Raymond Panthers 1:1 Student Guide

Raymond School District Mission Statement

Raymond School District is dedicated to providing a child-centered learning environment, expecting all students to learn and succeed. We commit to providing and utilizing a progressive, relevant curriculum encouraging all students to become responsible citizens prepared to meet the challenges of the future.

Table of Contents

1:1 Technology Student Expectations
As a learner I will…

1. Look after my laptop very carefully all of the time.
    a. Laptops will never be left unattended
    b. Laptops must be situated securely on the working surface
    c. Make sure the laptop is not subject to careless or malicious damage (i.e. as a result of horseplay)
    d. Take care when the laptop is transported that it is as secure as possible. Laptop MUST be carried with two hands when possible when transporting in a classroom and in a case when outside of a classroom. Use protective case when possible.
    e. Carry my laptop in the closed position with two hands in the classroom.
    f. Carry my laptop home in my laptop case when possible, outside of my backpack/book bag
2. Ensure that my laptop is charged every evening and ready for use the next day (i.e. plugging it in at home or making sure it is turned in at the end of the day).
3. Store my laptop in my locker on the top shelf when not in use (i.e. lunch, phy. Ed., etc.).
4. Print only after teacher gives permission.
5. Not decorate the laptop or carrying case and not allow it to be subject to graffiti.
6. Not install or download additional software without the permission of the IT department or teacher.
7. Be on the task assigned by my teacher at all times. Laptop will ONLY be used for educational purposes as directed by Raymond School District staff.
8. Only use web tools such as blogs, wikis, podcasts, social-bookmarking, multi-user role-playing environments, video games, and social networking authorized by my teacher.
9. Agree that all written and posted material on-line is appropriate and non-defamatory.
10. Not use the computer to bring harm to anyone else.
11. Not type profanity or otherwise offensive language.
12. Report to my teacher, school counselor, or administrator if I ever feel uncomfortable about an experience online including but not limited to receiving harassing messages or accidentally view any offensive or inappropriate content or being asked to meet someone I have met online without parental approval. I understand that my teacher is willing to help me and will not punish me as long as the rules are followed.
13. Use the Internet to search only areas appropriate to the school curriculum.
14. Only save material in my personal folders or to my laptop appropriate for educational use.
15. Not plagiarize from the internet.
16. Not share my passwords (my school network account, my e-mail account, my social networking account, etc.) with anyone else except my parents, teachers, school counselors, or administrators.
17. Not use a proxy or otherwise attempt to access Web sites or other forms of Internet content and communications technology that have been blocked from my school network.
18. Be prepared to be held accountable for my actions and for the loss of computer and/or laptop privileges if these expectations are violated.

TECHNOLOGY CODE OF CONDUCT

Offense Description	Disciplinary Actions 1st Offense	2nd Offense	3rd Offense
Level 1			
Internet Violations: Attempting to bypass filtering and/or security measures. Attempting to surf for inappropriate or non-academic items. Attempting to change filter settings. Accessing social media and networking that is non-academic. Playing games that do or do not bypass filtering. **Downloading Programs** **Production and Distribution of Inappropriate material** **Privacy** Attempting to hide computer activities. Attempting to hide, delete, or alter files or file types not belonging to the student. Revealing and/or sharing of account information. Attempting to access or use someone else's computer account information or profile **Use of inappropriate language**	*Minimum Action* Verbal Reprimand *Maximum Action* Detention	*Minimum Action* Detention *Maximum Action* Loss of computer or internet privilege	*Minimum Action* Detention *Maximum Action* Extended loss of computer/internet privileges and/or suspension

Level 2

For each offense in Level 2, the **minimum action** taken will be a detention and the **maximum action** taken will be suspension or expulsion based on the severity of the offense. Citations or legal charges may be issued.

