

**Adopted: 9-03**

**Revised: 6-04, 8-09, 1-12**

**SUBJECT: Electronic Communications, Internet Safety & Acceptable Use Agreement**

All PPS electronic information resources are the property of the District and shall be used only in a manner that supports the educational mission. The District offers to its users these resources to enhance communications and better perform tasks associated with their positions and assignments. Users who have access to the District electronic resources shall adhere to the following guidelines:

**A. Password Privacy**

Users shall not reveal their passwords to others. If anyone has reason to believe that a password has been lost or stolen or that their e-mail has been accessed by someone without authorization, he/she shall contact the District Technology Department immediately. The use of passwords should not imply that users should have an expectation of privacy in the materials they create or receive on the computer.

**B. Deletion of Mail**

Messages should be read, filed and deleted in a timely manner. On occasion the system administrator may purge the system of old mail without notice. Unless directed to the contrary, users should discard inactive e-mail after sixty days except in those cases where retention may be required by law.

**C. No Expectation of Privacy**

The computer system belongs to the District and may only be used for District business. The computers and computer accounts given to users are to assist them in the performance of their assignments. Users should not have the expectation of privacy in anything they create, store, send or receive on the District's computer system.

**D. Waiver of Privacy Rights**

Users expressly waive any right of privacy in anything they create, send, store or receive on the computer or through the Internet or any other computer network. Users consent to allowing personnel of the District to access and review all materials users create, store, send and receive on the computer or through the Internet or any other computer network.

**E. No Privacy in Communications**

Users should never consider electronic communications to be either private or secure. E-mail could be potentially stored indefinitely on any number of computers, in addition to that of the recipient. It is possible that copies of messages may be forwarded to others either electronically or on paper. In addition, e-mail sent to non-existent or incorrect user names may be delivered to users never intended.

**F. Monitoring of Computer Usage**

The District has the right, but not the duty, to monitor any and all aspects of its computer systems, including, but not limited to, monitoring sites visited by users on the Internet, monitoring newsgroups and chatgroups, reviewing material downloaded or uploaded to the internet; and reviewing e-mail and voice mail sent and received by others.

**G. Automated Monitoring**

Users should understand that the District may use automated software to monitor material stored, created, sent or received on its computer systems.

## **H. Prohibited Uses**

- Users shall not use the District's system or computers to engage in "hacking," spreading computer viruses, or engage in any unlawful activity.
- Without prior written permission from the Superintendent, the District's computers and network system may not be used for dissemination or storage of commercial or personal advertisements, solicitations, promotions, destructive programs (viruses), or political material.
- Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, child pornographic, harmful to minors, or otherwise unlawful or inappropriate may not be sent by e-mail, voice mail, or other form of electronic communication or stored or displayed on the District's computers. Users encountering or receiving this kind of material should immediately report the incident to their supervisors.

## **I. Law Enforcement**

Users should be aware that the messaging systems (e-mail and voice mail) are the property of the District and as such, the District reserves the right to open user accounts that are suspected of violations of the District user agreement, local, state and national laws, or misuse. The District will also cooperate fully with law enforcement agencies that present proper warrants from a judge or magistrate. Users should assume that the District may and will monitor all information created in District-owned systems.

## **J. Posting of Personal Information**

Users of the District network shall not post names, addresses and/or pictures of anyone without written approval from that person or, if that person is under 18, written permission from his/her parent(s) or guardian(s). Forms for such permission must be filed with the Technology Department prior to any such information being posted. Any information posted about students shall be in compliance with the Family Educational Rights and Privacy Act of 1974.

**K. Chain Mail**

Users may not initiate or forward chain e-mail. Chain e-mail is a message sent to a number of people asking each recipient to send copies with the same request to a number of other users.

**L. Communicating Accurate Information**

Content of all communications should be accurate. Users should use the same care in drafting e-mail and other electronic documents as they would for any other written communication. Anything created on the computer may, and likely will, be reviewed by others.

**M. Online Behavior**

Users shall adhere to the District's behavioral standards when using District computers or the District's system, especially when interacting with other individuals on social networking sites or in chat rooms. Social networking sites and chat rooms shall only be used with prior approval of a teacher or administrator. Individuals shall show respect for other users and shall not engage in cyberbullying (online bullying). Anyone aware of cyberbullying shall immediately notify a teacher or administrator.

**N. Internet Filtering**

As per PPS Regulation #5430, internet access is to be filtered.

**O. Education**

It shall be the responsibility of all members of the Portage staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Director of Information and Technology Systems or designated representatives.

