Administrative Directive 8.60.041-AD

Acceptable Use of District Technology Policy (AUP) for Students and Staff

Introduction

This administrative directive explains how students and staff should use District technology. It aims to prevent misuse, unauthorized disclosure of or access to sensitive information, comply with laws like the Children's Internet Protection Act ("CIPA"), and set clear expectations for the proper use of District computers, networks, software, internet and AI tools.

I. Definitions

A. "User" means any person using District computers, Internet (including social media, e-mail, and chat rooms), software, or other forms of direct electronic communications or equipment provided by the District.

B. "Network" means the District's PPSNet system that provides electronic communication and internet access.

C. "Mobile Devices" means any portable electronic device including telephones, tables, or laptops used for communication, email, web browsing, or data transfer.

D. "Artificial Intelligence (AI) Tools" means software or applications that use AI to generate content, analyze data, or automate tasks. This includes text generation, image creators, voice tools, grading systems, and large language models.

E. "Generative AI" means AI tools that create new content like text, images, audio, video or code based on data they have learned and provide responses that are often human like. Some examples include ChatGPT and Gemini.

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

C. By accessing the Network, each user agrees to follow the PPS Acceptable Use Policy and this Administrative Directive. This

Agreement stays in effect until:

1. For students: a parent revokes permission, the student loses Network privileges, or the student leaves PPS.

2. For employees, Board members, contractors, or volunteers: They lose Network privileges or no longer work, provide services, or volunteer for PPS.

D. All Network users are expected to follow this administrative directive and report any misuse of the Network to the Office of Technology and Information Services or building administrator. The Network is for educational purposes only, including administrative and student services, research, lesson planning, collaboration, communication with teachers staff, and accessing educational materials.

E. District employees may use the network for incidental personal use, but must keep it limited and follow all District policies, administrative directives, and other guidelines.

F. If a user is uncertain about whether a particular use is allowed under District policy, they should ask the Office of Technology and Information, a teacher, administrator, or other appropriate District staff.

G. All users authorized to access student information must follow the Family Educational Rights and Privacy Act (FERPA) of 1974 rules require that student education records are 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 a legitimate educational interest in the data.

If there is a loss of District data and/or a District device, users should immediately notify Risk Management and follow appropriate procedures established under District policy 8.90.030.

H. To protect student data and Personally Identifiable Information (PII), the IT Department may implement security measures like encryption on District devices. Individuals who have student or other District data on a mobile device are responsible for keeping that data secure. 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 should not expect privacy when using the District's network. Passwords protect the District's data and technologies and personal privacy.

J. Under the direction of the Superintendent, Human Resources, and/or the General Counsel's office, the IT Department may access and share, as appropriate, information stored on District technology or, transmitted over the District Network. Information and data on the District Network and devices may be subject to a public records request or in legal proceedings.

K. District staff can suspend or end any user's access.

L. Documents, emails, and other electronic records created or transmitted on the Network are public records and may be required to be disclosured by law and must be preserved in compliance with District policies and State law. Access to the District's Network from employee-owned computing devices such as home computers, or any portable computing device (such as a laptop, smartphone) may subject the content on an employee's personal devices to disclosure.

M. Staff using approved PPS social media must follow District policy, including Administrative Directive Social Media Use and Expectations 8.60.044.

N. Employees and students using Google Workspace for Education must abide by the terms and conditions signed upon initial log-in to Google Workspace for Education.

O. Staff must use District email for all district business and may not use personal email for District business.

P. AI Tools: responsible use and data protection:

1. District-approved AI Tools may be used for educational purposes. Please search the PPS App Library using the filters Category or Subject and selecting the term AI-Artificial Intelligence to see approved apps.

2. Staff may use District-approved AI tools to help with administrative tasks, lesson planning, and personalized learning, but must review all AI-generated content.

3. When using AI tools, users are responsible for all content created. AI use does not excuse following academic integrity standards, copyright laws, District policies, or applicable laws.

4. Users should always check AI-generated content for accuracy, bias, and appropriateness before using it for education or District purposes.

5. Never upload student work, grades, or personal information to AI tools unless specifically authorized by the District.

III. **Prohibited Use**

Users must not:

A. Access inappropriate content, 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, staff should notify their supervisor right away.

B. Violate any laws; access pornography, obscene depictions, harmful

materials, or content that encourage others to violate the law; or share confidential or copyrighted materials.

C. Sell or purchase illegal items or substances.

D. Cause harm to others or damage property, including:

1. Using offensive, profane, abusive, or impolite language; threatening, harassing, bullying or spreading false information;

2. Accessing or sharing offensive, harassing, or disparaging materials;

3. Damaging equipment, files, data, or the Network, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs; or

4. “Hacking” or trying to access or store protected information.

E. Access someone else’s password, accounts, or other computer networks, such as:

1. Attempting to gain unauthorized access to the Network or to any other computer system.

2. Interfering with other users’ ability to access their accounts;

3. Sharing passwords or allowing others use another user’s account(s);

4. Changing others’ files; impersonating others, disguising identity, or sending anonymous message; or

5. Disclosing personal information about or students without permission.

F. Use the network for:

1. Personal financial gain;

2. Personal advertising or promotion;

3. Business activities, non-District fundraising religious solicitation, or prohibited political lobbying;

4. Bypassing or interfering with security mechanisms.

5. Violating any District policy or rule..

G. Plagiarizing & Infringing on Copyright.

1. Do not plagiarize works on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were your own.

2. Respect copyright laws. Copyright infringement occurs when you reproduce a work without permission that is protected by a copyright. Copyright law is complex. If you have questions, ask staff, supervisor, or the General Counsel's Office.

3. Do not install, load or share any software that is protected under the copyright laws without the written consent of the copyright holder.

H. Google Workspace for Education.
Do not use Google Workspace for Education services to:

1. send SPAM or other unsolicited bulk commercial email;

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

3. Do anything unlawful, invasive, infringing, defamatory, or fraudulent;

4. spread viruses, hoaxes, or harmful files, ;

5. interfere with the services;

6. try to disable, interfere with or bypass any features of the Services;

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

I. Do not set up your own networks (including hotspots or peer-to-peer networks) on District property.

J. The use of a District account is a privilege. Misuse can result in: loss of access, disciplinary action, and/or legal consequences, depending on the nature and seriousness of the misuse.

K. Generative AI has a variety of uses in the classroom, including providing support with designing learning experiences for students, as a teaching tool, supporting differentiation, as an extension of

instructional support, and a starting point for providing student support. The key to using AI is to be intentional about the tools being implemented in the classroom to guard against:

1. Inadvertently violating FERPA by using generative AI tools for tasks that pull confidential student information into the data of the AI provider or other third party.

2. Allowing bias inherent in many AI tools to distort teaching and learning. It is important for teachers to provide instruction and information to students and their families about the potential bias found in the tools being used.

3. Use of inaccurate information from AI.

Using AI requires teaching students to fact check for misinformation within the generative AI responses.

It also requires lesson plans and assignments to increase student awareness of use of information generated from AI tools to avoid plagiarism and copyright infringement.

IV. **Internet Safety**

A. In accordance with the Children's Internet Protection Act (CIPA), the District uses filters, to the extent practicable, to block inappropriate content for 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.

C. PPS will educate students to be good digital citizens, including:

1. Online Safety and security on social networking websites, email, video games, chat rooms, instant messaging, and other forms of direct electronic communications;

2. Respectful online behaviors;

3. Cyberbullying awareness and response;

4. Cyber-ethics awareness including avoiding plagiarism, cheating and information literacy.

AD History: Amd. 8/2012, 8/2014, 8/2015; 8/2025