direct impact on students but often occurs away from school property.

Examples of cyberbullying include, but are not limited to:

- Sending cruel, vicious, and sometimes threatening messages;
- Creating websites that contain stories, cartoons, pictures, and jokes ridiculing others;
- Posting pictures of classmates on-line with intent to embarrass them;
- Breaking into an e-mail account and sending vicious or embarrassing material to others;
- Engaging in IM (instant messaging) to trick another person into revealing sensitive or personal information and forwarding that information to others; and
- Taking a picture of a person using a digital phone camera and sending that picture electronically to others without consent, or the equivalent of that.

Social Networking

Most teenagers visit websites to communicate with friends and meet new people. Social networking sites, have become increasingly popular with students. Many social networking sites allow students to create a personal website (for free), post pictures, add comments, and use it to meet “on-line friends.” The website often includes their full name, telephone number, address, school name, and a picture.

YouTube is a similar site dedicated to hosting video clips.

Hundreds of millions of people reportedly use social networking sites, including, but not limited to, myspace.com, twitter.com, friendster.com; livejournal.com; nexopia.com; and facebook.com. A significant number of users are younger than 18. The danger lies in that the Internet is vast, public, and constantly expanding. And, if students have not developed critical thinking skills, are unsupervised, or create websites that are not monitored, they can be at risk of unknowingly communicating with predators, spammers, or pornographers.

As such sites proliferate, students should be warned not to post identifying information to the site and never to meet someone in person they have met through the site unless an adult accompanies them. And parents should conduct frequent reviews of the site to ensure that identifying information or pictures have not been posted.

Some social networking sites will cooperate in shutting down a site created solely to harass another individual.

Internet Safety

No action is foolproof, but there are steps students can take to protect themselves on-line and lessen the chance of becoming the victim of unsolicited messages:

- Never give out personal information, passwords, PIN numbers, etc.
- Remember that personal information includes your name, age, e-mail address, the names of family or friends, your home address, phone number (cell or home), or school name.
- Choose a user name that your friends will recognize but strangers will not recognize (such as a nickname used at school). This will help you to identify yourself to friends and lets you know who is trying to communicate with you.
- Do not submit or post pictures of yourself to any website, including your own. These can easily be copied and posted to any other website.
- Passwords are secret. Never tell anyone your password except your parents or guardians.
- Do not respond to "spam" or unsolicited e-mail.
- Set up e-mail and instant messenger accounts with your parents.
- Do not respond to, or engage in, cyber abuse.

If you are the victim of a cyberbully:

- Do not reply to messages from cyberbullies.
- Tell an adult you know and trust. Just as with any other kind of bullying, ignoring it often leads to escalation.
- If the bullying is occurring through text messaging, use "call display" or dial *69 to identify the phone number and have it tracked through your cell phone/pager service provider.
- Instant messages (e.g. Yahoo instant messenger; Microsoft Messenger) are best handled by blocking messages from certain senders.
- Bullies are likely to register for an anonymous e-mail account, such as Hotmail, Yahoo, or G-Mail, using a fake name. If you receive threatening e-mail messages, instruct your e-mail program to block messages from that address. Then, inform your Internet Service Provider (ISP).
- If physical threats are made or the bullying escalates, inform your local police.
- Do not erase or delete messages from cyberbullies. You do not have to read them; but keep them as evidence. You may get similar messages from other accounts. The police, your ISP, and/or your telephone company can use these messages to help you.
- If necessary, get a new phone number, account, or e-mail address and give it out to only one (1) person at a time.
- If the bullying occurs at school or on District property, or is the act of another student, report the bullying to the appropriate official and refer to the District's bullying policy.

Suggestions for Parents

- Make sure your children understand how vast and public the Internet is. Remind them that anything they post or send in a message is virtually available to be seen or read by anyone in the world.
- Talk to your children about cyberbullying. Make sure they understand what it is. Let them know that cyberbullying is no less serious and unacceptable than other forms of bullying.
- Set up the family computer (how do parents deal with iPad, cell phones and other devices which have data plans?) in an open, common area so that you can monitor what your child is sending and receiving. And or due diligence.
- Inform your ISP or cell phone service provider of any abuse. Although it can take a lot of time and effort to get Providers to respond and deal with your complaints about cyberbullying, it is necessary in order to try to stop it from reoccurring.
- Purchase software that can help track activity. There are parental controls that filter both IM and chat rooms.

Revised: November 2015
Issued: October 2014
Cross Reference: 2607 Student Discipline
Legal Reference: Children's Internet Protection Act (2001 Public Law 106-554)
47 United States Code 254(h)(5); 47 CFR 54.520
Protecting Children in the 21st Century Act, 15 United States Code § 6551