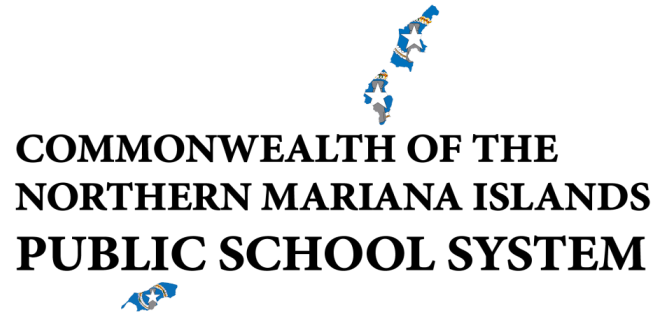




**CNMI  
PSS**



**CNMI Public School System Employee/Contractor  
/Student and Parent Acceptable Use Agreement**

## **Information and Technology Security Agreements**

**Please read this agreement carefully. Sign and date the last page and return to the State Infrastructure Technology Department. Keep pages 1 through 10 for future reference.**

### **Mandatory Review**

To educate CNMI PSS staff/contractors on proper computer/network/Internet use and conduct, users are required to review these guidelines at the beginning of each school year. All CNMI PSS staff/contractors shall be required to acknowledge receipt and understanding of all administrative regulations governing the use of the system and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines. These guidelines are included in the CNMI PSS's Employee Handbook. "Staff/Contractors" shall be used in this document to refer to all CNMI PSS employees/contractors.

### **Definition of CNMI PSS Technology System**

CNMI PSS computer systems and networks (system) are any configuration of hardware and software. The system includes but is not limited to the following:

- Telephones, cellular telephones, and voicemail technologies
- Email accounts
- Fax machines
- Copiers
- Servers
- Computer hardware and peripherals
- Software including operating system software and application software
- Digitized information including stored text, data files, email, digital images, and video and audio files
- Internally or externally accessed databases, applications, tools (Internet or server-based)
- PSS provided Internet access
- PSS filtered Wi-Fi
- Virtual environments
- New technologies as they become available.

### **Internet/Network/Email Acceptable Use Agreement**

As an employee, student and contractor of CNMI PSS, you are being given access to the CNMI PSS network system. You will be given a unique identification and password that is your responsibility to keep secure. Do not reveal or allow any person to use your ID and password. If you suspect someone may know your password(s), please contact the State Infrastructure Technology Helpdesk for assistance.

Additionally, you will have Internet access through the CNMI PSS network. The Internet offers vast, diverse, and unique resources. Our goal in providing this service is to promote educational excellence in our schools by facilitating resource sharing, innovation, and communication. With this opportunity comes responsibility. It is important that you read the CNMI PSS Board of Education Regulations on [www.cnmilaw.org](http://www.cnmilaw.org) (§ 60-30.2-370 Internet Usage and § 60-20-540 Library, Media, and Technology Services; Student Internet Usage), this agreement form, and ask questions if you need help in understanding them.

Please note that the Internet is a network of many types of communication and information systems. It is possible that you may run across some material you might find objectionable. While the District will use filtering technology to restrict access to such material, it is not possible to absolutely prevent such access. It will be your responsibility to follow the rules for appropriate use. In the same respect, email received from outside sources cannot be fully controlled. SPAM, or unsolicited email, is one of the single most widespread problems affecting technology resources and the Internet today. Please use caution when opening emails from unknown senders and never give out your email address unless you know the source.

In order to minimize obstacles such as unwanted spam, file-sharing applications, viruses, and spyware, the CNMI PSS State Infrastructure Technology Department has implemented processes to monitor these issues creating a more efficient delivery of technology. Be advised that these processes while providing quality service can reveal evidence of inappropriate computer usage or access to inappropriate sites/programs. Inappropriate use will result in the loss of the privilege of this educational and administrative tool. In addition, other disciplinary or legal action may occur, in accordance with CNMI PSS policies and applicable laws.

