COMMUNICATION AND COMPUTER TECHNOLOGY EMPLOYEE BEHAVIOR & ACCEPTABLE USE POLICY 522.7

The District encourages educational use of all technology. It is the position of the School District of Phillips that use of the District's computer technology is a privilege afforded to employees who are expected to act on their good behavior and in full compliance with all rules and regulations of the District concerning the same. Correspondingly, misconduct shall result in disciplinary action to ensure the integrity of the system, to protect the District's investment in the system, and to ensure its continued availability to employees and the general student body of the District.

Internet and Computer Uses, Rules, and Guidelines
The School District of Phillips offers the privilege of Internet access. With this learning tool, employees must understand and practice proper and ethical use.

This document contains the Acceptable Use Policy for use of the Network and its associated components. The term "Network" is defined as all computer operations that are electronically sent to and out of an individual workstation or computer; this includes electronic mail. "Components" refers to any and all devices/materials used in technology, including computers, printers, scanners, cameras, data lines, software, etc. The term “employee” refers to anyone who is employed by the School District of Phillips. This policy also applies to all other users of the Network except students.

I. Educational Purpose

A. The Network has been established for appropriate educational purposes. The term "educational purpose" includes classroom activities and career development.

B. The Network has not been established as a public access service. The School District reserves the right to place restrictions on the material one may access or post through the system. Employees are expected to follow the rules set forth in this policy and under the laws of the State of Wisconsin and United States with respect to their use of the Network. The School District further reserves the right to amend these regulations, from time-to-time, in which event it shall so notify users of the system.

C. Employees may not use the Network for commercial purposes. This means employees may not offer, or provide products or services through the Network. Employees are not prohibited from using the Network to raise funds if both of the following conditions are met:

1) the employee represents a recognized entity of the District, and
2) the profits for said products or services return directly to the District.

D. Employees may not use the Network for political lobbying. Employees and/or classes may use the system to communicate with elected representatives, to express opinions on political issues, and to gather information related to governmental operations.

E. Certain Web 2.0 services, such as social networking sites, wikis, podcasts, RSS feeds and blogs that emphasize online educational collaboration and sharing among users, may be permitted by the District. However, such use must be approved by the Technology Coordinator or designee, followed by training authorized by the District, which will include application and responsible use training. Users must comply with this policy as well as any other relevant policies and rules during such use.

II. Student Internet Access

(Section II is included here so that employees have an understanding of the procedures students are required to follow while under the jurisdiction of an employee.)

A. High School students shall have access to Internet information resources through their classroom, library, or school computer lab only upon receipt of written parental approval and assuming the privilege has not been revoked. High School students shall have "on site" supervision. On site supervision means that a staff member is physically present in the room in which the Network is being accessed/utilized by a student.

B. High school students and their parents must sign an Acceptable Use Policy Agreement to be granted access to the Internet using the Network. The student's parents can withdraw their approval at any time. Withdrawal of parental consent shall cause a revocation of a student's Internet use privileges.

C. Elementary and middle school students shall have Internet access only under the "direct supervision" of their teachers. Direct supervision is defined as eye contact with student screen, either electronically or physically, by a staff member.

D. Student email (electronic mail) is not supported at this time. However, circumstances may arise where email for middle and secondary students may be provided for a limited time and for purely educational purposes as a result of a class project.

III. Misconduct and Unacceptable Use of Computers

The following uses of the Network and associated components are considered unacceptable and shall be considered as misconduct.

A. Placing Others at Risk

Employees shall not post personal contact information about other people. Personal contact information may include one's address, telephone, school address, work address, photos etc.

B. Illegal Activities

1) Employees shall not attempt to gain unauthorized access to the Network or to any other computer system through the Network or go beyond authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing."

2) Employees shall not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal.

3) Employees shall not use the Network to engage in any illegal act, such as arranging for a drug sale or the purchase of alcohol, participating in criminal gang activity, threatening the physical and/or emotional safety of another person, etc.

C. System Security

1) Employees are responsible for their personal account and should take all reasonable precautions to prevent others from being able to use that account. Under no conditions should one provide his/her password to another person.

