APPROPRIATE USE OF DISTRICT TECHNOLOGY   IJNDC

Introduction

Portsmouth School District (PSD) is committed to providing authorized users with access to district technology, the Internet, and various technological resources to enhance educational excellence. Authorized users include students, staff, and guests, hereafter referred to as "users." Each user is responsible for their use of technology, whether it is provided by PSD or is a personal device. When utilizing district or personal technology resources on or near school property (including in school vehicles and at school-sponsored events) or when accessing PSD's technology resources remotely, users must adhere to school, district, and legal guidelines.

Use of PSD Technology Resources

PSD's information systems and Internet access are intended to support learning, enhance instruction, and facilitate school operations. While limited personal use that aligns with this policy is permitted, it should be minimal. The following uses of PSD technology are strictly prohibited:

- Personal gain, profit, or commercial activities
- Political lobbying
- Any actions that disrupt the operation of the network or interfere with the learning or work of others
- Activities related to terrorism or other unlawful actions
- **Misuse of Artificial Intelligence (AI) tools, including but not limited to generating misleading or harmful content, using AI to plagiarize or fabricate academic work, bypassing security measures, or impersonating others.**

The use of PSD's technology systems is a privilege, not a right. Access may be restricted or terminated by the administration without prior notice if deemed necessary for security or operational reasons. Additional disciplinary actions may be enforced in accordance with school handbooks. PSD is compliant with the **Children's Internet Protection Act (CIPA)** and implements internet filtering; however, it cannot guarantee students will not encounter inappropriate material.

Cybersecurity Awareness: Security is a shared responsibility. Users must report any suspicious or questionable activities immediately. Think before you click.

Privacy

All electronic information created, stored, sent, or received using PSD technology is considered public communication and is not private. While PSD does not regularly review archived files, it reserves the right to access and monitor all electronic information as needed for operational and security purposes. This may include disclosure to law enforcement or third parties in compliance with the **Family Educational Rights and Privacy Act (FERPA).**

PSD maintains the integrity, security, and privacy of confidential records and discloses information externally only for legitimate educational purposes or as required by law.

Respect for Others Using PSD Systems

Users must respect the rights of others when utilizing PSD technology resources by:

- Using assigned workstations appropriately.
- Being considerate when using shared resources.
- Logging off workstations after use.
- Avoiding actions that could disrupt system performance.
- Leaving shared technology equipment in good condition.

Photography and Videography Guidelines:

- Recording devices may not be used in locker rooms, restrooms, or other private areas.
- Teachers, staff, and administrators must announce intent before recording in classrooms.
- Students who have elected not to disclose "directory information" under FERPA or who signed the video/photo/media opt-out form must not be included in recordings or images.
- Recordings of classes or school activities require express permission.
- Unauthorized recording (Audio or Video) or dissemination of students, teachers, administrators, or staff is prohibited.

Ethical Conduct for Users

Users are responsible for:

- Accessing only their assigned accounts and maintaining password security.
- Locking their computer screen before stepping away.
- Honoring intellectual property and avoiding plagiarism.
- Using PSD resources in alignment with the school's educational mission.
- Refraining from offensive, obscene, or harassing language.

- Abstaining from using technology for personal financial gain, gambling, or non-educational purposes.
- Avoiding unauthorized installations of software or connection of personal devices to the PSD internal network.
- Handling confidential data responsibly, including securing printouts and storing files in approved PSD locations.
- Reporting lost or stolen devices immediately to IT.
- **Ensuring that AI-generated content is used responsibly, with proper attribution, and does not misrepresent work or violate academic integrity policies.**

Internet Safety and Security

The Portsmouth School Department has a responsibility to provide a safe technology environment for its educational community, in compliance with federal and state law. PSD will use internet filtering, user monitoring, and other mechanisms to protect the environment.

Users may not post or share information that:

- Violates others' privacy or jeopardizes student safety.
- Is obscene, libelous, or disruptive to the school environment.
- Plagiarizes or infringes on copyright.
- Is commercial in nature or unauthorized by administration.

Users must:

- Obtain teacher or administrator permission before engaging in real-time messaging or online chats.
- Refrain from sharing personally identifiable information on school based online social media platforms.
- If you encounter any malicious, inappropriate, or suspicious messages, please report them to IT using PSDs "Phish Hook" icon in the Gmail application, by submitting a ticket through the ticketing system, or via the anonymous reporting link.
- Avoid accessing Internet sites inconsistent with PSDs educational mission.
- Cite and credit all sourced online material. PSD prohibits copying, downloading, or distributing inappropriate content or illegal material on district owned or personal devices used for district related work.
- Understand that all devices on the PSD network are subject to monitoring and review, under the Freedom of Information Act (FOIA), and sequestered by school authorities if deemed malicious.

- Report any suspicious messages, chats, or social media posts to their teacher, immediate supervisor, utilize the anonymous reporting link on the PSD homepage, or IT Team via the PSD ticketing system.
- Create web pages/blogs/vlogs that are subject to approval and ongoing review by the site owner and/or school principal. All web pages should reflect the mission and character of the school and must be built within the schools website.

Social Media and Online Communication

PSD operates and maintains the official social media profiles to keep the community updated on events, celebrate accomplishments, and communicate essential information. Users are expected to follow these social media guidelines to:

- Not disclose personally identifiable student or employee information.
- Obtain written consent before sharing student work or images.
- Maintain professionalism in all social media interactions.
- Avoid using personal social media for PSD business.
- Not use PSD email addresses for personal social media activities.
- Avoid adding current PSD students as social media contacts. Former students must be over 18 to be contacted via personal accounts.

Enforcement and Compliance

Violations of this policy may result in disciplinary action, including but not limited to:

- Suspension or termination of access privileges.
- School disciplinary measures in accordance with student handbooks.
- Legal action if applicable.

Policy History:

Adopted: October 22, 2013   Portsmouth School Department
Amended: September 24, 2018   Portsmouth, Rhode Island
Revised: August 27, 2019
Revised: February 25, 2025

Reference:

IJK Policy

RIGL § 16-21.6-1 (Internet filtering)

APPROPRIATE USE OF DISTRICT TECHNOLOGY   **IJNDC**

Children's Internet Protection Act, 20 U.S.C. 9134, 47 U.S.C. 254

Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505

RIGL § 16-38-14 Use of school district listservs (Thrillshare)