Hardware

- Destruction of property
- Theft

Software

- Knowingly bringing in viruses
- Attempting to load programs to subvert function or security
- Improper use of computers to falsify documents or plagiarize
- Attempting to bypass security measures or access more privileged accounts
- Attempting to alter or block the proper operation or performance of the network
- Using school or other email inappropriately

Cyber bullying

Using electronic devices or social networking sites to intimidate, harass, or gossip by email, texting, posting or sending messages/photos

- Occurs during school hours
- Occurs using district technology
- Occurs beyond school hours but has a negative impact on the educational Environment for one or multiple students

Please not that intentional and/or willful damage caused to the laptop or laptop carrying case is subject to restitution. Students will be charged for any/all damage to the laptop.

Stakeholders' Roles, Responsibilities, & Guidelines

We understand that using Information Technology is an essential skill as well as a privilege. To protect student privacy and ensure safety, the following guidelines are to be followed:

District Responsibility

- Model appropriate use of technology.
- Keep abreast of current law in order to protect all students.
- Understand the Acceptable Use Policy (AUP) and enforce the terms.
- Maintain functionality of hardware, software, and networking to support student learning.
- Monitor student and staff use.
- Maintain devices that are safe to use.

Teacher Responsibility

- Model appropriate use of technology.
- Understand the Acceptable Use Policy (AUP) and enforce the terms. Ensure suggested sites are age-appropriate for student use.
- Monitor student creation of accounts within the classroom and student use of Internet and social media sites
- Be aware of and adhere to the federal Children's Online Privacy Protection Act laws and District Policies

Student Responsibility

- When creating accounts only provide first name and last initial. If asked to provide a birth date all students should use January 1st of their birth year. Students will not share personal, identifiable information. (i.e. last name, school or home address, etc)
- Students will use group/individual pictures of students that do not identify the individuals by name.
- Students will agree to use social media and content creation sites appropriately.
- Protect the laptops/netbooks from damage and theft per the *Student 1:1 Laptop Expectations*. Required precautions include the use of the protective case/sleeve when transporting the laptop to and from school. If the laptop is lost or stolen when outside of school grounds, it should be reported to the local police authorities and school personal immediately. Parents or guardians are financially responsible for any lost or stolen laptop that is not recovered in good working order by the authorities.
- Read and be familiar with the Acceptable Use Policy (AUP)

Parent/Guardian Responsibility

- Monitor student internet and social media use at home
- Contact teacher if there are any questions arise
- Parents/Guardians are encouraged to obtain their child's login and password in order to monitor their student's computer usage at home. If parents are unable to obtain passwords they should contact the school office or district IT office.
- When school issued laptops/netbooks are used at home it is recommended that they are used in a central location where supervision can be maintained.
- If damage is purposeful, or willful the parents or guardians will pay the full repair cost for the laptop, unless insurance through the Raymond School District has been purchased.

General Tips for Parents for Internet Safety

- Talk with your child often about online behavior, safety and security
- Set limits and expectations
- Monitor your child's computer use. Know their passwords and online profiles.
- Look into safeguarding programs and options that your online service provider may offer

Raymond School District
Acceptable Use Policy and Admin Guideline

7540.03-Student Network and Internet Acceptable Use and Safety

The District makes access to interconnected computer systems within the District as well as the Internet available to students to provide various means of accessing educational materials and opportunities.

The District's Internet system has a limited educational purpose and is not intended to serve as a public access service or a public forum. The Board of Education has the right to place restrictions on its use to assure that use of the District's computer system is in accord with its limited educational purpose. Student use of the District's computers, network and Internet services ("Network") will be governed by this policy, the related guidelines and the student disciplinary process.

The Board encourages students to utilize the Internet to develop the resource sharing, innovation, and communication skills and tools that are essential to both life and work. The instructional use of the Internet will be guided by the Board's policy on instructional materials.

The Internet is a global information and communication network that provides an incredible opportunity to bring previously unimaginable education and information resources to our students. The Internet connects computers and users in the District with computers and users worldwide. Through the Internet, students and staff can access up-to-date, highly relevant information that will enhance their learning and the education process. Further, the Internet provides students and staff with the opportunity to communicate with other people from throughout the world. Access to such an incredible quantity of information and resources brings with it, however, certain unique challenges.

