Administrative Directive 8.60.041-AD

Student and Staff Acceptable Use of District Technology Policy (AUP)

Introduction

The District's Acceptable Use Policy ("AUP") is intended to prevent online users from unauthorized access and other unlawful or improper activities, prevent unauthorized disclosure of or access to sensitive information, to comply with the Children's Internet Protection Act ("CIPA") and other applicable laws, and establish expectations for use of District systems.

I. **Definitions**

A. As used in this policy, "user" includes anyone using the computers, Internet (including social media, e-mail, and chat rooms), web-based PPS software systems and other forms of direct electronic communications or equipment provided by the District (the "network.")

B. The Network- The district has established PPSNet, an electronic communications network (network) for electronic communication and access to, and use of, the World Wide Web.

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

II. **Terms of Permitted Use**

A. Only current students, PPS employees, approved volunteers, school board members and District contractors are authorized to use the network.

B. The District sponsors and owns the network. The network is intended for District-related educational and administrative purposes as defined in Board Policy 8.60.040.

C. By accessing the network, 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 or is no longer a PPS student.

   2. In case of employees or volunteers, the employee or volunteer loses the privilege of using the District's network or is no longer a PPS employee.

D. All network users are expected to follow this policy and report any misuse of the network to a teacher, or other appropriate District personnel. Access to the 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.

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

F. 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.

G. 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. In the event of loss of data and/or device, it is the individual's responsibility to immediately notify Risk Management and follow appropriate established District policy as defined in Board Policy 8.90.030. .

H. In order to protect student data and Personally Identifiable Information (PII) the IT Department may implement end point protection including encryption on District mobile devices. Individuals who have student data on a mobile device are responsible for the security of that data at all times. It is the responsibility of the primary user of the device to immediately inform the Information Technology Department (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 network or configured to access District email is subject to IT oversight, which may include remotely erasing data on the device at any time.

I. Network users shall have no expectation of personal privacy in the use of the District's network. Passwords are used to protect the security of District data and technologies and are not intended to convey an expectation of personal privacy or exclusion from monitoring.

J. Under the direction of the Superintendent, Human Resources Director or the General Counsel's office. , 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.

K. Authorized District personnel may temporarily suspend or permanently end any user's access.

L. Documents, emails, and other electronic records created, sent or received using the Network are public records and may be subject to disclosure by law. They must be preserved in compliance with District and State record retention and preservation policies. Access the District's Network from employee owned computing devices such as employee owned home computers, or any portable computing device (such as a laptop, smartphone, or other electronic device used to access electronic data) may subject the employee's personal devices to disclosure.

M. Employees who participate in an approved PPS Social Media Presence must abide by the rules as defined in Administrative Directive Social Media Use and Expectations.

N. PPS uses Google Apps for Education for online collaboration with staff and students. Employees using Google Apps for Education must abide by the terms and conditions signed upon initial log-in to Google Apps for Education, as well as all terms of this policy.

O. PPS employees are required to use district email to conduct all district business, and may not use personal email for any district business.

III. **Prohibited Use**

A. District employees shall not use the network to access obscene material, including pornography, or any other material that is harmful to the district's educational purpose and mission or inconsistent with a professional work environment. If such material is inadvertently accessed, a district employee should notify his or her supervisor as soon as reasonably possible.

B. Violating any state or federal law or municipal ordinance, accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential

information, or copyrighted materials.

C. Selling or purchasing illegal items or substances.

D. Causing harm to others or damage to their property, such as:

1. Using profane, abusive, or impolite language; threatening, harassing, bullying or making damaging or false statements about others;

2. Accessing, transmitting, or downloading offensive, harassing, or disparaging materials;

3. 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

4. Using any device to pursue "hacking," internal or external to the District, or attempting to access or store information protected by privacy laws.

E. Engaging in uses that jeopardize access or lead to unauthorized access into others' accounts or other computer networks, such as:

1. Attempting to gain unauthorized access to the network or to any other computer system through the network or go beyond your authorized access.

