

**Network Privacy And Acceptable Use Policy
For
Staff Members**

It is the intention of the Portsmouth City Board of Education to acknowledge the privacy of staff members who use the school computers, computer network, and electronic messaging systems given the needs of the District. The purpose of this policy is to identify the limitations on this privacy and the general restrictions applying to the use of computer and electronic messaging systems of the District.

Acceptable and Unacceptable Uses

The computers, computer network and messaging system of the School District are intended for educational uses and work-related communications. Incidental use of the e-mail and voice mail systems by staff members for personal communications is permitted as long as such communications are limited in number, are initiated during non-work periods, and do not interfere with the primary intended uses of the system.

The following are uses, which are unacceptable under any circumstances:

- the transmission of any language, images or communication, which are of graphic sexual, violent, inappropriate or offensive nature
- the transmission of messages or any other content, which would be perceived by a reasonable person to be offensive, harassing or threatening
- uses that a reasonable person would consider to be defamatory constitute defamation
- uses that violate copyright laws
- uses that attempt to gain unauthorized access to another computer system or to impair the operation of another computer system (for example, the intentional transmission of a computer virus or an excessively large e-mail attachment)
- any commercial or profit-making activities
- any fundraising activities, unless specifically authorized by Superintendent
- uses constituting political activity
- uses on behalf of any other entity, association, or group, without the consent of the Superintendent
- uses that may be against the best interest of the District, its students, administrators, employees, or Board of Education
- forwarding of any 'chain letters' or 'joke' e-mails

Security and Integrity

Staff members shall not take any action, which would compromise the security of any computer, network or messaging system. This would include the unauthorized release or sharing of passwords and the intentional disabling of any security features of the system.

Staff members shall not take any actions, which may adversely affect the integrity, functionality, or reliability of any computer (for example, the installation of hardware or software not authorized by the System Administrator).

Staff members shall report to the System Administrator or Superintendent any actions by students or any other person which might violate the security or integrity of any computer, network or messaging system whenever such actions become known to them in the normal course of their work duties.

Staff must understand that as a matter of law an email is subject to being recognized as a “public record.” If the email meets the definition of a record in the Ohio Revised Code, Section 149.43, which states in part:

- Public record means any record that is kept by any public office, including, but not limited to, state, county, city village, township, and school district units, may be considered a public record and must be made available to the public, EXCEPT public records does not mean: medical records, records pertaining to adoption, probation, and parole proceedings, records pertaining to actions under section 2151.85 of the Revised Code and to appeals of actions arising under that section, records listed in division (A) of section 3107.42 of the Revised Code, trial preparation records, confidential law enforcement investigatory records and records the release of which is prohibited by state or federal law.

System administrators:

- Are expected to treat the contents of electronic files as private and confidential
- Must report all suspicious requests, incidents, and situations regarding a PCSD computer to the building principal, superintendent, or his/her designee
- Adhere to the PCSD System Administrator Code of Ethics (signed by each PCSD System Administrator)

The District reserves the right to freeze email or network accounts until consent to access the account is obtained from the principal/designee (regarding a student’s account), and from the superintendent/designee (regarding a staff member’s account). The Principal/Superintendent or his/her designee may access an account without the user’s permission upon reasonable suspicion that evidence of criminal activity, serious misconduct, or a violation of this policy will be found in the account.

Any individual who violates the confidentiality of records and/or fails to abide by the Policy will be subject to a loss of access to the system and be subject to disciplinary procedures up to and including termination of employment and dismissal from the District.

Right of Access

Although the Board of Education respects the natural desire of all persons for privacy in their personal communications, and will attempt to preserve this privacy, the operational and security needs of the District's computer network and messaging systems require that full access be available at all times. The School District therefore reserves the right to monitor, record, access and inspect any computer, device, or electronic media within its systems and any data, information, or messages, which may be contained therein. All such data, information, and messages are the property of the School District and staff members should have no expectation that any messages sent or received, or any data or information of any form, on the School District's systems will remain private.

Filtering and/or Logging

PCSD uses a filtering system for all schools, and for offices. This filtering system is designed to prevent access to educationally inappropriate sites. However, it is important to understand that no solution is perfect, and at times educational sites may be incorrectly blocked and conversely, inappropriate sites may not be blocked. It is the staff's responsibility to report any inappropriate site(s) to the tech department. Please also note that our filtering system allows us to track internet usage and the login times.

Social Networking Web Sites

- District staff who personally participate in social networking web sites are prohibited from posting student data, documents, photographs or inappropriate information on any web site that might result in a disruption of classroom activity. The Superintendent/designee has full discretion in determining when a disruption of classroom activity has occurred.
- Fraternalization between District staff and students via the Internet, person email accounts, social networking web sites and other modes of virtual technology is also prohibited.
- Access of social networking web sites during school hours is prohibited.
- Violation of the prohibitions listed above will result in staff and/or student discipline in accordance with State law, Board policies and regulations, the Student Code of Conduct and/or staff negotiated agreements. Nothing in this policy prohibits District staff and students from the use of education web sites.

Adoption date:

Re-adoption date: June 30, 2005

Re-adoption date: August 16, 2007

Portsmouth City School District
Network Privacy And Acceptable Use Policy
For
Staff Members

AGREEMENT

I have read the “Network Privacy and Acceptable Use Policy for Staff Members” relating to staff use of the computers, computer networks, and electronic messaging systems of the School District.

I would like to be given access to the School District’s computer network and any electronic messaging systems.

I agree to comply with the “Network Privacy and Acceptable Use Policy for Staff Members” and understand that access to the network and messaging systems is a privilege, which may be withdrawn in the event of noncompliance with the above Policy.

Staff Member Signature

PLEASE PRINT NAME:

Date

Adoption date:
Re-adoption date: June 30, 2005
Re-adoption date: August 16, 2007