First, and foremost, the Board may not be able to technologically limit access, to services through the Board's Internet connection to only those that have been authorized for the purpose of instruction, study and research related to the curriculum. Unlike in the past when educators and community members had the opportunity to review and screen materials to assess their appropriateness for supporting and enriching the curriculum according to adopted guidelines and reasonable selection criteria (taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students who would be exposed to them), access to the Internet, because it serves as a gateway to any publicly available file server in the world, will open classrooms and students to electronic information resources which have not been screened by educators for use by students of various ages.

The Board utilizes software and/or hardware to monitor online activity of students and to block/filter access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors. "Harmful to minors" is a term defined by the Communications Act of 1934 (47 U.S.C. 254(h)(7)) as any picture, image, graphic image file, or other visual depiction that:

A. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

B. depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals;

C. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

At the discretion of the Board or the District Administrator, the Technology Protection Measure may be configured to protect against access to other material considered inappropriate for students to access. The Technology Protection Measure may not be disabled at any time that students may be using the Network, if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection Act. The District Administrator or Technology Coordinator may temporarily or permanently unblock access to sites containing appropriate material, if access to such sites has been inappropriately blocked by the Technology Protection measure. The determination of whether material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the Technology Protection Measure.

The District Administrator or Technology Coordinator may disable the technology protection measure to enable access for bona fide research or other lawful purposes.

Parents are advised that a determined user may be able to gain access to services on the Internet that the Board has not authorized for educational purposes. In fact, it is impossible to guarantee students will not gain access through the Internet to information and communications that they and/or their parents/guardians may find inappropriate, offensive, objectionable or controversial. Parents assume risks by consenting to allow their child to participate in the use of the Internet. Parents of minors

are responsible for setting and conveying the standards that their children should follow when using the Internet. The Board supports and respects each family's right to decide whether to apply for independent student access to the Internet.

The District Administrator shall prepare guidelines which address students' safety and security while using e-mail, chat rooms, instant messaging and other forms of direct electronic communications, and prohibit disclosure of personal identification information of minors and unauthorized access (e.g., "hacking") and other unlawful activities by minors online.

Network and Internet access is provided as a tool for your education. The School District reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the School District and no user shall have any expectation of privacy regarding such materials.

Pursuant to Federal law, students shall receive education about the following:

A. safety and security while using e-mail, chat rooms, social media, and other forms of electronic communications;

B. the dangers inherent with the online disclosure of personally identifiable information; and,

C. the consequences of unauthorized access (e.g., "hacking"), cyberbullying, and other unlawful or inappropriate activities by students online.

Building principals are responsible for providing training so that Internet users under their supervision are knowledgeable about this policy and its accompanying guidelines. The Board expects that staff members will provide guidance and instruction to students in the appropriate use of the Internet. All Internet users (and their parents if they are minors) are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying guidelines.

Students and staff members are responsible for good behavior on the Board's computers/network and the Internet just as they are in classrooms, school hallways, and other school premises and school sponsored events. Communications on the Internet are often public in nature. General school rules for behavior and communication apply. The Board does not sanction any use of the Internet that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.

Students shall not access social media for personal use from the District’s network, but shall be permitted to access social media for educational use in accordance with their teacher’s approved plan for such use.

Users who disregard this policy and its accompanying guidelines may have their use privileges suspended or revoked, and disciplinary action taken against them. Users granted access to the Internet through the Board's computers assume personal responsibility and liability, both civil and criminal, for uses of the Internet not authorized by this Board policy and its accompanying guidelines.

The Board designates the District Administrator and Technology Coordinator as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to students' use of the Network.