The smooth operation of the CNMI PSS network relies upon the proper conduct of the end-users who must adhere to strict guidelines. These guidelines are provided so that users are aware of the responsibilities they are about to acquire. In general, this requires efficient, ethical and legal utilization of the network resources

### **Limitation of Liability**

1) CNMI PSS makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the CNMI PSS system will be error-free or without defect. CNMI PSS will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. CNMI PSS is not responsible for the accuracy or quality of the information obtained through or stored on the system. CNMI PSS will not be responsible for the financial obligations arising from a user's unauthorized use of the system.

2) Users will indemnify and hold the department and its respective district harmless from any losses sustained by the department as a result of intentional misuse of the system by the user.

### **Future Updates and Changes to CNMI PSS's Acceptable Use Agreement for Internet/Network Access and Email Use:**

- An employee's/contractor's signature acceptance of the AUA implies agreement to any and all future updates to the CNMI PSS AUA Policy. The employee/contractor must notify, in writing, the Director of Infrastructure Technology within 15 business days of the agreement update release date if there is any disagreement or conflict.
- All updates to the AUA Policy and Agreement will be emailed to all Principals and it will be the responsibility of the Principals to distribute to their respective school employees/contractors.
- It is the employee's/contractor's responsibility to review the change/update for acceptance.

### **Rules for Appropriate Use:**

**1) Acceptable Use** - The purpose of the backbone networks making up the Internet is to support research and education in and among academic institutions by providing access to unique resources and the opportunity for collaborative work. The use of the Internet must be in support of education and research consistent with the educational goals of the CNMI Public School System. The use of other organization's

networks or computing resources must comply with the rules defined for that network. Transmission of any material in violation of any national or state regulation is prohibited. This includes, but is not limited to copyrighted material, threatening or obscene material, or material protected by trade secrets.

**2) Privileges - The use of the Internet is a privilege, not a right, and inappropriate use will result in a possible cancellation of those privileges.** The Director of State Infrastructure Technology, in accordance with the Commissioner of Education, will deem what constitutes inappropriate use and this decision of what constitutes inappropriate use is final. This document and any other applicable district policy or law governs any further consequence related to inappropriate use. The administration, faculty, and staff of the CNMI Public School System may request the Director of State Infrastructure Technology to deny, revoke, or suspend specific user access. Also, the Director of State Infrastructure Technology may suspend or revoke access at any time for inappropriate use.

### **3) Rules for Appropriate Email Use:**

Email is a privilege and is provided for the purpose of exchanging information consistent with the mission of the CNMI Public School System. The following guidelines will ensure the proper use of electronic mail and define the responsibilities associated with the use of our computing resources.

- Messages relating to or in support of illegal activities are prohibited.
- The privacy of an email message is not guaranteed.
- Confidential information should not be sent by email.
- Users are not permitted to transmit, receive, submit, or publish any defamatory, inaccurate, abusive, obscene, profane, sexually-oriented, threatening, offensive, or illegal material. Although users possibly cannot control all emails received, it is the user's responsibility to delete any email and/or attachments containing inappropriate content as soon as possible. Users may choose to consult with the Director of Infrastructure Technology for options to stop unsolicited inappropriate email. Users that follow the instructions to remove "received" inappropriate email will not be subject to disciplinary action.
- Email messages are subject to CNMI PSS review at any time.
- Email should not be used for official record purposes; however, please understand that email can be used for legal purposes, is considered a legal document, and may be subject to the Public Information Act.
- Email cannot be used for the sale of private or commercial offerings.
- Email cannot be used to solicit products or services.
- Email cannot be used for political or religious purposes.
- Email language should not be rude, angry, or inflammatory.
- Email chain letters are not allowed.
- Bulk (Broadcast) emails must be approved. Permission for Bulk (Broadcast) mailing must be sent to the COE office. Please see OAS SOP for more information.
- Email Signatures should follow a standard format listed below. Please refrain from using flashy Images, Gifs, or Quotes that may distract or confuse the intended recipient(s) of the email.
  - Employee's/Contractor's Legal name
  - Job Title(s)
  - Contact information
  - Award or honor (e.g., Teacher of the Year, etc.)
  - School or Department

