



## Information Technology Procedures Student and Staff Acceptable Use of the District Network

### Introduction

The District's Acceptable Use Policy ("AUP") is intended to prevent online users from unauthorized access and other unlawful activities, prevent unauthorized disclosure of or access to sensitive information, and to comply with the Children's Internet Protection Act ("CIPA"). As used in this policy, "user" includes anyone using the computers, Internet (including social media, e-mail, and chat rooms) and other forms of direct electronic communications or equipment provided by the District (the "network."). **Only current students, approved volunteers, District contractors and PPS employees are authorized to use the network.** The District sponsors and owns the network. The network is intended for educational and administrative purposes as defined in [Board Policy 8.60.040](#).

Once the user acknowledges that they have read and understood the PPS Acceptable Use Policy, the conditions for use remain in effect until:

1. In case of students, revoked by the parent, or the student loses the privilege of using the District's network due to a violation of this policy or is no longer a PPS student.
2. In case of employees, the employee loses the privilege of using the District's network due to a violation of this policy or is no longer a PPS employee.

All network users are expected to follow this policy and report any misuse of the network or Internet to a teacher, or other appropriate District personnel. Access to the District electronic network has been established for educational use only, including support of administrative and student services, student and staff research, lesson planning, collaboration and sharing of ideas, contact with teachers and support staff, and the downloading of materials to be used as educational resources. Social networking has become a common medium of interaction. To learn about the District's policy on social networking, refer to the [PPS Web Policies and Guidelines](#).

District employees may use the network for incidental personal use, but this use should be limited and must be in accordance with all District policies, administrative directives, and other guidelines regarding computers, networks and Web pages.

**By using the network, users have agreed to this policy.** If a user is uncertain about whether a particular use is acceptable or appropriate, he or she should consult a teacher, supervisor or other appropriate District personnel.

### **I. Unacceptable Uses of the Computer Network or Internet**

1. Violating any state or federal law or municipal ordinance, such as: accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information, or copyrighted materials.
2. Selling or purchasing illegal items or substances.
3. Causing harm to others or damage to their property, such as:
  - a. Using profane, abusive, or impolite language; threatening, harassing, bullying or making damaging or false statements about others; accessing, transmitting, or downloading offensive, harassing, or disparaging materials;
  - b. Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs; or disrupting any computer system performance; causing physical damage to a technology resource; or
  - c. Using any District computer to pursue "hacking," internal or external to the District, or attempting to access information protected by privacy laws.

4. Engaging in uses that jeopardize access or lead to unauthorized access into others' accounts or other computer networks, such as:
  - a. Attempting to gain unauthorized access to the District network or to any other computer system through the District network or go beyond your authorized access.
  - b. Using another's account password(s) or identifier(s);
  - c. Interfering with other users' ability to access their account(s);
  - d. Disclosing anyone's password or allowing a person to use another user's account(s);
  - e. Providing your account information to others, or making your account readily accessible;
  - f. Deleting, copying, modifying, or forging other users' names, e-mails, files, or data; disguising one's identity, impersonating other users, or sending anonymous e-mail; or
  - g. Posting or distributing personal information about other District personnel on the District Web site without the employee's permission or making any reference to confidential student information on the District Web site.
5. Using the District network or Internet for:
  - a. Personal financial gain;
  - b. Personal advertising, promotion, or financial gain;
  - c. Conducting for-profit business activities and/or engaging in non-government related fundraising or public relations activities such as solicitation for religious purposes, lobbying for personal political purposes; or
6. Connecting personal equipment without virus protection to the network.
7. Using software or hardware designed to interfere with or circumvent security mechanisms.
8. Using the network or Internet in any manner that violates any District or school rule or policy, including, but not limited to any rule or policy in the District's Handbook on [Student Responsibilities Rights and Discipline](#).

