# SECTION 720 INTERNET SAFETY AND ACCEPTABLE USE POLICY

Computer networks, including the Internet, offer vast, diverse, and unique resources to both students and teachers. The District's goal in providing these services to all staff and students is to promote learning by facilitating resource sharing, innovation, and communication. Internet use, with staff supervision, has become a key component of school curriculum as we integrate technology use with all our subjects. Network access is intended and designed for educational purposes and governed by the terms and conditions outlined in this policy.

In compliance with the Children's Internet Protection Act (CIPA), the District filters Internet access on all devices capable of accessing the Internet. The District recognizes, however, that no technology measure can block 100 percent of the undesirable content, and emphasizes the importance of staff supervision in monitoring student use.

The smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines. The guidelines are provided below. In general this requires efficient, ethical and legal utilization of the network resources for academic purposes only. As students and staff use this network, it is essential that each user on the network recognize his or her responsibility in having access to the vast services, sites, and people. The user is ultimately responsible for his or her actions in accessing network services and for adhering to District access policies, other District policies that may apply, and building discipline procedures. If a Portage School District user violates these provisions, his or her account will be terminated and future access will be limited or denied.

## Privileges

The network hardware and software is the property of the Portage Community School District. The use of the network is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges.

## Acceptable Use

The use of an account must be consistent with the educational objectives of the Portage School District and any objectives assigned by staff for assignments or projects. Use of other organization's network or computing resources must comply with the rules appropriate for that network. Transmission of any material in violation of any United State or state regulation is prohibited. This includes, but is not limited to copyrighted material, threatening or obscene material, or material protected by trade secret. Use for commercial activity is prohibited. Use for product advertisement or political lobbying is also prohibited.

## Network Etiquette

Users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to the following:

1. Use appropriate language. Do not swear, use vulgarities or any other abusive language.
2. Do not reveal your full name, address or phone number without your teacher's permission.
3. Do not share your password and do not use others accounts.
4. Note that electronic mail is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
5. Do not use the network to harm or harass others. This includes sending unwanted e-mail or chain e-mail messages.

6. Do not use the network in such a way that would disrupt the use of the network by others, e.g. downloading excessively large files.
7. Do not download executable files, install programs, or change settings on the school computers without permission.
8. All communications and information accessible via the network are school property and are not private. Network operators do have access to all files.

Disclaimer

Portage Community Schools make no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or user's errors or omissions. The School District of Portage specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Security

Security on any computer system is a high priority, especially when the system involves many users. Users must notify the teacher or Library Media Specialist of security problems. Users should not demonstrate the problem to other users. Users shall not intentionally seek information on, obtain copies of, or modify files, or other data, or passwords belonging to other users, or misrepresent other users on the network. Attempts to log in as a systems administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems will be denied access to the District's network.

Vandalism/Harassment

Vandalism or harassment will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy hardware, software, and wiring, as well as the data of another user. This includes, but is not limited to, the uploading or creating of computer viruses. Harassment is defined as the persistent annoyance of another user, or the interference of another user's work. Harassment includes, but is not limited to, the sending of unwanted mail.

Penalties/Consequences

Disciplinary action will be determined according to the disciplinary policies of the teacher, the school, the Student Code of Conduct, and Portage Community School's School Board Policies. The disciplinary process may include combinations of the following consequences.

1. Warning
2. Loss of credit for the assignment
3. Loss of credit for the unit
4. Loss of privilege to use the network
5. Loss of privilege to use any computer
6. Referral to administration
7. Referral to law enforcement officials

PORTAGE COMMUNITY SCHOOL DISTRICT

**Internet Restriction Form**

Computer networks, including the Internet, offer vast, diverse, and unique resources to both students and teachers. The District's goal in providing these services to all students is to promote learning by facilitating resource sharing, innovation, and communication. Internet use, with staff supervision, has become a key component of school curriculum as we integrate technology use with all our subjects. Network access is intended and designed for educational purposes and governed by the terms and conditions outlined in the District's Internet Safety and Acceptable Use Policy #720, which is available in each building office and on the District Web Page.

In compliance with the Children's Internet Protect Act (CIPA), the District filters Internet access on all devices capable of accessing the Internet. The District recognizes, however, that no technology measure can block 100 percent of the undesirable content, and emphasizes the importance of staff supervision in monitoring student use.

Student access to technology resources is a privilege, not a right. The privilege may be revoked at any time for use not consistent with the educational goals of the district. General school rules for communication and behavior apply to the use of technology services, including confidentiality, bullying, and harassment.

If any parent/guardian objects to or refuses to permit the District to provide Internet access, they should annually submit this form to the building principal. An account that allows access to the school networked computers and installed software, but restricts access to the Internet, will be provided.

THE SIGNATURE BELOW CERTIFIES THAT INTERNET ACCESS SHOULD BE RESTRICTED FOR THE CURRENT SCHOOL YEAR FROM THE ACCOUNTS FOR THE STUDENT(S) LISTED BELOW.

Student(s) to be restricted from Internet access:

| Student Name | Grade | School |
|---|---|---|
| | | |
| | | |
| | | |

Parent or Guardian's Name (please print):_____

Signature_____Date_____

# Improper Technology Use

Name_____ Gr._____ Hour/Block._____

**Technology Violation**

_____1. Shared password
_____2. Used another's password
_____3. Vandalism
- Attempt to harm or destroy hardware
- Attempt to harm or destroy software
- Attempt to harm or destroy another's file
- Uploading or creating of computer viruses
- Inappropriate downloading

_____4. Harassment
- Persistent annoyance of another user
- Interference of another user's work
- Sending of unwanted communication

_____5. Not consistent with the educational use of the network (including Copyright infringement, non-permissible web browsing)
_____6. Severe Infraction
- ♦ Theft
- ♦ Hacking
- ♦ Any illegal activities

**Describe or attach copy**

_____

_____

Signature of staff member _____Date_____

**Consequence for above behavior**

**Type of loss**
- ☐ *Email use*
- ☐ *Internet use*
- ☐ *Network login*
- ☐ *All technology access*

**Status**
- ☐ *First Offense*
- ☐ *Second Offense*
- ☐ *Third Offense/Severe*

**Length of loss**
- ☐ *2 wks*
- ☐ *4 wks*
- ☐ *End of Term/Quarter*
- ☐ *End of Semester*
- ☐ *End of Year*
- ☐ *Other:*_____

Signature of Administrator_____ Date_____

***Please return copy to the tech. ctr. and staff member***