- o CNMI District Website

#### 4) Internet/Network Acceptable Use:

- CNMI PSS's Internet filtering device is not 100% accurate. The District can make no guarantee that all inappropriate content will be filtered. New websites are posted on the web every day; no filtering device will capture all or not block appropriate sites. If you access an inappropriate site, notify the Infrastructure Technology Department so it can be added to the filter. If you need access to a blocked site (for instructional or school business purposes only), you may submit a request to the Infrastructure Technology Department for review via the helpdesk system. Only sites used for work-related purposes will be considered for unblocking.
- The use of any tool to circumvent the internet filter is strictly prohibited. This includes using proxy servers or accessing other websites that allow you to bypass filters placed within our network.
- Users must respect all copyright laws that protect software owners, artists, and writers. Plagiarism will not be tolerated.
- Posting of personal addresses or phone numbers of students or colleagues is prohibited. Posting of student pictures with full names is prohibited.
- Physical or electronic tampering with computer resources will result in the cancellation of privileges and possible disciplinary action.
- The deletion of any system operating file is strictly prohibited. No system files shall be deleted at any time.
- All suspected viruses must be reported to the Infrastructure Technology Department. Users shall not attempt to remove any suspected virus without direction from the Infrastructure Technology Department.
- Immediately notify the Infrastructure Technology Department if inappropriate material is accessed unintentionally.
- The following practices using CNMI PSS wide-area networks shall be prohibited:
  - ❖ any use of computing resources for commercial purposes, product advertising, political lobbying, or political campaigning
  - ❖ any use that disrupts the educational and administrative goals of the District
  - ❖ any use of a network account by anyone but the authorized owner of the account
  - ❖ access to materials that have been deemed inappropriate for school use
  - ❖ The use of any tool to circumvent the internet filter is strictly prohibited. This includes using proxy servers or accessing other websites that allow you to bypass filters placed within our network.
- Downloading from the Internet: Staff and students shall not download or install any commercial software, shareware or freeware onto any device unless they have written permission from the State Infrastructure Technology Department.
- Downloading of browser-based apps and extensions: Apps and extensions for educational use are permitted. While staff and students have the capability to install apps and extensions to their devices, consideration needs to be given to each app/extension's Terms of Service and Privacy Policy. Specific attention should be paid to age restrictions and the creation of accounts in accordance with CIPA/COPPA. The same consideration should be given to all online resources for educational use.
- Downloading of content or music clips by students shall be monitored at all times, must be only for direct instructional purposes, and must be legal.
- Audio or Video Streaming from Internet: Staff and students shall not access the Internet for streaming (live) audio (music, etc.); or video (clips, movies, etc.) unless the content is approved/authorized by the Infrastructure Technology Department.

- Free or paid personal subscription streaming services will be filtered on district devices. Such services should not be used for educational purposes as they violate an individual's service agreement.
- Internet file-sharing services, also called Peer-to-Peer Networks are strictly prohibited and violations may result in disciplinary action.
- Personal portable devices (flash drives, portable hard drives, etc.) may be attached to a district computer. Data on the personal storage device is subject to review, inspection, and confiscation by the Director of Infrastructure Technology or other authorized district personnel.
- **Social media, if used during contract hours, should be used only to promote district initiatives, vision, and mission.**

**5) Security** - Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on the Internet, you must notify the Director of State Infrastructure Technology. Do not demonstrate the problem to other users. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the Internet.

For the security of your personal data and student data accessible from your networked computer, you should always

- log out of any systems,
- Lock your computer
- Log out of your computer when you are not sitting in front of it.
- Passwords should be kept secure at all times. Do not share passwords with other employees/people/students or post it in an accessible location.

**6) Vandalism** -Vandalism will result in cancellation of privileges, disciplinary action, and prosecution to the fullest extent of the law. Vandalism is defined as any malicious attempt to harm or destroy user data, application systems, Internet data, and systems that are connected to any of the Internet or network backbones. This includes, but is not limited to, the uploading or creation of computer viruses.

**7) CNMI PSS makes no warranties of any kind**, whether expressed or implied, for the service it is providing. CNMI PSS will not be responsible for any damages suffered. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or user errors or omissions. Use of any information obtained via the Internet is at your own risk. CNMI PSS specifically denies any responsibility for the accuracy or quality of information obtained through its services.