## **II. Plagiarism & Copyright Infringement**

- 1) Users will not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were yours.
- 2) Users will respect the rights of copyright owners. Copyright infringement occurs when you inappropriately reproduce a work that is protected by a copyright. If a work contains language that specifies appropriate use of that work, users should follow the expressed requirements. If users are unsure whether or not they can use a work, they should request permission from the copyright owner. Copyright law can be very confusing. If you have questions, ask a teacher or check out these copyright resources:
  - <http://www.techlearning.com/section/Copyright>
  - [http://www.techlearning.com/techlearning/pdf/events/techforum/tx05/TeacherCopyright\\_chart.pdf](http://www.techlearning.com/techlearning/pdf/events/techforum/tx05/TeacherCopyright_chart.pdf)
- 3) Any software that is protected under the copyright laws will not be loaded onto or transmitted via the network or other on-line servers without the written consent of the copyright holder.

## **III. Use of PPS Network Systems**

All users authorized to access student information are required to abide by the policies governing review and release of student education records. The Family Educational Rights and Privacy Act (FERPA) of 1974 mandates that information contained in a student's education record must be kept confidential and outlines the procedures for review, release and access of such information. Access to student information systems will be granted only to those individuals who have been determined to have a legitimate educational interest in the data. Individuals who have been granted access must understand and accept all responsibilities of working with confidential student records. If the individual loses the data, he/she should inform the appropriate District personnel immediately. Please review the *Portland Public Schools Email Etiquette Guidelines* on the [IT Forms and Policies](#) webpage for information about the expected use and etiquette related to District email systems.

## **IV. Mobile Devices**

A mobile device is any portable, electronic device used for communications including telephone, text messaging or data transmissions (eg. email, web-browsing, streamlining media, file transfer, etc.) over any network.

**Mobile Device Responsibilities** – Individuals who have student data on a mobile device are responsible to secure the data. It is the responsibility of the primary user of the device to immediately inform IT in the event of the device being lost, stolen, missing, infected with a virus/malware, hacked, or otherwise compromised. Any mobile device connected to the District network or configured to access District email is subject to IT oversight, which may include remotely erasing data on the device at any time.

**District Mobile Device Guidelines** – Detailed information regarding current technical specifications, stipends, and specific mobile device (eg. smartphones, tablets, laptops, etc.) guidelines is regularly updated in the *Portland Public Schools Personal Technology Guidelines* document found on the [IT Forms and Policies](#) webpage.

#### **V. Email Archiving and Retention**

The District email retention policy is as follows:

- All email and calendar items sent and received on the PPS email system will be archived.
- All active employees' email will be archived for 3 years.
- Inactive employees' email will be kept in its state on the date of account disable for 13 months past their inactive date. At that time, email and email account will be fully purged from the system.
- Under request or guidance from District HR or Legal personnel, email data from inactive employees may be kept longer than 13 months.

#### **VI. Filtering and Privacy**

In accordance with the Children's Internet Protection Act (CIPA), the District will use technology protection measures on the network to block or filter, to the extent practicable, access to material that is *obscene, pornographic and/or harmful to minors*. Use of the District network constitutes consent to be monitored. Users should have no expectation of privacy regarding their use of District property, network and/or Internet access or files, including e-mail. Under the direction of District HR or Legal authority, the IT Department reserves the right to access and disclose, as appropriate, all information and data stored on District technology, transmitted over the District network and technology. In addition, information and data relevant to any users' work in their District capacity may become discoverable evidence if a public records request is made or for any legal proceedings in which the District may be involved. "Deleted" or "purged" data from the District network may be retrieved for later public records disclosure or disciplinary purposes, as deemed necessary by the District.

#### **VII. Penalties for Improper Use**

The use of a District account is a privilege, not a right. Misuse could result in the restriction or cancellation of the account. Misuse may also lead to other disciplinary and/or legal action for both students and employees, including suspension, expulsion, dismissal from District employment, or, in the case of a student from school, or criminal prosecution by government authorities. The District will attempt to tailor any disciplinary action to meet the specific concerns related to each violation. When applicable, sanctions on employees will be in accordance with the appropriate labor agreement.

#### **VIII. Disclaimer**

**The District makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the network or accounts. Any additional charges a user accrues due to the use of the District's network are to be borne by the user. The District also denies any responsibility for the accuracy or quality of the information the user obtains using the District network. Any statement, accessible on the computer network or the Internet, is understood to be the author's individual point of view and not that of the District, its affiliates, or employees.**