

COMPUTER NETWORK AND INTERNET ACCEPTABLE USE POLICY FOR TEACHERS AND STAFF

The Pickerington Local School District (the “District”) is pleased to make available to teachers and certain staff members 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, all teachers and staff must take responsibility for appropriate and lawful use of this access. Teachers and staff must understand that one employee’s misuse of the Network may jeopardize the ability of all employees and students to enjoy Network access. While the District’s administration and Network administrators will make reasonable efforts to administer use of the Network, they must have teacher and staff cooperation in exercising and promoting responsible use of this access.

This document shall constitute the Computer Network and the Internet Acceptable Use Policy for Teachers and Staff (“Policy”). Upon accepting your account information, you are agreeing to follow this policy and you will then be given the opportunity to enjoy Network access in your building.

If you have any questions about the provisions of the Policy listed below, you should contact the Director of Technology. If any user (that is, you or anyone whom you allow to use your account -- which itself is a violation) using your account violates this policy, your access will be denied or withdrawn and you may be subject to additional disciplinary action.

Purpose and Use

The District’s Network access is provided to staff for purposes related to school programs and operations, and performance of their job responsibilities. Uses that interfere with normal District business or violate District policies are strictly prohibited, as are any uses for the purposes of engaging in or supporting any kind of business or other profit-making activity. If you have any doubt about whether a contemplated activity is consistent with the intended purpose and use of the District Network, you may consult with the Director of Technology for the District.

Reporting Misuse of the Network

In addition to following the terms of this Policy, you should report any misuse of the Network to the Director of Technology. Misuse means any violation of this policy, or violation of the Computer Network and the Internet Acceptable Use Policy and Agreement for Students or any other use that is not included in this policy, but has the effect of harming another or another's property.

Term of the Permitted Use

This policy applies to staff members if and when they are granted access. That access may be granted to the extent that the District determines appropriate, based on the staff member's duties or other factors. 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. Staff members shall not share their passwords or otherwise allow anyone to gain unauthorized access to the Network. A staff member is subject to disciplinary action under Board policy and/or applicable law for any violations of this Policy committed by someone else who, with the staff member's express or implied permission, or through the staff member's negligence, accessed the Network with the staff member's password. By accepting Network access, users waive any and all rights of privacy in connection with their communications over the Network, or communications achieved through the use of District equipment, including but not limited to protections provided by state and Federal law.

Unacceptable Uses

The Board or authorized District officials will make a good faith judgment as to which materials, files, information, software, communications and other content and activity are permitted and prohibited based on the following guidelines and under the particular circumstances. Uses that are considered unacceptable and constitute a violation of this policy include, but are not limited to, the following:

1. 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 employees while using school computers, or while using privately-owned computers on school property.

2. Any use involving materials that are obscene, pornographic, sexually explicit or sexually suggestive.
3. Any inappropriate or unprofessional communication with students or minors.
4. Any use for private financial gain, or commercial, advertising or solicitation purposes.
5. 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 staff.
6. Any use as a forum for communicating by email or any other medium with other school users or outside parties to solicit, proselytize, advocate or communicate the views of an individual or non-school sponsored organization; or to raise funds for any non-school sponsored purpose, whether profit or not-for-profit. No employee shall knowingly or negligently provide school email addresses to outside parties whose intent is to communicate with school employees, students and/or their families for non-school purposes.
7. Any communication that represents an employee's personal views as those of the school unit or that could be misrepresented as such.
8. Downloading or loading software applications without permission from the Director of Technology.
9. Any malicious use or disruption of the District's computers or Network services; any breach of security features; or misuse of computer passwords or accounts (the employee's or those of other users).
10. Any misuse or damage to the District's computer equipment.
11. Any attempts to access unauthorized sites, or any attempt to disable or circumvent, or to help others disable or circumvent, the District's web filtering technology.
12. Failing to report a breach of security to the Director of Technology.
13. Any attempt to delete, erase, or otherwise conceal any information stored on a school computer that violates this Policy or other Board policies or school rules, or refusing to return computer equipment issued to the employee upon request.
14. Revealing another's personal information such as their home address, telephone number or Social Security number.

15. Making ethnic, religious, sexual preference or gender-related slurs or jokes.

Employee Responsibility to Supervise Computer Use

Employees who use the Network with students for instructional purposes have a duty of care to supervise such use. Teachers and other staff members are expected to be familiar with the District's policies and rules concerning student Network use and to enforce them. When, in the course of their duties, employees become aware of a student violation, they are expected to stop the activity and inform the building principal.

