Communication and Computer Technology Student Behavior & Acceptable Use Policy 361.4

The District encourages educational use of all technology. It is the position of the School District of Phillips that the use of District computer technology is a privilege afforded to students 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 the staff and general student body of the District.

Internet and Computer Uses, Rules, and Guidelines

The School District of Phillips offers the privilege of Internet access for student use. With this learning tool, students must understand and practice proper and ethical use. Parents/guardians shall be notified annually that their child may be using School District resources and accounts to access the Internet.

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.

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. Students 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. Certain Web 2.0 services, such as social networking sites, wikis, podcasts, RSS feeds and blogs that emphasize on-line educational collaboration and sharing among users, may be permitted by the District under the supervision of an instructor. 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.

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

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

E. Individuals may not use the Network for political lobbying. Individuals 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.

II. Internet/Network Safety

The District's response to the Children's Internet Protection Act (CIPA), the Neighborhood Children's Internet Protection Act (N-CIPA) and the instructional curriculum for cyber bullying and safe use of social networking sites as required by the Broadband Data Improvement Act of October 2008 is recognized by identifying procedures to monitor access by minors to inappropriate matter on the Internet; identifying actions to promote safety and security of minors who use email, chat rooms and other forms of direct electronic communications; responding to unauthorized access, including "hacking", and other unlawful activities by minors online; preventing unauthorized disclosure, use, and dissemination of personal identification information regarding minors; and identifying measures designed to restrict access to materials harmful to minors.

A. Student Internet Access

   1. High School students shall have access to Internet information resources through their classroom, library, or school computer lab only upon receipt of written parental/guardian 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.

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

3. 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.

B. Safety and Security of Minors (Placing Self/Others at Risk)

1) Individuals shall not post personal contact information about him/herself or other people. Personal contact information may include one's address, telephone, school address, work address, photos, etc. Personal contact information may be posted for the purpose of filling out scholarship and college entrance forms, enrolling in on-line coursework and for career development activities, with approval from the building principal.

2) Individuals shall not agree to meet with someone contacted "on line" without parent/guardian approval. Parents/guardians are strongly encouraged to accompany students to such meetings.

C. Unauthorized Use/Illegal Activities

1) Individuals 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) Individuals shall not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means.

3) Individuals 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.

D. System Security

1) Individuals 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 passwords to another person.

2) Individuals 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) Students shall immediately notify a teacher, the librarian, or 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. Students are not to show other students the security problem.

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

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

E. Inappropriate Language

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

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

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

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

5) Individuals 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) Individuals shall not knowingly or recklessly post false or defamatory information about a person or organization.

F. Dissemination of Personal Identification (Respect for Privacy)

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

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

G. Respecting Network Resource Limits

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

2) Individuals 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) Servers are provided for the purpose of saving files.

4) Users on the Network can expect to have individual storage capacity limited by the District in accordance with the needs of the District and the amount of usage made of the system. The District reserves the right to change the amount of capacity allowed to individual users, in its sole discretion.

5) Users may neither prevent others from accessing the system, nor unreasonably slow down the system.

H. Inappropriate Access to Material by Adults or Minors

Users may encounter material which is controversial and which the users, parents/guardians, teachers, 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 to students from the Internet exceed the disadvantages. Nevertheless, students are cautioned about accessing such data within the school system.

1) Individuals 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 if the purpose is to conduct research, and both the teacher and parent/guardian have approved, in writing, such action prior to doing the research.

2) No inappropriate materials, as defined in the preceding paragraph, may be loaded onto 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 and report the incident to the supervisor/teacher. This shall protect the individual 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 individual 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.

5) Parents/guardians should instruct students if there is additional material they think would be inappropriate to access. The District fully expects that students shall follow parents'/guardians' instructions in this matter, as well as those of the District.

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 at potential risk.
k) High Risk Events - Sites which lack editorial control. Some of these may fall into one of the other blocked 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 Access to Sites

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

2) Staff and students 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 a 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) Individuals 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) Students shall not have access to the Web page password or the server on which the Web page resides.

6) 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.

7) 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.

8) 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.

9) 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

10) 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.

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

12) 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.