H.R. 4577, P.L. 106-554, Children's Internet Protection Act of 2000
47 U.S.C. 254(h), (1), Communications Act of 1934, as amended
20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended
18 U.S.C. 2256
18 U.S.C. 1460
18 U.S.C. 2246

Revised 8/15/11
Revised 8/19/13

7540.03-Student Network and Internet Acceptable Use and Safety

Students are encouraged to use the Board's computers/network and Internet connection for educational purposes. Use of such resources is a privilege, not a right. Students must conduct themselves in a responsible, efficient, ethical, and legal manner. Unauthorized or inappropriate use, including any violation of these guidelines, may result in cancellation of the privilege, disciplinary action consistent with the Student Handbook, and/or civil or criminal liability (see Sec. 943.70, Wis. Stat. (Computer Crimes) and Sec. 947.0125, Wis. Stat. (Unlawful Use of Computerized Communication Systems)). Prior to accessing the Internet at school, students must sign the Student Network and Internet Acceptable Use and Safety Agreement. A minor student must also have the permission of his/her parent or guardian before accessing the Internet at school.

Smooth operation of the Board's Network relies upon users adhering to the following guidelines. The guidelines outlined below are provided so that users are aware of their responsibilities.

A. Students are responsible for their behavior and communication on the Internet.

B. Students may only access the Internet by using their assigned Internet/E-mail account. Use of another person's account/address/password is prohibited. Students may not allow other users to utilize their passwords.

C. Students may not intentionally seek information on, obtain copies of, or modify files, data, or passwords belonging to other users, or misrepresent other users on the network.

D. Students may not use the Internet to engage in "hacking" or other unlawful activities.

E. Transmission of any material in violation of any State or Federal law or regulation, or Board policy is prohibited.

F. Any use of the Internet for commercial purposes, advertising, or political lobbying is prohibited.

G. Students are expected to abide by the following generally-accepted rules of network etiquette:

   1. Be polite, courteous, and respectful in your messages to others. Use language appropriate to school situations in any communications made through the Board's computers/network. Do not use obscene, profane, vulgar, sexually explicit, defamatory, or abusive language in your messages.
   2. Never reveal names, addresses, phone numbers, or passwords of yourself or other students, family members, teachers, administrators, or other staff members while communicating on the Internet.
   3. Do not transmit pictures or other information that could be used to establish your identity without prior approval of a teacher and unless expressly authorized by your parent or guardian on the "Student Network and Internet Acceptable Use and Safety Agreement Form."
   4. Never agree to get together with someone you "meet" on-line without prior parent approval.
   5. Diligently delete old mail on a regular basis from the personal mail directory to avoid excessive use of the electronic mail disk space.

H. Use of the Internet to access, process, distribute, display, or print child pornography and other material that is obscene, objectionable, inappropriate, and/or harmful to minors is prohibited. For example, the following material is prohibited: material that appeals to a prurient interest in nudity, sex, and excretion; material that depicts, describes or represents in a patently offensive way with respect to what is suitable for minors an actual or simulated sexual act or sexual contact, actual or stimulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and material that lacks serious literary, artistic, political or scientific value as to minors. Offensive messages and pictures, inappropriate text files, or files dangerous to the integrity of the Board's computers/network (e.g., viruses) are also prohibited.

   To ensure that the Board's computer resources are not used for inappropriate purposes and consistent with the Children's Internet Protection Act, the Board has implemented technology protection measures on all computers with access to the Internet and World Wide Web that protect against access to visual depictions that are obscene, child pornography, and/or harmful to minors. These measures are operating at all times, and enable the Board to monitor and protect against access to the aforementioned visual depictions. We have additional and extensive systems and security mechanisms in place to ensure the security, integrity, and appropriateness of the data on our networks. We also rely on and respect each family's right to decide whether to allow their children access to the Internet and World Wide Web.

I. Malicious use of the Board's computers/network to develop programs that harass other users or infiltrate a computer or computer system and/or damage the software components of a computer or computing system is prohibited.

Students may not use the Board's computers/network in such a way that would disrupt their use by others. Students must avoid intentionally wasting limited resources.

J. All communications and information accessible via the Internet should be assumed to be private property (i.e. copyrighted and/or trademarked). All copyright issues regarding software, information, and attributions of authorship must be respected.