2) Employees shall not break into or attempt to break into secure areas of the Network. This includes breaking into or attempting to break into the District's Network, or any other secured network, including Internet sites.

3) Employees shall immediately notify the system administrator if a possible security problem has been detected. Seeking out security problems/issues may be construed as an illegal attempt to gain access and may result in the loss of future use of the Network.

4) Employees shall avoid the inadvertent spread of computer viruses by following the District virus protection procedures.

5) Educational software has been installed for student and employee use. Only District personnel are to install software on workstations.

D. Inappropriate Language

1) Restrictions regarding inappropriate language apply to public messages, private messages (email), and material posted on Web pages.

2) Employees shall not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.

3) Employees shall not post information that could cause damage or a danger of disruption.

4) Employees shall not engage in personal attacks, including prejudicial or discriminatory attacks.

5) Employees shall not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If one is told by a person to stop sending him/her messages, one must stop.

6) Employees shall not knowingly or recklessly post false or defamatory information about a person or organization.

E. Dissemination of Personal Identification (Respect for Privacy)

1) Employees shall not repost a message that was sent privately without the permission of the person who sent the original message.

2) Employees shall not post private information about another person.

F. Plagiarism and Copyright Infringement

1) Employees shall not plagiarize works that are found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were one's own.

2) Employees shall respect the rights of copyright owners. Copyright infringement occurs when one inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies appropriate use of that work, one should follow the expressed requirements. If there is uncertainty whether or not one can use a work, permission should be requested from the copyright owner.

3) The District will put in place measures to maintain compliance with State Statute Section 943.70(2), the Federal Copyright Act and the “fair use doctrine”.

G. Respecting Resource Limits

1) Employees shall use the system only for appropriate educational and career development activities.

2) Employees shall not download large files unless absolutely necessary. If necessary, the data should be downloaded at a time when the system is not being heavily used. The file should immediately be removed from the system computer when finished. Storage capability is restricted.

3) Employees on the Network can expect to have individual storage capacity limited by the District in accord with the needs of the District and the amount of usage made of the system. The District reserves the right to, from time-to-time, change the amount of capacity allowed to individual users, in its sole discretion.

4) Employees may neither prevent others from accessing the system, nor unreasonably slow down the system.

H. Inappropriate Access to Material

Employees may encounter material which is controversial and which the users, parents, other employees or administrators may consider inappropriate or offensive. On a global network, it is impossible to effectively control the content of data. The School District of Phillips believes that the benefits from the Internet exceed the disadvantages. Nevertheless, employees are cautioned about accessing such data within the school system.

1) Employees shall not use the Network to access material that is profane or obscene (pornography), that advocates illegal acts, that advocates drug use, or that advocates violence or discrimination towards other people (hate literature). A special exception may be made to a particular employee if the purpose is to conduct research, and the supervisor has approved, in writing, such action prior to doing the research.

2) No inappropriate materials, as defined in the preceding paragraph, may be loaded onto School District workstations, the Network, or printed from school printers.

3) If one mistakenly accesses inappropriate information, one should immediately discard the file, or move to another Web site. This shall protect the employee against a claim that he/she has intentionally violated this Policy. If District personnel observe that a user has contacted such sites and information on more than one occasion, the employee shall be found in violation of this Policy and subject to potential discipline.

4) Failure to stop and/or failure to immediately turn the control of the computer over to district personnel for reviewing the history of one's Internet travels, or to view files, shall be declared as a deliberate attempt to cover up wrong doing.

