

Raymore-Peculiar School District

Technology Acceptable Use Policy (AUP)

This AUP defines the parameters of proper use of Raymore Peculiar School District computer technology resources

Contents

- I. [Usage Guidelines](#)
- II. [Code of Conduct](#)
- III. [Internet and Email](#)
- IV. [Enforcement](#)
- V. [Disclaimers](#)
- VI. [District Webpage Guidelines](#)
- VII. [Social Media Guidelines](#)
- VIII. [Agreement](#)

Rev. September 2013

The Raymore-Peculiar School District (RPSD) Board of Education believes in the importance of students, and staff to have reasonable access to electronic-based research tools and master skills for their application to learning, problem solving, production of work, and presentation of information. The Board also recognizes that while these resources represent extraordinary learning opportunities and enriching educational materials, they also offer persons with illegal, immoral, or inappropriate motives avenues for reaching students, teachers, staff, parents/guardians, and members of the community. Additionally, these resources present tempting opportunities for users to explore areas that are confidential, have restricted access, are inappropriate, and are disruptive to the classroom or workplace. It is the purpose of the District Technology Acceptable Use Policy (AUP) to outline acceptable student and employee behavior with respect to use of District technology and electronic resources.

This AUP applies to any situation where any person (or persons) utilizes the RPSD's technology resources. For purposes of this policy, RPSD's technology resources are meant to include, but are not limited to: email, local and externally accessed databases, network drives, Inter- and Intranet(s), and any other computer technology equipment.

The purpose of the RPSD's technology resources is:

- To improve learning and teaching through research, teacher training, collaboration and dissemination of successful educational practices, methods, and materials.
- To educate students on safe and appropriate use of computers and technology resources, including the Internet.
- To support research, educational and administrative activities, by providing access to these resources and an opportunity for collaborative work.

All use of RPSD's technology resources must be supportive of these purposes and consistent with the educational objectives of the RPSD. RPSD technology resources are not a public forum including District website pages. Students or employees who misuse electronic resources or who violate laws will be disciplined at a level appropriate to the seriousness of the misuse. Users must acknowledge their understanding of the general policy and guidelines as a condition of receiving access to technology resources.

Regulations for the Acceptable Use Policy

I. Usage Guidelines

- A. These guidelines should be followed concerning technology resources and equipment:
- Do not seek information about, obtain copies of, or modify electronic information belonging to other users unless explicitly authorized to do so by those users. Do not share passwords with others or use passwords not belonging to you. This protects you from wrongful accusation of misuse of electronic resources or violation of District policy, state, or federal law.

- The laws of copyright, licensing agreements and trade secret laws control the distribution of programs, databases, and other electronic information resources. Appropriate licensing must be secured prior to loading any software on a District computer. Students and employees may not claim personal copyright privileges over files, data, or materials developed in the scope of their employment, nor may students or employees use copyrighted materials without the permission of the copyright holder.
 - Access to electronic mail (E-mail) is a privilege and designed to assist students and employees in the acquisition of knowledge and in efficiently communicating with others. The District E-mail system is designed solely for educational and work related purposes. E-mail files are subject to review by District and school personnel. Chain letters, "chat rooms" or Multiple User Dimensions (MUDs) are not allowed, with the exception of those bulletin boards or "chat" groups that are created by teachers for specific instructional purposes or employees for specific work related communication.
 - Students or employees who engage in "hacking" are subject to loss of privileges and District discipline, as well as the enforcement of any District policy, state and/or federal laws that may have been violated. Hacking may be described as the unauthorized review, duplication, dissemination, removal, damage, or alteration of files, passwords, computer systems or programs, or other property of the District, a business, or any other governmental agency obtained through unauthorized means.
 - To the maximum extent permitted by law, students and employees are not permitted to obtain, download, view or otherwise gain access to "inappropriate matter," which includes materials that may be deemed inappropriate to minors, unlawful, abusive, obscene, pornographic, descriptive of destructive devices, or otherwise objectionable under current District policy or legal definitions.
 - The District and school administration reserve the right to remove files, limit or deny access, and refer staff or students violating the Board policy to appropriate authorities or for other disciplinary action.
 - Behavior which shall result in revocation of access of RPSD resources shall include, but will not be limited to: damage to or theft of system hardware or software; alteration of system hardware or software; placement of unlawful information, computer viruses, or harmful programs on or through the computer system; or attempts to gather confidential/sensitive information through deceptive means; entry into restricted information on systems or network files in violation of password/account code restrictions; violation of other users' rights to privacy; unauthorized disclosure, use or dissemination of personal information regarding minors; using another person's name/password/account to send or receive messages on the network; and use of the network for personal gain, commercial purposes, or to engage in political activity.
- B. Activities involving use of the RPSD's technology resources must be in accordance with employee handbook(s), student handbook(s), and relevant local, state, federal, and international laws and regulations.
- C. Utilization of any RPSD technology resource constitutes acceptance of the terms of the RPSD AUP. Users acknowledge they have read and understand the AUP and they shall be personally responsible for their acts or omissions in connection with utilization of this policy.