2. Using another's account password(s) or identifier(s);

3. Interfering with other users' ability to access their account(s);

4. Disclosing anyone's password or allowing a person to use another user's account(s);

5. Providing your account information, including passwords, to others, or making your account readily accessible;

6. 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

7. Posting or distributing personal information about other District personnel on the District Web site or public Internet without the employee's permission or making any reference to confidential student information on the District Web site or public Internet.

F. Using the network for:

1. Personal financial gain;

2. Personal advertising, promotion, or financial gain;

3. 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

4. Using software or hardware designed to interfere with or circumvent security mechanisms.

5. Using the network in any manner that violates any District or school rule or policy, including, but not limited to any rule or policy in the "Student Responsibilities, Rights and Discipline Handbook" located on the PPS website.

G. Plagiarism & Copyright Infringement

1. Users are prohibited from plagiarizing works they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were your own.

2. Users must 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 is complex. If you have questions, ask a teacher, supervisor or the General Counsel.

3. Any software that is protected under the copyright laws may not be loaded onto or transmitted via the network or other on-line servers without the written consent of the copyright holder.

H. Google Apps for Education

PPS uses Google Apps for Education for online collaboration with staff and students. Users agree to not use Google Apps for Education services:

1. to generate or facilitate unsolicited bulk commercial email;

2. to violate, or encourage the violation of, the legal rights of others;

3. for any unlawful, invasive, infringing, defamatory, or fraudulent purpose;

4. to intentionally distribute viruses, works, Trojan horses, corrupted files, hoaxes, or other items of a destructive nature;

5. to interfere with the use of the Services, or the equipment used to provide the Services, by customers, authorized resellers, or other authorized users;

6. to alter, disable, interfere with or circumvent any aspect of the Services;

7. to test or reverse-engineer the Services in order to find limitations, vulnerabilities or evade filtering capabilities.

I. No user shall establish a peer-to-peer network or wireless ad-hoc using their personal device, or any other wireless device while on district property. This includes, but is not limited to using a privately owned electronic device such as a cabled or wireless hotspot.

J. 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.

IV. **Internet Safety**

A. 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 visual depictions that are obscene, pornographic and/or harmful to minors.

B. 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, files, and other District systems including e-mail. Monitoring technologies may be used to identify and mitigate issues with access of inappropriate materials.

C. It is the intention of Portland Public Schools to educate our students to be good Cybercitizens. With input from building administrators, teachers,

instructional leaders and parents, Information Technology will provide resources and curriculum around topics such as:

1. Safety and security of minors when using technology such as social networking websites, email, video games, chat rooms, instant messaging, and other forms of direct electronic communications;
2. Respectful and appropriate online behaviors;
3. Cyberbullying awareness and response;
4. Cyber-ethics awareness including plagiarism, cheating and information literacy.

D. Instructional materials will be presented through a variety of age-appropriate methods. Tracking of student education efforts will be required. For more detailed information, please see the District's *Internet Safety Guidelines*.

V. **Archiving and Retention**

A. The District email retention policy is as follows:

1. All email and calendar items sent and received on the PPS email system will be archived.
2. Active employees' email will be archived for 3 years based on date of receipt or origination.
3. 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.
4. Under request or guidance from the Human Resources Director or the General Counsel's Office, email data from inactive employees may be kept longer than 13 months.

B. Files saved on the District network are retained as follows:

1. Active employees' files will be retained for the duration of their employment.
2. Inactive employees' files will be kept in its state on the date of account disable for 13 months past their inactive date. At that time, files will be fully purged from the system.
3. Under request or guidance from District HR or Legal personnel, files from inactive employees may be kept longer than 13 months.

C. User accounts are maintained as follows:

1. Active employees' accounts are maintained for the duration of their employment.
2. Inactive employees' accounts are disabled 14 days after the date of inactive status with HR.
3. Inactive employees' accounts are fully purged from the system 13 months past their inactive date, coinciding with the full email purge.
4. Under request or guidance from District HR or Legal personnel, accounts from inactive employees may be kept longer than 13 months.

AD History: Amd. 8/2012, 8/2014, 8/2015