



CNMI Public School System Employee/Agent Acceptable Use Agreement For Internet/Network Access and Email Use

Please read this agreement carefully. Sign and date the last page and return to the Human Resources Department. Keep pages 1 through 7 for future reference.

Mandatory Review

To educate CNMI PSS staff 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 shall be required to acknowledge receipt and understanding of all administrative regulations governing 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" shall be used in this document to refer to all CNMI PSS employees.

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 or agent 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 Infrastructure Technology Helpdesk for assistance.

Additionally, you will have Internet access through 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 Technology policy, 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 email 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 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 of 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 user.

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

- An employee's signature acceptance of the AUA implies agreement to any and all future updates to the CNMI PSS AUA Policy. The employee 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.
- It is the employee'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. 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 secret.

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 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 Infrastructure Technology to deny, revoke, or suspend specific user access. Also, the Director of 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 email 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 Legal name
 - Job Title(s)
 - Award or honor (e.g., Teacher of the Year, etc.)
 - School or Department

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.

DRAFT

- 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 cancellation of privileges and possible disciplinary action.
- 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 Infrastructure Technology Department. Users shall not attempt to remove any suspected virus without direction from the Infrastructure Technology Department.
- Immediately notify 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 of materials that has been deemed inappropriate for school use
 - 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 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 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 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 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.

1) 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 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.

**CNMI Public School System
Acceptable Use Agreement
For Internet/Network Access and Email Use**

I have read the CNMI PSS Acceptable Use Agreement for Internet/Network Access and Email Use and agree to abide by its provisions and to promote the agreement in student usage. I understand that my computer use is not private and that the CNMI PSS monitors all network activity. I understand that the CNMI PSS's Internet, Network, and Email system is a privilege and violation of the provisions is unethical and may result in access to the system being revoked and/or disciplinary/legal action being taken.

With regard to all future AUA update releases from Technology Services, I understand that I am responsible for notifying the Director of Infrastructure Technology in writing within 15 business days of AUA update release date if I have any issue with the current update.

I hereby release CNMI PSS, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use of, or inability to use, the system, including, without limitation, the type of damages identified in the CNMI PSS's policy and SOPs.

Employee Number: _____

Employee's Printed Name: _____

Employee's Signature: _____ Date: _____