I. Internet Filtering

1) The School District of Phillips employs hardware and software that is designed to filter and block inappropriate sites, and to a lesser degree, high-risk activities. The current filter will block sites that contain:
   a) Nudity - The absence of clothing or exposing any and all parts of the human genitalia. Exceptions include "classical " nudes and swimsuit models.
   b) Adult Content - Any material that has been publicly labeled as being strictly for adults.
   c) Sex - Description or depictions or all sexual acts and any erotic material.
   d) Violence - Graphic depictions of all graphically violent acts including murder, rape, torture and/or serious injury.
   e) Drug Use - Usage or encouraging usage of any recreational drugs, including tobacco and alcohol advertising. Exceptions include material with valid educational use, e.g., drug abuse statistics.
   f) Bad Language - Crude or vulgar language or gestures.
   g) Discrimination - Denigration of others' race, religion, gender, nationality, and/or sexual orientation.
   h) Crime - Encouragement of, tools for, or advice on carrying out universally criminal acts. This includes lock-picking, bomb-making, and hacking information.
   i) Tastelessness - Excretory functions, tasteless humor, graphic medical photos outside of medical context and some extreme forms of body modification, e.g., cutting, branding, genital piercing.
   j) Chat Sites - Online chatting creates a situation in which the activity cannot be monitored. It further places the student and employee at potential risk.
   k) High Risk Events - Sites which lack editorial control. Some of these may fall into one of the other blockable categories.
   l) Non-educational Sites - The District reserves the right to block other sites that do not support the goals of the Network, namely, the enhancement of classroom activities and career development. The District is further interested in preparing students for the work place. Therefore, sport and entertainment sites may also be blocked.
   m) Auction sites – Auction sites do not monitor for weapons, sexual items, or other illegal merchandise unsuitable for minors.

2) The employment of an Internet filter shall not diminish the user's personal responsibility for appropriate use of the Network. Filtering is not infallible.

J. Blocking Sites

1) The District reserves the right to block sites that do not enhance classroom activities and/or career development.

2) Employees are encouraged to contact the Technology Coordinator and/or the filtering vendor directly, should any one inadvertently access a site that is inappropriate for the school setting.

K. Removing the Filter

1) Removing a site/activity from the blocked list will require a high level of justification. Anyone wishing that removal will put the request in writing. The request will be given to the building administrator. The committee will review the site/activity in question. The committee shall be composed of the following:

a) Building Administrator
b) Director of Instructional Services
c) Technology Coordinator
d) An uninvolved staff member

2) The decision to remove the block on the site/activity will be based on the following criteria. Each of the criteria will be judged using contemporary community standards.

a) Does the educational value of the site/activity significantly outweigh the inappropriate nature of the site/activity?

b) Does the site/activity significantly enhance the curriculum?

c) Can the material/information be obtained from other more appropriate sources?

3) Employees will be notified of the approval or disapproval of the request in a timely manner. If the removal of the site/activity is granted, the committee will further indicate the length of time the block is to be removed.

L. Web Pages and Social Media

1) The District maintains a web server for the purpose of disseminating information about District events, highlighting educational activities, and serves as a resource for students, staff, and community.

2) Individuals whose names, photos, and the like, shall be incorporated into the Web page must give written authorization before such items can be used. (Minors must have a parent/guardian signature.) Businesses, organizations, etc. shall be granted the same right.

3) The Web page shall not violate any part of this Policy.

4) There shall be no links on the established Web page to sites that violate any part of this Policy.

5) The School District of Phillips' website will remain the district's primary internet presence. Content posted to the district's social media sites will also be available on the district's website and/or will include a link to the district's website.

6) The School District of Phillips recognizes the value of social media sites as a means of communication and education and authorizes the district use of such social media in accordance with established board policy to further the goals of the district.

7) All social media sites posted by district staff members will be subject to approval by the district administrator and the district's information technology director. The district reserves the right to restrict or remove any content that is deemed in violation of board policy or state law.

   - Visitors and users of district sponsored social media sites shall be notified that the intended purpose of the site is to serve as a form of communication between the district and the public.
   - Social media sites posted by district staff members will limit public interaction by restricting the public's involvement (ie. Limiting participation in social media sites to a "fan" type of status rather than a "friend" type of status).
   - Social media sites posted by district staff members will not permit others to identify any person included in photographs.

