

COMPUTER NETWORK AND INTERNET ACCEPTABLE USE POLICY FOR STUDENTS

The Pickerington Local School District (the "District") is pleased to make available to each student access to interconnected computer systems, computer equipment, computer programs, electronic mail, the world-wide network known as the Internet, and other technologies (collectively, the "Network"). By giving users access to this Network, the District does not intend to create a limited or a public forum for the expression of opinion. The Network exists as part of the function of the governmental mission of the District, and is operated solely in support of that mission. Neither the public, nor staff, nor students are invited to use the Network in expression of their opinions. The District fully supports the right of all students, staff, and citizens to express their opinions through legitimately established public and limited forums dedicated to that use.

In order for the District to be able to continue to make Network access available, each student must take responsibility for appropriate and lawful use of this access. Students are responsible for good behavior on the Network just as they are in a classroom, school hallway or other District property. While the District's teachers and other staff may make reasonable efforts to supervise student use of Network access, the ultimate responsibility for exercising and promoting responsible use of this access is that of the student and the parent/guardian.

This document shall constitute the District's Computer Network and Internet Acceptable Use Policy for Students ("Policy"). Any parent/guardian of a student under the age of 18 may direct that the student not be given access to the Network. An "opt out" form for this purpose may be obtained from the School District.

Each student is responsible for reading and abiding by this Policy. If you have any questions about the provisions of this Policy, you should contact the Principal or other designated administrator in your school building. Any use of your account that violates this Policy may result in your access being withdrawn and/or additional disciplinary action. You and your parent/guardian should be familiar with the Student Discipline Code, Board Policy JFC, et seq. (the "Student Discipline Code"). Violations of this Policy are considered violations of the Student Discipline Code and may result in disciplinary action as specified therein.

Purpose and Use

The District is providing you access to its Network only for educational purposes. If you have any doubt about whether a contemplated activity is educational, you may consult with the Principal or other designated person in your school building.

Reporting Misuse of the Network

In addition to following the terms of this Policy, you should report any misuse of the Network to a teacher or school administrator. Misuse means any violations of this Policy or any other use that is not included in this Policy but has the intent or effect of harming another or another's property.

Term of the Permitted Use

Access to the Network is a privilege, not a right, and as such it may be suspended or revoked by the District at any time for technical, policy or other reasons. The District may also limit access depending on student and staff schedules and equipment availability.

Access

Network resources are only intended for use by authorized users. Anonymous use is not permitted, and access may not be shared or transferred. Students shall not share their passwords or otherwise allow anyone to gain unauthorized access to the Network. A student is subject to disciplinary action under the Student Disciplinary Code for any violations of this Policy committed by someone else who, with the student's express or implied permission, accessed the Network with the student's password.

Unacceptable Uses

Students should not use the School District's Network for activities that cause harm to others or damage to their property; or that violate the law, Board policy, or the Student Discipline Code. The Board or authorized District officials will make a good faith judgment as to which materials, files, information, software, communications and other content and activities are permitted and prohibited under the particular circumstances based on the following guidelines. Uses and activities that are considered unacceptable and constitute a violation of this Policy include, but are not limited to, the following:

1. **Illegal Activities** – Any use that is illegal or which violates other Board policies, procedures or school rules, including harassing, intimidating, abusive, defamatory, discriminatory or threatening communications and behavior; violations of copyright laws, etc. The District assumes no responsibility for illegal activities of students while using school computers, or while using privately-owned computers on school property.
2. **Accessing Inappropriate Materials** – Accessing, submitting, posting, publishing, forwarding, downloading, scanning, or displaying materials that are obscene, pornographic, sexually explicit or sexually suggestive.

3. Inappropriate or Insensitive Communication – Making ethnic, religious, sexual preference or gender-related slurs or jokes.
4. Violating Copyrights – Copying, downloading or sharing any type of copyrighted materials (including music or films) outside the scope of fair use without the owner’s permission. The District assumes no responsibility for copyright violations by students.
5. Copying Software – Copying or downloading software without the express authorization of the Director of Technology. Unauthorized copying of software is illegal and may subject the copier to substantial civil and criminal penalties. The District assumes no responsibility for illegal software copying by students.
6. Plagiarism – Representing as one’s own work any materials obtained on the Internet (such as term papers, articles, music, etc.). When Internet sources are used in student work, the author, publisher and web site must be identified.
7. Non-school-related Uses – Using the District’s Network for non-school-related purposes such as private financial gain; commercial, advertising or solicitation purposes; or any other personal use not connected with the educational program or assignments.
8. Misuse of Passwords/Unauthorized Access – Sharing passwords, using other users’ passwords, and accessing or using other users’ accounts.
9. Malicious Use/Vandalism – Any malicious use, disruption or harm to the District’s Network, including but not limited to hacking activities and creation/uploading of computer viruses.
10. Unauthorized Access to websites, Social Networking sites, etc. – Using web proxies or other means to circumvent school Internet filters in order to access websites, blogs, social networking sites, or other pages that are blocked by the District’s Internet filtering technology.

Use of Privately-Owned Computing Devices by Students

Students may use privately-owned computers and other wireless communication devices under the terms and conditions set forth in Board policy JFCK (Use of Wireless Communication Devices by Students).

1. Students are required to comply with all Board policies, administrative procedures and school rules while using privately-owned computing devices at school. Failure to adhere to Board policies and school rules while using a privately-owned computing device at school may result in confiscation of the device by District officials and further consequences consistent with the terms of the Board Policy, the Student Handbook, and applicable law.