III. Plagiarism and Copyright Infringement

Individuals 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. The District may, on occasion, use an Internet service that is designed to check for plagiarism.

Individuals 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.

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”.

IV. Hardware

A. Staff Computers and Phones

All computers and phones, except those designated for student use, are off limits to students. Students are not to use a staff member's computer or phone without consent.

B. Food and Beverage:

Fluids, foods, and computers don't mix. Individuals are not to bring food, beverage or candy into the labs or next to workstations.

C. 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.

2) The playing of audio CD's/ DVD's for non-educational purposes is not permitted.

3) Students are prohibited from connecting their networkable, private (not school-owned) devices to the Network without consent of the building Principal and the Technology Coordinator. The exception to this rule is students are permitted to use flash drives. The same rules regarding down/uploading unauthorized data, programs or gaming programs through a flash drive is prohibited.

D. Printers

1) Students are free to use District printers for educational purposes. The printing of excessive multiple copies shall not be tolerated. Students must have teacher approval for printing large documents or large quantities of documents. If District personnel make observations of what they deem, under the circumstances, to be the printing of excessive multiple copies, the user shall be subject to discipline.

2) Students wanting personal black and white prints shall be charged 10 cents per page. Students wanting personal color prints shall be charged 25 cents per page. Teacher approval is necessary prior to printing such prints.

E. Physical Damage

Intentionally unplugging cables from computers, damaging mice or other peripherals, or engaging in other activities that can result in damage to equipment shall result in the loss of computer privileges.

F. Non-Supervised and Non-School Hours

Students are not to be in the labs using the equipment before and/or after school unless District personnel are present. Students are further instructed not to use any part of the Network without on site supervision by a faculty member. 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.

V. Consequences of Misuse

A. The failure or refusal to obey the directives of this policy shall result in the following progressive discipline action:

1) First Offense - loss of all computer use for 4 weeks
2) Second Offense - loss of all computer use for 9 weeks
3) Third Offense - loss of all computer use for one (1) calendar year

The School District of Phillips reserves the right to accelerate the progressive discipline or hand out more severe discipline on the basis of the seriousness and number of offenses with which a student has been charged and held to be in violation of this policy.

B. Students who lose computer privileges shall be held to the same degree and standard as other students. Assignment requirements, will not diminish because of a student's loss of computer use.

C. Depending upon the nature of the misconduct, the individual may face further consequences as a result of violations identified in the Student Handbook, and/or other appropriate Board Policy, and/or may be reported to local authorities.

VI. Computer Games

A. The playing of a computer game by students will only be supported if the activity meets all three (3) of the follow criteria:

1) The game must fit into the current classroom topic and it must enhance/support the goals and objectives of the curriculum.

2) The game is utilized under the supervision of an instructor and for a limited time.

3) There is an expectation expressed by the instructor that the students will gather one or more concepts from the activity.

B. Staff members are encouraged not to reward students with "computer time" that does not promote computers as educational, productive tools.

VII. Your Rights

A. Free Speech

The School District of Phillips reserves the right to regulate student speech disseminated under the auspices of the District. Thus, because student and staff use of the system is a component of the District curriculum and because the District desires to establish high standards for student speech which is disseminated under its auspices, it reserves the right to regulate student 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 Student Handbook, and/or other appropriate Board policy, students 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 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 District relinquish its exclusive control of any hardware or software provided for convenience of students and staff. 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 Student 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 Student 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 a student has violated this Policy, the Student Handbook, and/or other appropriate Board policy regarding the use of the Network, the individual shall be provided with a verbal and/or 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) If the violation also involves a violation of other provisions of the Student Handbook, and/or other appropriate Board Policy it shall be handled in a manner described therein. Additional restrictions may be placed on the use of an Internet account and/or Network.

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

VIII. 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 devices, software, CD's, etc., as a result of using District equipment.

IX. Personal/Social Responsibility

A. If an individual 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 school 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 individual shall be disciplined in the same manner as the original perpetrator. See Section V.

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

Board Policy: 522.7 Communication and Computer Technology 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: 05/19/03
Revised: 12/21/09
Revised: 02/20/12