8) District and staff web pages, social media sites, articles and comments containing any of the following content will not be allowed:
   - Comments in support of or opposition to political campaigns or ballot measures

- Profane language or content
- Content that promotes, fosters, or perpetuates discrimination on the basis of factors including race, creed, religion, color, age, religion, sex, marital status, status with regard to public assistance, national origin, physical or mental disability or sexual orientation.
- Sexual content or links to sexual content
- Solicitation of commerce not related to authorized school district sponsored activities.
- Conduct or encouragement of illegal activity
- Information that may tend to compromise the safety or security of the district, district systems, students or staff
- Any other inappropriate materials written or otherwise

9) District social media sites are subject to the Wisconsin public records laws. The person or department responsible for creating/maintaining a site will ensure that content is available in an accessible format that is easily produced in response to a request for public records. Each site must state that all requests for public records must be directed to the district administrator.

10) Persons/departments responsible for creating/maintaining a site will preserve records in accordance with established district records retention schedules.

11) For each social media tool approved for use by the district, the following documentation will be developed, adopted, and distributed to staffs: (a) operational use guidelines, (b) standards and processes for managing accounts on social media sites, (c) district and departmental branding standards, (d) district-wide design standards, and (e) standards for the administration of social media sites.

M. Cyber Bullying

Any form of harassment using electronic devices, commonly known as “cyber bullying” by students, staff or third parties is prohibited and will not be tolerated in the District. “Cyber bullying” is the use of any electronic communication device to convey a message in any form (text, image, audio or video) that defames, intimidates, harasses or is otherwise intended to harm, insult or humiliate another in a deliberate, repeated or hostile and unwanted manner under a person’s true or false identity. In addition, any communication of this form which disrupts or prevents a safe and positive educational or working environment may also be considered cyber bullying.

N. Cyber Bullying Awareness and Response
Prior to receiving authorization to access district owned devices, computers, or networks; students, staff and/or third parties will be made aware of our

stance on cyber bullying by agreeing to the terms outlined in the communication and computer technology acceptable use policy.

Actions identified by district administration or its designee as cyber bullying will be handled in accordance with district policies, discipline procedures, and state law. Discipline can include verbal/written warning, suspension, expulsion, or referral to law enforcement.

O. Social networking training will include application and responsible use training. Users must comply with this policy as well as any other relevant policies and rules prior to obtaining authorization to use social networking sites.

IV. Hardware

A. CD's DVD's, Computers, and other Peripheral Devices

1) The District will not be responsible for loss or damage to personal items used on the District's network/computers. CD's, DVD's and any other peripheral devices are supplied by the District for student and staff use.

B. Printers

1) Employees are free to use District printers with some restrictions. The printing of excessive multiple copies shall not be tolerated. If District personnel make observations of what they deem, under the circumstances of use of the system by the particular user, to be the printing of excessive multiple copies, the user shall be subject to discipline.

Color printers are available within each District building. Employees wanting personal color prints shall be charged 25 cents per page. If color printing is required for a particular project, there shall be no charge.

V. Software

A. The District shall purchase and maintain the appropriate software licenses for all lab computers.

B. Staff computers have been configured with the software identified in the District's current technology plan. Any employee adding software to District owned computers needs to have a copy and the appropriate number of licenses for each computer on which the software is added.

VI. Consequences of Misuse

Depending upon the nature of the behavior and the results of that behavior, the employee may face serious consequences as a result of violations identified in the building staff handbook, and/or other appropriate Board Policy, and/or may be reported to local authorities.

VII. Electronic Mail

A. Cautions

Employees should be aware of the following:

1) Both the nature of electronic mail and the public nature of the School District's business make electronic mail less private than users may anticipate. For example, electronic mail intended for one person sometimes may be widely distributed because of the ease with which it can be forwarded to others by recipients. Furthermore, protections used to secure the integrity of electronic mail, such as system back-ups, may also compromise its privacy.

2) The School District cannot routinely protect users against such eventualities. Neither can the school district, in general, protect users from receiving electronic mail they may find offensive. Nevertheless, members of the School District community are strongly encouraged to use electronic communications with the same personal and professional courtesies and considerations they would use in other forms of communication.

3) There is no guarantee, unless "authenticated" mail systems are in use, that electronic mail received was in fact sent by the purported sender, since it is relatively easy for senders to disguise their identity. Furthermore, electronic mail that is forwarded may also be modified. Receivers of electronic mail documents should check with the purported sender if there is any doubt about the identity of the sender or the authenticity of the contents.