Personal Use of District Computer Equipment and Network

District computers and Network services are provided to employees for purposes related to school programs and operations, and performance of their job responsibilities. Incidental personal use of school computers is permitted, as long as such use: 1) does not interfere with the employee's job responsibilities and performance; 2) does not interfere with system operations or other system users; and 3) does not violate this policy and the accompanying rules, or any other Board policy, procedure or school rules. "Incidental personal use" is defined as use by an individual employee for occasional personal communications.

Mobile Computer Equipment Issued Directly to Employees

This policy and the accompanying rules also apply to mobile District computers and computer equipment issued directly to employees, whether in use at school or off school premises.

Employee Responsibility for District-issued Computer Equipment. Employees are responsible for all District computer equipment issued directly to them. Reasonable efforts should be taken to prevent damage to the equipment and/or loss or theft of the equipment. Reasonable efforts include the following:

1. Children should not handle District-issued computer equipment.
2. Liquids and food should not be placed or handled near the equipment.
3. District computer equipment should be protected from weather elements such as heat, rain, and snow.
4. District computer equipment should not be left unattended in a motor vehicle or public venue.
5. While at school, unattended mobile computer equipment should be secured in a locked office or desk when possible.

Misuse, abuse, or failure to provide reasonable efforts to safeguard mobile computer equipment issued directly to employees may constitute neglect and result in employee responsibility for any repair or replacement costs and possible disciplinary action.

Leave and Disability. Employees who will be out of the District on an extended leave of absence or sabbatical must return any District computer equipment prior to the beginning of the leave.

Procedures for Reporting Lost or Stolen Equipment. If an employee's assigned equipment is stolen or lost the employee is required to immediately notify the Director of Technology and provide relevant information about the circumstances of the theft/loss. The Director of Technology will file a report with the Human Resources department and with local authorities, if necessary.

Use of Privately-Owned Computing Devices by Employees

Employees may use privately-owned computers and other wireless communication devices (see Board policy JFCK) at school in accordance with the following guidelines:

1. Employees 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 Employee Handbook, the Collective Bargaining Agreement, 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 employee 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. Employees 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.

Data Handling and Security

The Pickerington Local School District does not authorize the placement or storage of sensitive data related to anyone associated with the District on computer equipment issued directly to employees or on privately-owned computing devices without the written consent of the Superintendent. Sensitive data is defined as any individually identifiable information that is not public record, including but not limited to, social security numbers; student identification numbers; financial records; health records; academic records; and discipline records. Persons associated with the District include but are not limited to, staff members; students; parents or guardians of students; vendors; and game officials. Any noncompliance with these requirements will constitute a security violation. Serious violations may result in disciplinary action up to and including termination and/or civil or criminal prosecution.

Procedures for Reporting a Breach of Data Security. If an employee becomes aware of or suspects a breach of data security, the employee is required to immediately notify the Director of Technology and provide relevant information about the circumstances of the breach. The Director of Technology will file a report with the Human Resources department and with local authorities, if necessary. The employee may be required to take appropriate action to notify any affected persons of the breach.

Privacy

Network access is provided as a tool for education or educational administration. 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

Employees 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 employee is using the Network, including the cost of investigating such violations. The District assumes no responsibility for any unauthorized charges or costs incurred by an employee while using the Network.

Failure to Follow Policy

Your use of the Network is a privilege, not a right. If you violate this policy, 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 of this policy or the student policy by other users that come to your attention. Further, you violate this policy if you permit another to use your account or password to access the Network, including someone whose access has been denied or terminated. If that other person whom you allow to use your account violates this policy using your account, it is considered to be the same as you violating this policy. Both of you are then subject to the consequences of that violation. The District may take other disciplinary action under Board policy. A violation of this policy may also be a violation of the law and subject the user to investigation and criminal or civil 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. 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. By using the Network, 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 through your account, including but not limited to any fees or charges incurred through purchases of goods or services by the user. You agree to cooperate with the District in the event of the District's initiating an investigation of use or access to the Network 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: August 19, 1997]

[Re-adoption date: May 10, 2010]

[Re-adoption date: pending]

LEGAL REFS.: U.S. Const. Art. I, Section 8
Family Educational Rights and Privacy Act; 20 USC 1232g et seq.
Children's Internet Protection Act; (P.L. 106-554, HR 4577, 2000,
114 Stat 2763)
ORC 1329.54 through 1329.67
3313.20
3319.321

CROSS REFS.: AC, Nondiscrimination
ACA, Nondiscrimination on the Basis of Sex
ACAA, Sexual Harassment
IB, Academic Freedom
IIA, Instructional Materials
JFC, Student Conduct (Zero Tolerance)
Staff Handbooks
Student Handbooks