Adopted: February 24, 2014

Revised: July 21, 2014 / August 15, 2016

Rushford-Peterson Schools
Technology/Social Media Acceptable Use Policy #524

TECHNOLOGY/SOCIAL MEDIA ACCEPTABLE USE POLICY

Introduction

Rushford-Peterson Schools recognizes that access to technology in school gives students and teachers' greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st-century technology and communication skills.

To that end, we provide access to technologies for student use. This Acceptable Use Policy outlines the guidelines and behaviors that users are expected to follow when using school technologies or when using personally-owned devices on the school campus.

- The wireless networks are intended for educational purposes.
- All activity over the wireless networks or using district technologies may be monitored and retained.
- Access to online content via the wireless networks may be restricted in accordance with our policies and federal regulations, such as the Children's Internet Protection Act (CIPA).
- Students are expected to follow the same rules for good behavior and respectful conduct online as offline.
- Misuse of school resources can result in disciplinary action.
- We make a reasonable effort to ensure students' safety and security online, but will not be held accountable for any harm or damages that result from misuse of school technologies.
- Users of the wireless networks or other technologies are expected to alert IT staff immediately of any concerns for safety or security.

Technologies Covered

Rushford-Peterson Schools may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more.
As new technologies emerge, Rushford-Peterson Schools will attempt to provide access to them. The policies outlined in this document are intended to cover all available technologies (including personal owned devices), not just those specifically listed.

Usage Policies

All technologies provided by Rushford-Peterson Schools are intended for educational purposes. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, careful and kind; don't try to get around technological protection measures; use good common sense; and ask if you don't know.

Internet Access

Rushford-Peterson Schools provides its students with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with CIPA regulations and school policies. Web browsing may be monitored and web activity records may be retained indefinitely.

Users are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn't be, the user should follow protocol to alert an IT staff member or submit the site for review.

Email

Rushford-Peterson Schools provides students with email accounts for the purpose of school-related communication only. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed by the district policy or the teacher.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

Social / Web 2.0 / Collaborative Content

Recognizing that collaboration is essential to education, Rushford-Peterson Schools may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally-identifying information online.

Personal-Owned and School-Owned Device (1:1 Program)

- The student takes full responsibility for his or her device at all times by keeping it in their possession or locked securely in their locker. **R-P Schools is not responsible for any lost or stolen devices.**
- The student is responsible for the proper care of his or her personal device, including any costs of repair, replacement or any modifications to use the device at school. R-P Schools will not provide any technical support, training, updating, or repair of any devices outside of connecting to the district wireless network and printing facilities.
- The school reserves the right to inspect a student's personal device if there is reason to believe the student has violated district school board policies, administrative procedures, school expectations, or has engaged in other misconduct while using their personal device.
- Violations of any R-P Schools school board policies, administrative procedures, or school rules involving use of personally owned devices may result in the loss of use of the device in school and/or disciplinary action as outlined in the student handbook.
- The student must comply with a staff request at any time to shut down the device or put the screen to sleep.
- No devices are allowed during district wide assessments.

- The student may not use the device to record, transmit, or post photos or video of a person or persons on school property. Additionally, students may not transmit or post any images or video recorded at school without the express permission of a teacher or administrator and of any filmed subjects.
- During class periods, the student is expected to only use their device to access classroom and academic related activities.
- The student will use the "RPStudents" or "RPMacBooks" wireless networks while in school. Use of 3G or 4G personal data plan connections is not permitted.

Security

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. If you believe a computer or device you are using might be infected with a virus, please alert IT. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

Downloads

Users should not download or attempt to download or run any programs over the school network or onto school resources without permission from IT staff. You may be able to download other file types, such as images of videos only from reputable sites, and only for educational purposes.

Netiquette

- Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.
- Users should also recognize that among the valuable content online is unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet.
- Users should also remember not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see. Once something is online, it's out there—and can sometimes be shared and spread in ways you never intended.

Plagiarism

- Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet.
- Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Personal Safety

If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if you're at school; parent if you're using the device at home) immediately.

- Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without adult permission.
- Users should recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others.
- Users should never agree to meet someone they meet online in real life without parental permission.

Cyberbullying

Cyberbullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Don't be mean. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else.

Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.

Limitation of Liability

Rushford-Peterson Schools will not be responsible for damage or harm to persons, files, data, or hardware. While Rushford-Peterson Schools employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness. Rushford-Peterson Schools will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Violations of this Acceptable Use Policy

Violations of this policy may have disciplinary repercussions, including:

- Suspension of network, technology, or computer privileges in extreme cases
- Notification to parents in most cases
- Detention or suspension from school and school-related activities
- Legal action and/or prosecution

I have read Rushford-Peterson's computer network/internet use and social media policies and agree to abide by them. I understand that any violation of the above terms may result in discipline, up to and including my termination.

_____

(User's Printed Name)

_____

(User's Signature)

_____

(Date)

I have read and discussed this Acceptable Use Policy with my child:

_____

(Parent Printed Name)

_____

(Parent Signature)

_____

(Date)