K. Downloading of information onto the Board's hard drives is prohibited; all downloads must be to floppy disk. If a student transfers files from information services and electronic bulletin board services, the student must check the file with a virus-detection program before opening the file for use. Only public domain software may be downloaded. If a student transfers a file or software program that infects the Network with a virus and causes damage, the student will be liable for any and all repair costs to make the Network once again fully operational.

L. Students must secure prior approval from the Technology Coordinator before joining a Listserv (electronic mailing lists) and should not post personal messages on bulletin boards or "Listservs."

M. Students are prohibited from accessing or participating in on-line "chat rooms" or other forms of direct electronic communication (other than e-mail) without prior approval from a teacher or Technology Coordinator. All such authorized communications must comply with these guidelines.

N. The Board has software and systems in place that monitor and record all Internet, World Wide Web, and computer usage. The Board wants users to be aware that security systems are capable of recording, for each and every user, each World Wide Web site visit, the amount of time spent actively using the World Wide Web, each chat, news group access, e-mail message, and every file transfer into and out of our internal networks to the Internet. No District student or employee should have any expectation of privacy as to his/her Internet or World Wide Web usage, or the privacy of any electronic mail message, file, download, note, or other data stored on or transmitted or received through any Board computing facility. The Board reserves the right to review computing activity and analyze usage patterns, and may choose to publicize this data to assure that the Board's computing resources are devoted to maintaining the highest standards of educational benefit and employee productivity. Messages relating to or in support of illegal activities will be reported to the appropriate authorities. The use of passwords does not guarantee confidentiality, and the Board retains the right to access information in spite of a password.

O. Use of the Internet and any information procured from the Internet is at the student's own risk. The Board is not responsible for any damage a user suffers, including loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions. The Board is not responsible for the accuracy or quality of information obtained through its services. Information (including text, graphics, audio, video, etc.) from Internet sources used in student papers, reports, and projects should be cited the same as references to printed materials.

P. Disclosure, use, and/or dissemination of personal identification information of minors via the Internet is prohibited, except as expressly authorized by the minor student's parent/guardian on the "Student Network and Internet Acceptable Use and Safety Agreement Form."

Q. Proprietary rights in the design of web sites hosted on the Board's servers remains at all times with the Board.

943.70, Wis. Stats.
947.0125, Wis. Stats.
Family Educational Rights and Privacy Act of 1974, as amended

H.R. 4577, P.L. 106-554, Children's Internet Protection Act of 2000
47 U.S.C. 254(h), (1), Communications Act of 1934, as amended
20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended
18 U.S.C. 2256
18 U.S.C. 1460
18 U.S.C. 2246

Student User Names and Passwords
Reference Sheet

Chromebook
Access: Open screen
User Name: Raymond School Gmail
Password: (on an individual basis)

Gmail
Access: Sign in through Google Chrome
*be sure when using a desktop in the Media Center or other classroom, sign out of your Gmail/Google account before logging off
User Name: First four digits of last name followed by first three digits of first name
(example: smitjoe@raymond.k12.wi.us)
Password: Generic password to begin the year (can be reset by IT office)

General Maintenance of Device & Troubleshooting

General Maintenance

Turning On / Off:

When turning on…

- Open the screen and press the "Power" button
- Wait for the computer to boot up, then log in

When turning off…

- Double check to save any documents / close all open programs
- For Chromebooks click battery icon in lower right hand corner, then choose shutdown icon

Allow device to completely shut down before closing the screen! *(Otherwise it may go into sleep mode and continue to use battery rather than shut down)*

Storage When Not In Use:

Within a classroom…

- Shut down and store in district provided bag
- If the classroom teacher has a power source available and your power is low, plug it in!