B. Ownership

1) An employee school email address is owned and provided by the School District of Phillips. Usage of such address constitutes a privilege afforded to an individual and is subject to withdrawal or revocation at any time by the District.

2) When an employee’s affiliation with the district is terminated, the School District shall terminate the employee’s email and associated accounts.

C. Personal Use

School District electronic mail services may, subject to the foregoing, be used for incidental personal purposes provided such use does not interfere with School District operation of information technologies or electronic mail services, burden the School District with incremental costs, or interfere with the user's employment or other obligations to the School District.

VIII. Your Rights

A. Free Speech

The School District of Phillips reserves the right to regulate student and employee speech disseminated under the auspices of the District, it being the mission of the District to inculcate community values. Thus, because student and employees use of the system is a component of the District curriculum and because the District desires to establish high standards for student and employee speech which is disseminated under its auspices, it reserves the right to regulate student and employee speech and to refuse to be associated with speech which is ungrammatical, poorly written, vulgar, profane or unsuitable for immature audiences. Subject to his/her reservation of rights in the School District and subject also to the exercise of free speech rights for purposes validly associated with an educational purpose and further subject to the building staff Handbook, and/or other appropriate Board policy, students and staff shall have the ability to exercise their rights of free speech in use of the system in the context of a limited public forum, which designation the District applies to the system.

B. Search and Seizure

All of the hardware and software associated with the School District computer system and access to and use of the Internet are the property of the School District of Phillips. At no time does the School District relinquish its exclusive control of any hardware or software provided for employee convenience. Periodic inspections of software, email addresses, input and output (including personal files) may be made by school authorities for any reason at any time without notice, without user consent and without a search warrant so as to ensure compliance of use with this policy and the building staff handbook and to protect system security and to make certain that use conforms with the law. In addition, routine maintenance and monitoring of the system may lead to discovery of violations of a user's responsibilities. Furthermore, a specific search may be made by school authorities of a user's input, output, email address, etc., if there is a reasonable suspicion that a particular user has violated this policy, the staff building handbook or the law.

C. Due Process

1) The District shall cooperate fully with local, state, and/or federal officials in any investigation related to any illegal activities conducted through the Network.

2) In the event there is a claim that an employee has violated this Policy, the building staff handbook, and/or other appropriate Board policy regarding the use of the Network, the employee shall be provided with a written notice of the suspected violation and given an opportunity to present an explanation before the building administrator.

3) The building administrator shall deem what is inappropriate and the decision is final.

4) As a result of one's actions, legal action may be taken.

IX. Limitation of Liability

The School District of Phillips makes no guarantee that the functions or the services provided by or through the District system shall be error-free or without defect. The District shall not be responsible for any damage one may suffer, including but not limited to, loss of data or interruptions of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the system. The District shall not be responsible for financial obligations arising through the unauthorized use of the system, nor shall the District be responsible for damage done to personal disks, software, CD's, etc., as a result of using District equipment.

X. Personal/Social Responsibility

A. If an employee has knowledge that someone is engaging in or has engaged in unauthorized behavior on a computer, associated components, or with the Network, the individual is required to immediately report the behavior to supervisory personnel. This can be an anonymous report. Failure to report the event/s is the same as contributing to the damaging behavior. As such, the employee shall be disciplined in the same manner as the original perpetrator.

B. When the District incurs a cost due to employee negligence or misuse, the employee shall be responsible for all costs associated with the repairs.

XI. Employee Use of System

All employees of the District who have access to and who use the Network shall obey all of the rules of this policy. Their failure or refusal to do so may result in

the imposition of the penalties, and/or in job related action which, depending upon the severity of the offense, may include but not limited to any form of discipline available to the District by contract or under the laws of Wisconsin.

Board Policy: 361.4 Communication and Computer Technology Student Behavior & Acceptable Use
411.1 Harassment: Bullying/Hazing
512 Employee Harassment: Bullying/Hazing

Approved: 07/21/97
Revised: 05/17/99
Revised: 05/15/00
Revised: 04/16/01
Revised: 12/21/09
Revised: 02/20/12