Instruction

Acceptable Use of Computer Network for Students

The Internet is a powerful global information infrastructure used by private individuals, businesses, organizations, educators and governments. In school, the Internet can serve as a valuable educational resource. The Putnam Board of Education provides computers, networks and Internet access to support the educational mission of the schools and to enhance the curriculum and learning opportunities for students.

Student access to the District's computers and Internet service is provided for educational purposes, consistent with the District's educational mission, curriculum and instructional goals only. Students may use computers for personal use that is consistent with the school district's mission of developing lifelong learners. Any student who violates this policy will be subject to appropriate disciplinary action, up to and including expulsion. Improper use may also be reported to law enforcement officials, as appropriate.

The Putnam Board of Education is aware that the Internet is essentially an unregulated communication environment within which information changes constantly, and which contains information that is inappropriate for some users based upon factors such as age and developmental level. The Board seeks to provide students with the understanding and skills needed to use the Internet in an appropriate and responsible manner that is conducive to learning.

Prohibited Use

Each student must take responsibility for his or her actions and activities in using the District's computers and Internet service, and must cooperate with teachers and staff in promoting responsible use . Inappropriate and/or irresponsible use is prohibited, including but not limited to, the following:

1. Any use that is illegal or in violation of any of the District's policies, rules or regulations, including but not limited to, harassing, discriminatory, or threatening communications and violation of copyright laws.

2. Any use involving inappropriate materials and/or inappropriate communications, including but not limited to materials and/or communications that are obscene, pornographic, sexually explicit or sexually suggestive.

3. Any use for personal or commercial financial gain or political lobbying.

4. Any use involving harassment, hate mail, discrimination, or other offensive communications.

5. Any use for the purpose of improperly infiltrating and/or damaging a software program or computer system, or for the purpose of improperly obtaining or modifying files, passwords or data.

Instruction

Acceptable Use of Computer Network for Students (continued)

6. Any use for the purpose of misrepresenting the District or others.

7. Misuse of passwords or accounts.

8. Misuse or damage to computer equipment or software.

9. Any use of pseudonyms, impersonations or anonymity. Each student must remain accountable for his or her use at all times.

10. Any use of unauthorized games, programs, files or other electronic media.

11. Any use involving plagiarism or the improper downloading or purchasing of materials, including, but not limited to, research papers or essays, in order to complete assignments.

Security

The security of the Districts computer systems must be preserved by all student users. Each student is responsible for the use of their account. Passwords should not be shared. Students must take care to avoid degrading the performance of the network. Students must avoid the spread of computer viruses. Intentional or deliberate spread of computer viruses will be grounds for disciplinary action, up to and including expulsion. Any student who becomes aware of a potential security problem must immediately notify the appropriate teacher or other staff member.

Network Etiquette

Students are expected to use the District computers and Internet service in a mature and responsible manner. Students should never engage in inappropriate behavior while using the Districts computers and in so doing, will be subject to disciplinary action up to and including expulsion. Inappropriate behavior includes, but is not limited to, the following:

1. Sending impolite communications.
2. Sending abusive or threatening communications.
3. Using inappropriate, offensive or obscene language.
4. Revealing names, addresses or other personal information of others without proper authorization.

Safety

The District will seek to protect student users from inappropriate communications and/or materials on the Internet, to the extent reasonably possible. Any student user who receives inappropriate communications on a school computer, including but not limited to, threatening remarks or offensive or obscene materials, must immediately notify the appropriate teacher or other staff member so that appropriate action may be taken.

Instruction

Acceptable Use of Computer Network for Students (continued)

Privacy

Network and Internet access is provided as a tool for your education. The school district reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the school district and no user shall have any expectation of privacy regarding such materials.

Warranties/Indemnification

The school district makes no warranties of any kind, either express or implied, in connection with its provision of access to and use of its computer networks and the Internet provided under this policy. It shall not be responsible for any claims, losses, damages, or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any user or his or her parent(s) or guardian(s) arising out of the user's use of its computer networks or the Internet under this policy. By signing this policy, users are taking full responsibility for his or her use, and the user who is 18 or older or, in the case of a user under 18, the parent(s) or guardian(s) are agreeing to indemnify and hold the school, the school district, the Data Acquisition Site that provides the computer and Internet access opportunity to the school district and all of their administrators, teachers, and staff harmless from any and all loss, costs, claims, or damages resulting from the user's access to its computer network and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The user or, if the user is a minor, the user's parent(s) or guardian(s) agree to cooperate with the school in the event of the school's initiating an investigation of a user's use of his or her access to its computer network and the Internet, whether that use is on a school computer or on another computer outside the school district's network.