Before lunch…

- Shut down and store in locker in district provided bag
- **REMEMBER: Nothing is to be stacked on top**

End of the day…

- Take device home & charge the battery
- Laptops should be transported home outside of a backpack in the district provided bag

Battery Life / Charging:

Checking battery life…

- Scroll your cursor over the battery icon in the toolbar on the bottom right-hand side of your screen
- If your battery gets low (below 15% is probably less than an hour left), plan to recharge as soon as a possible
- Let your battery drain to a low percentage before recharging; this will prolong the life of the battery

Troubleshooting

Issue:

1. **Chromebook will not turn on or boot up**

Teacher:

-Try plugging in device to make to rule out a dead battery.
-If battery isn't the issue give student pass to take their laptop to the IT office *immediately* to report the issue and file a ticket with tech support.
-If possible, provide the student another computer. If no computer is available, student can hand write planned activity and/or work on an alternate activity if appropriate based on teacher expectations and class procedures.

Student:

-Try plugging in device to rule out a dead battery
-Report issue to teacher. Teacher will provide a pass to the IT office and/or file a ticket with tech support.
-Take laptop to the IT office and report the issue.
-Return to class and follow teacher directive for alternate activity as needed. When possible another computer may be available for use, however, if a computer is not available activities may need to be completed by hand or converted to an electronic version at a later date.

2. **Able to access some programs, but others do not work (i.e. cannot establish wireless connection, cannot print, etc.)**

Teacher:

-If student reports an issue that is not preventing their ability to complete their work for class, please have student take their Chromebook to the IT department at the end of the class period during passing time and file a ticket with tech support.
-If the issue is impeding the student's ability to complete their work for class and basic troubleshooting in class does not work, please give student a pass to the IT office when convenient to report the issue.

Student:

-Attempt to troubleshoot on your own
-Report the issue to your teacher
-Go to IT office when the teacher issues a pass or at the end of the period.
-Return to class and follow teacher directive for alternate activity as needed. When possible another computer may be available for use, however, if a computer is not available activities may need to be completed by hand or converted to an electronic version at a later date.

3. **Laptop is being fixed, not charged, forgot at home, or otherwise unable to be used**

Teacher:

-Student may check out a spare
-If another computer is available, you may allow the student to use an alternate computer if the use follows your teacher expectations and class procedures

Student:

-Report to the teacher at the beginning of the period that you are without a device
-As needed, follow teacher directive for alternate activities. When possible another computer may be available for use, however, if a computer is not available activities may need to be completed by hand or converted to an electronic version on the student's time at a later date.

Email Etiquette & Gmail

Reference Board Policy 7540.06

Policy

All messages sent or received via the Raymond School District e-mail system are the property of the district and may be reviewed, accessed, and disclosed as deemed necessary by the district.

Transmitting spam messages, chain letters, or inappropriate e-mail may be considered a violation of district policies and procedures and may result in disciplinary action.

Etiquette

E-mail Structure

- Addressing the recipient and having a proper closing
- Be specific in the subject line regarding the nature of the e-mail. Do not leave the subject line blank.
- Write in complete sentences, but also be concise - no text lingo
- E-mails should never contain vulgar or inappropriate language
- Be mindful of the tone of voice in the e-mail. Written language can easily be misinterpreted. Face to face communication may be needed at times.
- DO NOT TYPE IN ALL CAPS, bold print, multiple colors, etc.

Reminders

- Spam messages or chain letters should not be sent or forwarded
- E-mails are not private. If a comment is inappropriate to say, it is inappropriate to write in an e-mail.
- DO NOT "REPLY ALL" unless it is appropriate for a group project or class assignment. Replying to an inappropriate message using school email may result in disciplinary action.
- If you receive an inappropriate or harassing e-mail, report it to a teacher, counselor, or administrator. Do **not** replay or respond to an inappropriate or harassing e-mail.
- Reply to e-mails in a timely fashion. Your classmates or teachers may be depending on your response to complete their work.
- School e-mail is **not** to be used for personal communication or social networking unless otherwise okayed by your teacher, administer, or the IT office
- Any e-mails sent can be retrieved even after deleted and are the property of the Raymond School District
- Do not share your passwords
- Make sure you always log out after finished

Username: first four digits of last name followed by first three digits of first name @raymond.k12.wi.us
(smitjoe@raymond.k12.wi.us)

Password: Use generic password at the beginning of the year. You will be prompted to change your password. New students should contact their teacher or stop by the IT department to get their password to login the first time