- D. Any and all of the RPSD's technology resources are District property. Network administrators may review files and communications on District systems to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files stored on RPSD equipment would always be private. Users are not permitted to store personal documents using RPSD resources. Network management, reporting, and monitoring technology may be used for educational and security purposes.

II. Code of Conduct

- The use of District technology and electronic resources is a privilege, not a right, and inappropriate use will result in discipline by the school, loss of technology privileges and up to expulsion from school. Unacceptable (and strictly forbidden) uses include the following:
 - Accessing or viewing sexually explicit materials
 - Attempting to alter system software or hardware configurations
 - Causing congestion on a network by such things as the propagation of "chain letters," "broadcasting," streaming music, or unauthorized downloads.
 - Inappropriate messages (including abusive, insulting, harassing, or threatening) to lists or individuals
 - Loading software without prior District authorization
 - Deliberately attempting to degrade system performance or capability, or attempting to damage systems, software, or intellectual property of others
 - Disseminating destructive/disruptive material
 - Sharing of login credentials and passwords for access to network, computer, email, student databases, financial databases, and other secure files, database, and systems.
 - Intercepting or altering network packets
 - Attempting to circumvent the District's Internet firewall to access inappropriate, non-educational websites.
 - Malicious, intentional, or willful introduction and/or spreading of computer viruses
 - Misrepresenting your identity or affiliation in the use of information technology resources
 - Reproducing and/or distributing copyrighted materials without appropriate authorization
 - Sending or storing for retrieval harassing, intimidating, abusive or offensive material
 - Unauthorized copying or modifying files
 - Unauthorized use of registered trademarks
 - Connecting personal (non-District) technology equipment, such as computers, laptops, printers, scanners or software, to District resources, equipment or network. This does not include removable media such as CD's, DVD's, USB flash drives or devices connecting to projectors (doing so is at your own risk and will not be supported by the district Technology Department.)
 - Unauthorized viewing or use of computer files, programs, or any electronic information including all restricted information
 - Using profanity, obscenity, or other offensive language
 - Using someone else's identity and password for access to technology resources or otherwise attempting to evade, disable or "crack" passwords or other security provisions of systems on

the network(s)

- Using the resources for any purpose which violates federal or state laws
- Using technology resources for financial gain, for commercial activity, to engage in political activity, or for any illegal activity
- Violating copyright and/or software agreements
- Violating the privacy of other users
- Displaying or disseminating information that violates the District Sexual Harassment Policy (See Regulations 2130 and 4810)
- Storing personal files using District resources

III. Internet & Email

Internet services are provided by the Missouri Research and Education Network (MOREnet). Any users of the District's technology resources must abide by MOREnet's Acceptable Use Policy, which may be viewed via the Internet at <http://www.more.net/content/service-policies>

System users should assume that all communications and information is public when transmitted via the network and may be viewed by other users. The system administrators may access and read district E-mail.

The District shall use filtering, blocking, or other technology to protect students and staff from accessing Internet sites that contain visual depictions that are obscene or harmful to minors. The District shall comply with the applicable provisions of the Children's Internet Protection Act (CIPA) and the Neighborhood Internet Protection Act (NCIPA).