Portage Public Schools will provide age appropriate training for students who use the Internet facilities. The training provided will be designed to promote the commitment to:

- a. The standards and acceptable use of Internet services as set forth in this regulation
- b. Student safety with regard to:
  - i. safety on the Internet;
  - ii. appropriate behavior while on online, on social networking Web sites, and in chat rooms; and
  - iii. cyberbullying awareness and response.
- c. Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use policies.

**Acceptable Use Agreement  
PPSNet EDUCATIONAL NETWORK  
ACCEPTABLE USE AGREEMENT**

This agreement covers access to and the use of PPSNet and Internet Services through network connections.

Portage Public Schools Network (PPSNet) is offering staff and students in our school district accounts to access the educational network which is coordinated through a complex association of governmental agencies, regional and statewide networks. This document contains the terms and conditions of use that an employee and/or student agrees to follow when using PPSNet. This agreement may be modified by Portage Public Schools (PPS) at anytime with notice to the user.

**Terms and Conditions**

**Purpose and Acceptable Use**

1. PPS established the PPSNet for limited purpose. Use of any account must be in support of Education, research, and consistent with the educational and business objectives of PPS. The Superintendent of PPS and his/her designees may at any time make determinations that particular uses are or are not consistent with the purpose of PPSNet.

The term “educational purpose” includes classroom and work activities, career development activities to develop skills in technology and limited, high-quality, self-discovery activities.

2. PPSNet has **not** been established as a public access server or a public forum. PPS retains the right to place reasonable restrictions on the materials users access or post through PPSNet. In addition, users are expected to abide by the rules set forth in their school’s or district’s policies, and all applicable laws and regulations when using PPSNet.
3. Users may express opinions on political issues. However, PPS prohibits the use of PPSNet for political lobbying.
4. Users must respect the privacy of others; for example, users shall not intentionally seek information on, obtain copies of, or modify files, other than data, or passwords belonging to others, or represent themselves as another user unless explicitly authorized to do so by that user.
5. Users must respect the legal protection provided by copyright and license to programs and data.
6. Users must respect the integrity of computing and network systems; for example, users shall not intentionally develop or use programs that harass other users or infiltrate a computer, computing system or network and/or damage or alter the software components of a computer, computing system or network.

7. Users must monitor email on a regular basis (at least once a week) and delete mail from the personal mail directory to avoid excessive use of the file server hard disk system.
8. Users are responsible for maintaining the integrity of the electronic mail system, which includes reporting all violations of privacy to PPSNet. The user is responsible for making sure all email sent or received by him/her does not contain pornographic or indecent material, copyrighted material, inappropriate information or any other information which may be potentially threatening or dangerous to others in PPSNet.
9. Users who can identify a security problem on the PPSNet must notify the PPS Technology Department and not demonstrate the problem to others.
10. Web Pages. Refer to PPS Regulation 1114 Web Site Information and Images.

### **Unacceptable Use**

1. PPS prohibits the use of PPSNet for commercial or for-profit purposes. This means that users shall not offer, or provide products or services through PPSNet. Users may purchase personal products or services that are lawful. The user agrees to be fully responsible for any financial obligations arising from purchases via PPSNet. The user agrees to hereby release PPS, their personnel, and any institution affiliated with them from any and all liability arising out of, or in any way connected to, any purchase by the user including, but not limited to, purchase(s) made by user which are related to the official business of the user's educational institution, personal, or unauthorized purchases.
2. Use of obscene, profane, lewd, abusive, threatening, discriminatory or harassing language is prohibited on PPSNet. This prohibition applies to public messages, private messages, and material posted on web pages.
3. Users shall not engage in any unlawful activity over PPSNet.
4. PPS prohibits the use of PPSNet to access or post pornographic materials, indecent material, or inappropriate information. It is the users responsibility to insure that such material is not accessed or posted.
5. Users agree to not knowingly or recklessly post false or defamatory information about a person or organization.
6. Plagiarism and copyright infringement is prohibited. Users shall not take ideas or writings of others and present them as if they were their own. Also, users shall not inappropriately or illegally reproduce on PPSNet as a work protected by copyright. Respect the rights of copyright holders.

7. Users agree to not intentionally attempt to disrupt PPSNet or destroy data accessible through PPSNet by spreading computer viruses or by any other means.
8. Posting chain letters on PPSNet is prohibited.
9. Users shall not bombard other users with email messages or send annoying messages to other persons or organizations on PPSNet.
10. Users shall not forge (spoof) electronic mail messages or IP addresses.
11. PPSNet prohibits the sharing of user names and passwords. Users must not let anyone else use their user name or password.