#### **Consequences for Inappropriate Internet/Network or Email Use:**

- Formal warning from immediate supervisor, Director of State Infrastructure Technology, or Commissioner of Education
- Suspension of access to Internet or Email
- Revocation of your computer system account
- Other disciplinary or legal action, in accordance with CNMI PSS's policies and applicable laws

---

**The required signature(s) on the following page is (are) legally binding and indicates the party (parties) who signed has (have) read the terms and conditions carefully and understand(s) their significance. Please sign the area that is applicable to you as a staff, contractor, student, or parent.**

### ***Employee Information and Technology Security Agreement***

I acknowledge that PSS information and technology security policies, guidelines, and procedures have been made available to me for adequate review and consideration. I also certify that I have been given ample opportunity to have any and all questions about my responsibilities addressed. I am, therefore, aware that I am accountable for information and technology security procedures as they govern the acceptable performance of my job. I understand that failure to abide by any and all policies, guidelines, and procedures can result in organizational, civil, or criminal action and/or the termination of my employment.

Signature: \_\_\_\_\_ Printed Name: \_\_\_\_\_

Job Title: \_\_\_\_\_ Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

\_\_\_\_\_

### ***Contractor/Consultant/Outsider Information and Technology Security Agreement***

I acknowledge that PSS has provided me with adequate time to review and consider the information and technology security policies, guidelines, and procedures it deems applicable to responsibilities I am undertaking on behalf of PSS, regardless of my employment status. I also certify that I have been given ample opportunity to have any and all questions about my responsibilities addressed. I am, therefore, aware that I am accountable for those information and technology security procedures as they relate to my work for, or on the behalf of, [name of organization]. I understand that failure to abide by any and all policies, guidelines, and procedures can result in organizational, civil, or criminal action and/or the termination of my relationship with PSS.

Signature: \_\_\_\_\_ Printed Name: \_\_\_\_\_

Affiliation: \_\_\_\_\_ Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

## High School Student Guidelines for Acceptable Internet Use\*

Access to computer, network, and Internet equipment and software at PSS offers students an almost unlimited source of resources and information to support their educational development. Under staff supervision, students will have the privilege of searching the Internet for expert resources, communicating with other students from around the world, and participating in various distance-learning activities. But with the use of these powerful tools comes great responsibility. Access to these resources is a privilege, not a right. Students are advised that some Internet sites may contain offensive or inappropriate information, messages, and pictures for an educational setting. PSS does not condone or permit the use of such material. Therefore, access to the Internet is granted only on the condition that a student agrees to be accountable for appropriate use of these resources. In addition to all information and technology security policies, guidelines, and procedures that govern computer and network use at PSS. The following statements guide acceptable use of Internet resources by all high school students:

1. Students may not use equipment or facilities in a way that is inconsistent with the general rules of conduct that govern student behavior at PSS.
2. Students may not damage or mistreat equipment or facilities under any circumstances.
3. Students may not intentionally waste computer resources.
4. Students may not employ the network for personal financial gain or commercial purposes.
5. Students may not violate regulations prescribed by the network provider.
6. Students may not engage in practices that threaten the integrity of the network (e.g., knowingly download files that contain a virus).
7. Students may not write, use, send, download, or display obscene, threatening, harassing, or otherwise offensive messages or pictures, including pornography.
8. Students may not use the equipment or network for any illegal activities, including the violation of copyright laws and/or software piracy.
9. Students may not load or copy any software or other programs to or from organizational equipment.
10. Students may not use anyone else's password, nor may they share their password with others.
11. Students may not trespass into or in any way alter anyone else's folders, documents, or files.
12. Students may not disclose anyone's personal information (e.g., address, phone number, or confidential information), including their own or that belonging to a fellow student, community members and families, or staff member.

Students should be advised that in an effort to maintain system integrity and to ensure responsible use, files and communications can and will be monitored. *Students should not under any circumstances expect that messages or files that are created, modified, transmitted, received, or stored on organizational equipment are private.* Students who violate any of the above conditions will be subject to the suspension or termination of their Internet and computing privileges, as well as other disciplinary action as determined appropriate by school officials.

Student: "I have read these Student Guidelines for Acceptable Internet Use and agree to use the Internet and all associated equipment and information in a way that is consistent with these policies. I understand that failure to do so will result in the loss of my Internet privileges and/or other disciplinary action as deemed appropriate by school officials."