IV. Enforcement

- A. The RPSD characterizes as unethical and unacceptable, and just cause for taking disciplinary action, removal of networking privileges, legal action, and/or discipline up to and including termination of staff for violating any activity through which an individual:
- Interferes with the intended use of the technology resources;
 - Seeks to gain or gains unauthorized access to /networked technology resources;
 - Violates any portion of this AUP
 - Violates such matters as institutional or third party copyright, trademark, license agreements and other contracts;
 - Uses or knowingly allows another to use any technology resource to devise or execute any scheme to defraud or to obtain money, property, services, or other things of value by false pretenses, promises, or representations;
 - Without authorization, destroys, alters, dismantles, disfigures, prevents rightful access to or otherwise interferes with the integrity of computer-based information and/or other technology resources;
 - Without authorization invades the privacy of individuals or entities that are creators, authors, users, or subjects of the technology resources.

- B. Security on any computer system is a high priority. Security poses challenges for collective and individual users. Any intrusion into secure areas by those not authorized creates a risk for all users of the information system. If you feel you can identify a security problem within any RPSD network, notify a teacher, administrator, technology director, or system administrator immediately. Do not show or identify a security problem to others.
- C. Any and all of the RPSD's network storage areas are District property. Network administrators may review files and communications to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files stored on RPSD equipment would always be private. Users are not permitted to store personal files using RPSD resources. Network management, reporting, and monitoring technology may be used for educational and security purposes.
- D. Violation of this policy may result in revocation of utilization privileges, administrative discipline or criminal and civil prosecution. The RPSD is obligated to cooperate with government and civil authorities in the prosecution of any criminal and civil matter against any person who violates this policy, including disclosure of any records, information, data, images, communications, recordings, or other evidence in the custody of, or accessible by the District.

V. Disclaimers

- A. RPSD will not be responsible for any damages you may suffer. This includes loss of data resulting from delays, non-deliveries, or service interruptions caused by our own negligence, your errors, acts of nature, or omissions. Use of any information obtained via network and/or Internet services provided by the RPSD is at your own risk. RPSD denies any responsibility for the accuracy or quality of information obtained through network services or Internet access.
- B. Neither the RPSD nor the operators of any attached networks shall be liable for any damage arising from any event that is out of its control. Neither the RPSD nor the operators of any attached networks shall be liable for indirect, special, incidental, exemplary, consequential, or any other form of money damages, including, but not limited to the loss of data or information of any kind, however caused, and arising out of or in connection with the performance or the provision of service by the RPSD or by the operators of any other attached networks, whether based in contract, tort, or any other legal theory, and whether or not RPSD or the operators of any attached networks has been made aware of the possibility of such damages.
- C. Any user of RPSD's technology resources agrees to accept the sole responsibility for abiding by the policies of any network or political or administrative domain his/her messages traverse. The user agrees that RPSD's has no responsibility to inform the user of the policies or regulations of those domains.
- D. With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. There may be some material or individual communications which are not suitable for school-aged children. The RPSD views information gathered from the Internet in the same manner as reference materials identified by the schools. Specifically, the district supports resources that will enhance the learning environment with directed guidance from the faculty and staff. Exploration and manipulation of resources is encouraged. However, it is impossible to control all

materials on a global network and an industrious user may discover inappropriate information. The RPSD, in compliance with the Children’s Internet Protection Act (Public Law No. 106-554), employs the use of Internet filtering to reduce the incidence of accidental and intentional access to objectionable websites, but cannot guarantee its effectiveness.

VI. District Webpage Guidelines

The purpose of the RPSD website is to communicate vital information to District employees, students, parents and members of the community. RPSD webpages serve as a representation of the District; therefore, must be created and maintained with the highest standards. These guidelines are to be adhered to in order to maintain those standards and to provide the expectations of the District.

- Web pages must be in compliance with all state, federal and international laws concerning copyright, intellectual property, and the Federal Communications Commission.
- Published information must relate to school matters only. These should be areas of curriculum, instruction, school-authorized activities, school-related information, or district information.
- District, school, and teacher webpages must be hosted on the RPSD webpage system, or on district approved purchased services that are approved by the superintendent or designee.
- All information must be professional with no personal information posted – i.e. personal hobbies, home address, home phone numbers, etc... No links should be supplied to personal webpages.
- Staff are strictly prohibited to share their webpage system username and passwords. The District Technology Acceptable Use Policy (AUP) must be followed. Violating the AUP or these webpage guidelines will result in removal of permissions of the webpages and can result in disciplinary action.
- PTO/PTA and Booster webpages that are linked to the District pages must follow all District guidelines as outlined in the District AUP and these guidelines.
- Student work and posting of student information must comply with Policy and Regulation 2400.