2. School district technology staff will not handle privately-owned computing devices or modify the hardware or software configuration of privately-owned computing equipment without the permission from the Director of Technology.
3. The student is responsible for the proper care of his/her privately-owned computing device, including any costs for repair, replacement, or any modifications needed to use the device at school.
4. The District is not responsible for damage, loss or theft of any privately-owned computing devices.
5. Students have no expectation of privacy in their use of a privately-owned computing device while it is being used at school. The contents of the device may be searched in accordance with applicable laws and policies.

Privacy

Network access is provided as a tool for your education. The District reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the Network and any and all materials, files, information, software, communications and other content transmitted, received or stored in connection with this usage. All such information, content and files shall be and remain the property of the District and you should not have any expectation of privacy regarding those materials. Network administrators may review files and intercept communications for any reason, including but not limited to for purposes of maintaining system integrity and insuring that users are using the system consistently with this Policy.

Compensation for Losses, Costs and/or Damages

The student and his/her parents are responsible for compensating the District for any losses, costs, or damages incurred by the District due to violations of Board policies or school rules while the student is using the Network, including the cost of investigating such violations. The District assumes no responsibility for any unauthorized charges or costs incurred by a student while using the Network.

Internet Safety

- (a) General Warning. All students and their parents/guardians are advised that access to the Network and particularly the Internet may include the potential for access to materials inappropriate for school-aged pupils, including materials that may be illegal, defamatory, obscene, inaccurate or offensive. Certain of these areas on the Internet may contain warnings as to their content, and users are advised to heed these warnings. Not all sites that may contain inappropriate material, however, will include warnings. You must take responsibility for your use of the Network and stay away from these sites.

Parents/guardians of minors are the best guide to the materials to avoid. If you find that other users are visiting offensive or harmful sites, you should report that use to the Principal or other designated administrator in your school.

(b) Personal Safety. Be safe. Do not use the Network or the Internet to access chat rooms or chat lines. In using the Network or the Internet, do not reveal personal information such as your or another's home address, telephone number, social security number or photograph. Due to the anonymous nature of the Internet, students should not arrange a face-to-face meeting with someone you "meet" through the Network or the Internet without permission of your parent or guardian.

(c) Confidentiality of Student Information. Personally identifiable information concerning students may not be disclosed or used in any way on the Network without the permission of a parent/guardian or, if the student is 18 or over, the permission of the student himself/herself. Students should never give out private or confidential information about themselves or others on the Internet.

(d) Active Restriction Measures. Consistent with applicable law, the District, either by itself or in combination with the Information Technology Center providing Internet access, will utilize filtering software or other technologies to limit student access to visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors. The District may also monitor the online activities of students, through direct observation and/or technological means, to limit student access to such depictions or any other material which is inappropriate for minors. As it is impossible to limit access to all materials that may be considered inappropriate, the ultimate responsibility for monitoring Network usage is that of the student and the student's parents/guardians.

Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary for purposes of bona fide research or other educational projects being conducted by students age 17 and older.

The term "harmful to minors" as used herein shall have the same meaning as defined in the Communications Act of 1934 (47 USC Section 254 [h][7]).

System Security

The security of the District's Network is a high priority. Any student who identifies a security problem must notify his/her teacher immediately. The student shall not demonstrate the problem to others or access unauthorized material. Any user who attempts to breach system security, causes a breach of system security or fails to report a system security problem shall be subject to disciplinary and/or legal action in addition to having his/her Network privileges limited, suspended or revoked.

Failure to Follow Policy

Your use of the Network is a privilege, not a right. If you violate this Policy, you may be subject to disciplinary action. At a minimum you will be subject to having your access to the Network terminated, which the District may refuse to reinstate for the remainder of your tenure in the District. You breach this Policy not only by affirmatively violating the above Policy, but also by failing to report any violations by other users that come to your attention. A violation of this Policy may also be a violation of the law and subject the user to criminal or civil investigation and prosecution.

Warranties and Indemnification

The District makes no warranties of any kind, either express or implied, in connection with its provision of access to or use of its Network or the Internet. It shall not be responsible for any claims, losses, damages or costs (including attorneys' fees) of any kind suffered, directly or indirectly, by any user or the user's parents or guardians arising out of the user's use of, or inability to use, the Network or the Internet. By using the Network or the Internet, you are taking full responsibility for your use, and are agreeing to indemnify and hold the District and the Information Technology Center and all of their administrators, teachers and staff harmless from any and all loss, costs, claims or damages (including attorneys' fees) resulting from access to and use of the Network or the Internet through your account, including but not limited to any fees or charges incurred through purchases of goods or services by the user. You, or, if you are a minor, your parents or guardians, agree to cooperate with the District in the event of the District's initiating an investigation of use or access to the Network or the Internet through your account, whether that use is on a District computer or on another's outside the Network.

Updates

You may be asked from time to time to provide new or additional registration and account information, for example, to reflect developments in the law or technology. You must provide this information if you wish to continue to receive service. If after you have provided your account information, some or all of the information changes, you must notify the Technology Help Desk Manager or other person designated by the District to receive this information. This policy may also be updated by the District from time to time, for example to reflect developments in the law or technology.

[Adoption date: May 24, 2004]

[Re-adoption date: May 23, 2011]