**Signature:** \_\_\_\_\_

**Printed Name:** \_\_\_\_\_

**Date:** \_\_\_\_/\_\_\_\_/\_\_\_\_



**\*This agreement should be accompanied by a signed and dated *Parent/Guardian Internet Permission Letter*.**

***Elementary, Middle, and Junior High School Student Guidelines for Acceptable Internet Use\****

Access to the Internet is offered to help students learn. With the help of teachers, the Internet can be used for researching, studying, and communicating. But the Internet also includes some information that is not appropriate for students and the school environment. Therefore, students must agree to behave properly when using this powerful learning tool. The following rules should help a student understand what type of behavior is expected of Internet users.

1. Students must be kind and polite when using the Internet.
2. Students must use Internet equipment only for school-related activities.
3. Students may use the Internet only when they have permission from a teacher.
4. Students should not damage or mistreat computer equipment under any circumstances. This includes trying to "fix" plugs, cables, or other parts of the equipment. Leave that to your teacher.
5. Students should not access files that do not belong to them.
6. Students should not copy, download, or install any software or programs to or from school computers.
7. Students must not write, send, download, or display obscene, threatening, harassing, or otherwise harmful messages or pictures.
8. Students must not share their personal address, phone number, or any other contact information over the Internet. They must not share information about other people either, including friends, fellow students, or teachers.
9. Students should be aware that e-mail and Internet use can and will be monitored and therefore is not private.
10. Students must obey all rules that normally govern their behavior at school when using the Internet.

Student: "I have read or have read these Student Guidelines for Acceptable Internet Use and agree to use the Internet in a way that is consistent with these policies. I understand that failure to do so will result in the loss of my Internet privileges and/or other disciplinary action as deemed appropriate by school officials."

Student Signature: \_\_\_\_\_

Printed Name: \_\_\_\_\_ Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

**\*This agreement should be accompanied by a signed and dated *Parent/Guardian Internet Permission Letter***

Parent/Guardian Internet Permission Letter\*

Dear Parent/Guardian,

We are pleased to offer students at PSS access to the Internet. The Internet is a global computer network that is used by educators, students, government, business, and a host of other organizations and individuals to communicate electronically. As a learning resource, the Internet is similar to books, magazines, video, CD-ROM, and other information sources, except that it quite literally enables students to explore countless numbers of computers, networks, libraries, and databases from throughout the world. Use of the Internet for educational purposes will assist students in identifying resources, gathering information, and developing the technical skills they will need for life and work in the twenty-first century.

It must be made clear, however, that although your child's use of the Internet will be supervised, we cannot guarantee that a student will not be able to access information that you might consider to be objectionable. Therefore, it is imperative that both students and their parents be aware of each individual student's responsibility for ethical and appropriate Internet use. Just as students are expected to behave properly in the classroom and school hallways, they will also be required to behave responsibly while using school computers and networks. Technical resources are provided to help students meet their information needs within the context of teacher-planned assignments and school-sponsored activities. Access to these resources, however, is a privilege, not a right. It is permitted only on the condition that a student agrees to act in a responsible manner. School staff reserve the right to suspend or terminate the use of the Internet by any student who violates these policies. Similarly, Internet use is subject to all policies and regulations that govern student behavior in other school activities.

Please review the attached Student Guidelines for Acceptable Internet Use agreement that your child will be required to read and sign before being granted Internet access. We encourage you to take advantage of this opportunity to discuss your family's values with your child and how they, too, should affect Internet use. Please feel free to contact PSS State Infrastructure Technology Department at (670)322-1238 if you have any questions about Internet use or Internet policies at PSS. You are not required to grant permission for your child to access the Internet, but we firmly believe that Internet use in an approved educational setting, with specific educational objectives, and under appropriate supervision will prove to be a positive learning experience for your child.

Parent/Guardian: "I have read this letter and the Student Guidelines for Acceptable Internet Use, and give permission for my son/daughter to use the Internet at PSS."

Parent/Guardian Signature: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

---

Student: "I have read or have read the Student Guidelines for Acceptable Internet Use as attached and agree to use the Internet in a way that is consistent with these policies. I understand that failure to abide by these policies will result in the loss of my Internet privileges and/or other disciplinary action as deemed appropriate by school officials."

Student Signature: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

**\*Any *minor* should present written permission from a parent/guardian before receiving access to the Internet.**