### **Liability**

PPS makes no warranties or assurances of any kind, whether expressed and/or implied, for the service it is providing, including, but not limited to, loss of data resulting from delays, nondeliveries, mis-deliveries or service interruptions caused by PPS negligence or users' errors or omissions. PPS does not guarantee nor is in any way responsible for the accuracy or quality of information obtained through PPSNet. Use of any information obtained via PPSNet is at the user's own risk. PPS is not responsible for any damage users suffer, nor responsible for financial obligations arising from the unauthorized use of PPSNet to purchase personal product(s) or service(s) for his/her employer.

### **Rights and Violations**

1. Users should expect only limited privacy in the contents of personal files on PPSNet. PPS makes no guarantees of any kind, expressed or implied, regarding the privacy of electronic mail or any other telecommunications transmitted or received over PPSNet, a monitored telecommunications network. Routine maintenance and monitoring of PPSNet may lead to the discovery that a user has violated this agreement, policies of his/her educational institution and/or the law.
2. If there is reasonable suspicion that the user has violated this agreement, PPS policies or procedures, or the law, PPS will conduct a search of individual user files. This search and investigation will be reasonable and related to the suspected violation.
3. In the event there is a suspected violation of this agreement, PPS policies or procedures, or the law, the user will be provided with notice and an opportunity to be heard before the user's access is suspended or terminated. In addition, improper use of PPSNet may also lead to further disciplinary action consistent with the user's educational institution's policies and procedures.
4. A user's access to PPSNet may be suspended or terminated for a violation of this agreement. If the user's account privileges are terminated, PPS will not refund any use fee or portion thereof. Users shall not use PPSNet while access privileges are suspended or revoked.

**PORTAGE PUBLIC SCHOOLS  
PPSNet User Agreement**

**Student Signature Sheet**

I understand that I am responsible for materials accessed and acquired on the PPSNet, and I will abide by the PPSNet user Agreement. I further understand that any violation of the regulations is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, and disciplinary action, including legal referral, may be taken.

**Student First and Last Name** \_\_\_\_\_  
(Please Print)

**User Signature** \_\_\_\_\_  
(If you are under the age of 18, a parent or guardian must also read and sign this agreement.)

**Year of Graduation** \_\_\_\_\_

**School** \_\_\_\_\_

**Date** \_\_\_\_\_

**\*PARENT OR GUARDIAN**

As the parent or guardian of this student, I have read the PPSNet user Agreement. I understand that this access is designed for educational purposes. Portage Public Schools has taken precautions to eliminate controversial access. However, I also recognize it is impossible for Portage Public Schools to restrict access to all controversial materials, and I will not hold the District responsible for materials acquired on the network. Further, I accept full responsibility for my child's computer use while using District equipment, PPSNet. I hereby give permission to Portage Public Schools to issue an account for my child, and I certify that the information contained on this form is correct.

**Parent or Guardian Name** \_\_\_\_\_  
(Please Print)

**Parent or Guardian  
Signature** \_\_\_\_\_

**COMPUTER USE & INTERNET ACCESS**

**“OPTING OUT” PROCEDURE**

**PARENT FORM FOR REQUESTING TO HAVE THEIR CHILD (or CHILDREN)  
EXCLUDED FROM USING THE DISTRICTS COMPUTERS AND/OR EXCLUDED  
FROM USING THE INTERNET**

Portage Public Schools believes that the use of technology is an important and integral part of each child’s education. A technologically enriched environment is provided for students in our District. Students will have access to video and computer systems that can and will connect them to electronic informational resources in our District and around the world.

The integration of technology into the curriculum is an on going process and is continually evolving in our District. Students will have regularly scheduled times when computers are available for them to use. These computers are typically connected to the District’s internal network as well as to the Internet. The information flowing into our District from the Internet is **filtered** in order to exclude inappropriate content. Student computers are restricted to this **filtered** content from the Internet.

As a parent, you may exclude your child from having computer access and/or Internet access by completing the form below and submitting it to your child’s building principal. Please note that this “Opting-Out” procedure must be completed each year for each child.

I wish to exclude: \_\_\_\_\_ (child’s name) from using **computers**.

I wish to exclude: \_\_\_\_\_ (child’s name) from using the **Internet**.

Parent Signature: \_\_\_\_\_

Parent Signature: \_\_\_\_\_

Date: \_\_\_\_\_

School: \_\_\_\_\_

---

(Office use only) Date submitted to Network Administrator: \_\_\_\_\_