Linkage Guidelines

- Links Permitted:
 - links to government institutions – i.e. DESE, NASA
 - links to educational websites – i.e. Scholastic, Follett
 - links to reference material, suitable for educational work – i.e. online dictionaries,
- Links Not Permitted:
 - no link to sites that are commercial in nature.
 - no links to inappropriate websites i.e. adult content, violence, illegal activities, or social-networking sites.
 - no links to personal webpages, or social-networking sites.
 - no links to search engines - i.e. Google, Yahoo

- no links to online journals, blogs, public discussion forums, or newsgroups.

VII. Social Media Guidelines

- Social Media refers to any usage of Web 2.0 technologies and sites such as forums, blogging, microblogging (ie. Twitter, plurk), photosharing (ie. Flickr), video sharing (ie. Youtube, Vimeo), networking (ie. Facebook, LinkedIn).
- Personal blogs should have clear disclaimers that the view expressed by the author in the blog is the author's alone and do not represent the views of the district.
- Information published should comply with the district's confidentiality policies.
- Be respectful to the district, other employees, and the community.
- Do not harass, cyberbully or cyberstalk anyone.
- Be mindful that an online presence reflects the district and one's profession.
- Remember to protect one's name, identity and reputation.
- Please remember with social media technologies that nothing is truly private.
- Personal use of social media during work time or on any district computers or resources is strictly prohibited.
- The district will maintain one Facebook account through the Community Relations Department for official use. No other staff member, district department, school, student organization or athletic team can have an official Facebook account representing the school district (ie. classrooms, clubs, teams, etc...). Any exceptions must be approved with the Superintendent.
- The district Technology Office will setup approved official district Twitter accounts for departments, schools, classrooms, activities or teams. Use of Twitter accounts should be in full compliance of district policies, regulation and procedures.

VIII. Agreement

- A. You must request access to the RPSD's technology resources. This access includes connections to computers through the Internet, which will connect you with educational resources all over the world. Please read the attached Acceptable Use Policy. In submitting a signed agreement, you accept the responsibility of using any of the RPSD's technology resources in an appropriate manner. Your signature indicates that you have read and agreed to this AUP. When you submit your signed agreement, it will be kept on file as a legal, binding document. In order to modify or rescind the agreement, you (if at least eighteen years of age) or your parent/guardian (if under eighteen years of age) must provide the Superintendent with a written request.

Raymore-Peculiar School District
EMPLOYEE Agreement for Access to Technology Resources

I, _____, accept and agree that:
(Print your name here)

- I have reviewed and understand the District’s Technology Acceptable Use Policy (AUP).
- I understand that the primary purpose of the Raymore-Peculiar School District’s technology resources is educational, and that the use of this technology is solely to support the educational objectives of the District.
- I understand that inappropriate behavior may lead to penalties including revoking or suspension of my access, disciplinary action, and/or legal action.
- I agree not to participate in the transfer of inappropriate or illegal materials (including those which may be considered treasonous or subversive) through the use of the Raymore-Peculiar School District’s technology resources. I understand that in some cases, the transfer of such material may result in legal action against me.
- I understand not to allow other individuals to use any account(s) assigned to me for network or Internet activities, nor will I give anyone my password(s).
- I understand that by requesting access to the Raymore-Peculiar School District’s technology resources, that this access includes connections to other computers through networks, e-mail, and the Internet.
- I understand that students are NOT allowed any access to technology resources without direct supervision.

I agree to release and indemnify the Raymore-Peculiar School District and all other organizations related to the Raymore Peculiar School District’s technology resources from any liability or damages that may result from any use of the District’s technology resources. In addition, I accept full responsibility and liability for the results of my actions with regards to the use of any technology resources. If I should violate any portion of this policy, I understand that I may be held financially liable for any costs incurred by the District to remedy the damage resulting from the violation(s).

Signed _____
(Sign your name here) (Print your name here)

Date _____ Grade/Dept _____
(Write the name of your school here)

Home telephone # _____ Work telephone # _____