Legal Reference: Connecticut General Statutes
53a-182b. Harassment in the first degree: Class D felony. (as amended by PA 95-143)
20 U.S.C. Section 6777, No Child Left Behind Act
20 U.S.C. 254 Children's Internet Protection Act of 2000
47 U.S.C. Children's Online Protection Act of 1998

Policy adopted: January 17, 2012

PUTNAM PUBLIC SCHOOLS
Putnam, Connecticut

Instruction

Internet Acceptable Use: Filtering

Acceptable Use of Electronic Networks

All use of electronic networks shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. These procedures do not attempt to state all required or prescribed behavior by users. However, some specific examples are provided. The failure of any user to follow these procedures will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

Terms and Conditions

1. **Acceptable Use** - Access to the District's electronic networks must be (a) for the purpose of education or research, and be consistent with the educational objectives of the District, or (b) for legitimate business use.

2. **Privileges** - The use of the District's electronic networks is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The system administrator will make all decisions regarding whether or not a user has violated these procedures and may deny, revoke, or suspend access at any time; his or her decision is final.

3. **Unacceptable Use** - The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:

    a. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or State law;

    b. Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused;

    c. Downloading copyrighted material for other than personal use;

    d. Using the network for private financial or commercial gain;

    e. Wastefully using resources, such as file space;

    f. Hacking or gaining unauthorized access to files, resources, or entities;

    g. Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature;

    h. Using another user's account or password;

    i. Posting material authorized or created by another without his/her consent;

    j. Posting anonymous messages;

Instruction

Internet Acceptable Use: Filtering

Acceptable Use of Electronic Networks

Terms and Conditions (continued)

k. Using the network for commercial or private advertising;

l. Accessing, submitting, posting, publishing, or displaying a defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and

m. Using the network while access privileges are suspended or revoked.

4. Network Etiquette - The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

a. Be polite. Do not become abusive in messages to others.

b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.

c. Do not reveal personal information, including the addresses or telephone numbers, of students or colleagues.

d. Recognize that electronic mail (E-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.

e. Do not use the network in any way that would disrupt its use by other users.

f. Consider all communications and information accessible via the network to be private property.

5. No Warranties - The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

6. Indemnification - The user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any violation of these procedures.

Instruction

Internet Acceptable Use: Filtering

Acceptable Use of Electronic Networks

Terms and Conditions (continued)

7. Security - Network security is a high priority. If the user can identify a security problem on the Internet, the user must notify the system administrator or Building Principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account without written permission from that individual. Attempts to log-on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

8. Vandalism - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

9. Telephone Charges - The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.

10. Copyright Web Publishing Rules - Copyright law and District policy prohibit the republishing of text or graphics found on the Web or on District Web sites or file servers without explicit written permission.

a. For each republication (on a Web site or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the Web address of the original source.

b. Students and staff engaged in producing Web pages must provide library media specialists with e-mail or hard copy permissions before the Web pages are published. Printed evidence of the status of "public domain" documents must be provided.

c. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the Web site displaying the material may not be considered a source of permission.

d. The "fair use" rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.

e. Student work may only be published if there is written permission from both the parent/guardian and student.

Instruction

Internet Acceptable Use: Filtering

Acceptable Use of Electronic Networks

Terms and Conditions (continued)

11. Use of Electronic Mail

a. The District's electronic mail system, and its constituent software, hardware, and data files, are owned and controlled by the School District. The School District provides e-mail to aid students and staff members in fulfilling their duties and responsibilities, and as an education tool.

b. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student or staff member to an electronic mail account is strictly prohibited.

c. Each person should use the same degree of care in drafting an electronic mail message as would be put into a written memorandum or document. Nothing should be transmitted in an e-mail message that would be inappropriate in a letter or memorandum.

d. Electronic messages transmitted via the School District's Internet gateway carry with them an identification of the user's Internet "domain." This domain name is a registered domain name and identifies the author as being with the School District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of this School District. Users will be held personally responsible for the content of any and all electronic mail messages transmitted to external recipients.

e. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.

f. Use of the School District's electronic mail system constitutes consent to these regulations.

Internet Safety

1. Internet access is limited to only those "acceptable uses" as detailed in these procedures. Internet safety is almost assured if users will not engage in "unacceptable uses," as detailed in these procedures, and otherwise follow these procedures.

Instruction

Internet Acceptable Use: Filtering

Acceptable Use of Electronic Networks

Internet Safety (continued)

2. Staff members shall supervise students while students are using District Internet access to ensure that the students abide by the Terms and Conditions for Internet Access contained in these procedures.

3. Each District computer with Internet access has a filtering device that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee.

4. The system administrator and Building Principals shall monitor student Internet access.

Legal Reference: Children's Internet Protection Act, P.L. 106-554.
20 U.S.C § 6801 et seg.
47 U.S.C. § 254(h) and (1).
720ILCS 135/0.01.

Regulation approved: January 17, 2012

PUTNAM PUBLIC SCHOOLS
Putnam, Connecticut