

POLAND REGIONAL HIGH SCHOOL COMMITTEE	CODE: IJNDB Page: 1
SUBJECT: STUDENT AND STAFF COMPUTER AND INTERNET USE AND RULES	
DATE OF ORIGINAL POLICY: February 2006 REVISION DATE:	
JURISDICTION: Poland Regional High School	

POLICY:

The school unit provides computers, networks and Internet access to support the educational mission of the schools and to enhance the curriculum and learning opportunities for students and school staff. The Poland Regional High School Committee believes that the resources available through the Internet are of significant value in the learning process and preparing students for future success. At the same time, the unregulated availability of information and communication on the Internet requires that schools establish reasonable controls for lawful, efficient and appropriate use of this technology.

Student and staff use of school computers, networks and Internet services is a privilege not a right. All users are required to comply with this policy and these rules. Users who violate the policy and/or rules may have their computer privileges revoked and may also be subject to further disciplinary and/or legal action.

All school unit computers remain under the control, custody and supervision of the school unit. The school unit reserves the right to monitor all computer and Internet activity by users. Users have no expectation of privacy in their use of school computers.

While reasonable precautions will be taken to supervise student use of the Internet, the school unit cannot reasonably prevent all inappropriate uses, including access to objectionable materials and communication with persons outside of the school, in violation of Poland Regional High School Committee policies/procedures and school rules. The school unit is not responsible for the accuracy or quality of information that students obtain through the Internet.

Before a student or staff member is allowed to use school computers and Internet services (including email), they must sign and return the Computer/Internet Access Acknowledgment (IJNDB-E). Both the student and the student's parent/guardian shall sign the form. The signed acknowledgment will be retained by the school.

The Superintendent/designee shall be responsible for overseeing the implementation of this policy and these rules and for advising the Poland Regional High School Committee of the need for any future amendments or revisions to the policy/rules. The Superintendent/designee may develop additional administrative procedures/rules governing the day-to-day management and operations of the school unit's computer system as long as they are consistent with the Poland Regional High School Committee's policy/rules. The Superintendent/designee may delegate specific responsibilities to building principals and others as he/she deems appropriate.

SUBJECT: STUDENT AND STAFF COMPUTER AND INTERNET USE AND RULES

RULES:

These rules are intended to provide general guidelines and examples of prohibited uses but do not attempt to state all required or prohibited activities by users. Failure to comply with this policy and these rules may result in loss of computer and Internet access privileges, disciplinary action and/or legal action.

A. Computer Use is a Privilege, Not a Right

Student use of the school unit's computers, networks and Internet services is a privilege, not a right. Unacceptable use/activity may result in suspension or cancellation of privileges, as well as additional disciplinary and/or legal action.

The building principal shall have final authority to decide whether a student's privileges will be denied or revoked.

B. Acceptable Use

Student access to the school unit's computers, networks and Internet services are provided for educational purposes and research consistent with the school unit's educational mission, curriculum and instructional goals.

The same rules and expectations govern student use of computers as apply to other student conduct and communications.

Students are further expected to comply with these rules and all specific instructions from the teacher or other supervising staff member/volunteer when accessing the school unit's computers, networks and Internet services.

C. Prohibited Use

The user is responsible for his/her actions and activities involving school unit computers, networks and Internet services and for his/her computer files, passwords and accounts. Examples of unacceptable uses that are expressly prohibited include but are not limited to the following:

1. **Accessing Inappropriate Materials** – Accessing, submitting, posting, publishing, forwarding, downloading, scanning or displaying materials that are defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing and/or illegal;
2. **Illegal Activities** – Using the school unit's computers, networks and Internet services for any illegal activity or activity that violates other Poland Regional High School Committee policies, procedures and/or school rules;

SUBJECT: STUDENT AND STAFF COMPUTER AND INTERNET USE AND RULES

3. **Violating Copyrights** – Copying or downloading copyrighted materials without the owner’s permission;
 4. **Plagiarism** – Representing as one’s own work any materials obtained on the Internet (such as term papers, articles, etc.). When Internet sources are used in student work, the author, publisher and Website must be identified;
 5. **Copying Software** – Copying or downloading software without the express authorization of the system administrator;
 6. **Non-School-Related Uses** – Using the school unit’s computers, networks and Internet services for non-school-related purposes such as private/personal financial gain, commercial, advertising or solicitation purposes, assisting a campaign for election, or the promotion or opposition to any ballot initiative. School computers may be used for limited and reasonable personal email communications which do not interfere with uses that support the mission of the schools, nor violate other provisions of this policy;
 7. **Misuse of Passwords/Unauthorized Access** – Sharing passwords, using other users’ passwords without permission and/or accessing other users’ accounts; Passwords must remain private and not be shared with others. Policy violation traced to users passwords will become the responsibility of the owner of the password.
 8. **Malicious Use/Vandalism** – Any malicious use, disruption or harm to the school unit’s computers, networks and Internet services, including but not limited to hacking activities and creation/uploading of computer viruses; and
 9. **Unauthorized Access to Chat Rooms/News Groups** – Accessing chat rooms or news groups without specific authorization from the supervising teacher.
 10. Poland computers, computer networks and electronic mail shall not be used to share confidential information on students or staff including attached files.
- D. **No Expectation of Privacy**
The school unit retains control, custody and supervision of all computers, networks and Internet services owned or leased by the school unit. The school unit reserves the right to monitor and/or review all computer and Internet activity by network users at the request of the principal or superintendent or incidentally as part of routine computer and network maintenance and administration... Users have no expectations of privacy in their use of school computers, including e-mail and stored files. Violations of this policy that are discovered by I. T. staff, either by administration request or incidentally, are required to be reported to the building principal and/or the superintendent.

SUBJECT: STUDENT AND STAFF COMPUTER AND INTERNET USE AND RULES

- E. **Compensation for Losses, Costs and/or Damages**
The student and/or the student's parent/guardian shall be responsible for compensating the school unit for any losses, costs or damages incurred by the school unit related to violations of this policy and/or these rules, including investigation of violations.
- F. **School Unit Assumes No Responsibility for Unauthorized Charges, Costs or Illegal Use**
The school unit assumes no responsibility for any unauthorized charges made by students including but not limited to credit card charges, long distance telephone charges, equipment and line costs, or for any illegal use of its computers such as copyright violations.
- G. **Student Security**
A student shall not reveal his/her full name, address or telephone number on the Internet without prior permission from a supervising teacher. Students must never meet people they have contacted through the Internet without parental permission. Students must inform their supervising teacher if they access information or messages that are dangerous, inappropriate or make them uncomfortable in any way.
- H. **System Security**
The security of the school unit's computers, networks and Internet services is a high priority. Any user who identifies a security problem must notify the system administrator immediately. The user shall not demonstrate the problem to others. Any user who attempts or causes a breach of system security shall have his/her privileges revoked and may be subject to additional disciplinary and/or legal action.
- I. **Parental Permission Required**
Students and their parent/guardian are required to sign and return the Computer/Internet Access Acknowledgment Form (IJNDB-E) before being allowed to use school computers.
- J. All administration, faculty and staff members who use school computers are required to sign and return the Computer/Internet Acknowledgment Form (IJNDB-E) before using school computers.

Cross Reference: IJNDB-E – Student Computer/Internet Use Acknowledgement Form

