TECHNOLOGY ACCEPTABLE USE POLICY FOR SCHOOL EMPLOYEES

PURPOSE

This policy provides the procedures, rules, guidelines and codes of conduct for the use of the technology and information networks at Plumas Lake Elementary School District (PLESD). Use of such technology is a necessary, innate element of the PLESD educational mission, but technology is provided to staff and students as a privilege, not a right. PLESD seeks to protect, encourage and enhance the legitimate uses of technology by placing fair limitations on such use and sanctions for those who abuse the privilege. The reduction of computer abuse provides adequate resources for users with legitimate needs.

SUMMARY

Public technology that includes but is not limited to computers, wireless & LAN access, electronic mail, Internet access, Telephone/Voice Mail systems, printing devices and all other forms of instructional, networking and communication tools are provided a service by PLESD to teachers, staff, and administrators ("employees") at their respective locations. Use of these technologies is a privilege, not a right. Employees are expected to observe the following:

- All users are required to be good technology citizens by refraining from activities that annoy others, disrupt the educational experiences of their peers, or can be considered as illegal, immoral and/or unprofessional conduct.

The employee is ultimately responsible for his/her actions in accessing technology at PLESD. Failure to comply with the guidelines of technology use (as stated either in this document or in the PLESD Board Policy Manual) may result in the loss of access privileges and/or appropriate disciplinary action. Severe violations may result in civil or criminal action under the California Revised Statutes or Federal Law.

OWNERSHIP

All hardware, software, documents and data on retrievable medium residing on the PLESD network or are saved to file management systems including, but not limited to, network drives, floppy disks, hard-drives, CD-ROMs, or zip drives that are resident on PLESD equipment, are and shall remain the property of PLESD. PLESD administration reserves the right to confiscate, remove, search or otherwise investigate any of the above mentioned items at its discretion.

COMPUTER USE

Inappropriate use of any computer or the PLESD network can be a severe offense. Please note that it is a violation of PLESD policy to:

1. Duplicate copyrighted software provided by PLESD. It is a criminal offense to copy ANY software that is protected by copyright, unless such copying is expressly provided for within the copyright agreement, and PLESD will treat it as such.

2. Use PLESD' licensed software in a manner inconsistent with the licensing agreement. Information on licenses is available from the Technology Department ("Tech")

3. Copy, rename, alter, examine, install or delete the files or programs of another person or PLESD except in the case of Tech personnel or their agents who are troubleshooting or otherwise repairing a computer.

4. Use a computer or PLESD' network to annoy others including, but not limited to, sending offensive messages or intentionally causing a computer system or network to crash.

5. Use a computer for non-school-related activities including, but not limited to, personal or private business (with the limited exception of using personal email during breaks such as lunch or non-working times). Except in extraordinary situations, all work-related email should be transmitted using PLESD-issued email accounts. Any use

of personal email during working hours must meet the same standards as established throughout this document.

6. Create, disseminate, or run a self-replication program (virus, worm, or any program that inhibits operation of any computer or network whether it is destructive or not) or distributing large quantities of information that overwhelm any network including but not limited to chain letters, network games, inappropriate use of the "All Users" email address, mass copying of files, and so on.

7. Fail to consult with TD before making any technology purchases, downloads, updates or installations. It is a violation to purchase, download, install or use software, hardware, applications and/or peripherals on district equipment and networks that have not been expressly approved by the Director of Technology. All purchases and downloads (including those with an official PLESD purchase order) must be reviewed and approved by TD. Further, prior to purchase, users are responsible for forwarding the appropriate technical information to TD for their review and assessment. For all technology-related purchases, a copy of the license agreement must be forwarded to TD and the building administrator for tracking and audit purposes.

8. Download, install or run executable applications and software from the Internet, including the use of proxy servers to bypass the PLESD "Content Filter" to run. Use of any proxy server to bypass the PLESD Content Filter (as required by the Children's Internet Protection Act – CIPA) is considered a severe violation. Only TD may authorize the installation of technology purchases and, in most cases, only TD personnel are permitted to install such technology purchases.

9. Install personally purchased computers, hardware, software or peripherals (such as printers and scanners) on PLESD computers or the PLESD network with the limited exception of the wireless network described below. The Director of Technology may approve installation of personally-purchased software if requested by a building administrator AND TD determines it to be compatible with PLESD systems. If permission is attained, then a copy of the license agreement and the installation media must be housed with the administrator of that building for audit purposes.

10. Access the PLESD network and programs with personal computers unless such programs are made available by TD (such as the web-based email server or the web-based version of JMAC). Personal computers may not be tied into the PLESD network, either through wireless, VPN or LAN connections EXCEPT with the express permission of the Superintendent or the Director of Technology, and with security devices installed by TD. Further, the use of that computer will be subject to the policies and procedures outlines in this document.

11. Use portable storage devices, Internet drop boxes or off-site network storage sites to access programs, files and applications that might otherwise be blocked by the CIPA Content Filter. The use of portable storage devices (such as CD-RW, DVD-RW, flash drives and iPods) and other devices (such as a Blackberry or other PDA's) on district equipment is permissible provided that such devices are used in a professional manner and do not violate any rules, policies or guidelines delineated in this document (including copyright laws).

12. Take, scan or publish pictures of students without signed permission of the parents and permission from the building administrator. Additionally, no pictures of District property may be taken without administrator approval.

13. Post any political, commercial, pornographic or otherwise questionable material to the District web site or any PLESD hosted web site. Additionally, any postings must meet general District Policies and be approved by TD, the Superintendent or an approved delegate.

14. Access or attempt to access a desktop, network, or host computer without having obtained the appropriate access log-in ID and password legitimately. Further, it is considered a severe violation to share log-in and password information with another user; likewise, it is also a severe violation to use the log-in and password information of another user. These actions are considered "hacking" and/or "trespass" and will be dealt with appropriately.

15. Share, distribute or otherwise provide personal log-in and password information with another individual other than representatives from TD. Employees sharing passwords with others, especially students, will be subject to disciplinary action. All employees are required to contact TD immediately if they suspect that their password has been compromised.

16. Tamper with switch settings or hardware (including keyboards, monitors and mouse devices), or to move, reconfigure, and/or do anything that could damage PLESD property (including but not limited to hardware such as terminals, computers, printers, and other peripherals). Any individual responsible for causing damage in any manner to any PLESD property (including but not limited to hardware, software, computer systems, or computer labs) will be FINANCIALLY responsible for all repairs and/or replacements. This includes, but is not limited to unplugging cables, plugging cables into inappropriate locations, or other related activities that may cause the network or connection to the network to fail or to function improperly.

17. Use PLESD equipment, networks, software and systems without the proper training in the correct usage. All employees are required to receive the appropriate training in the use of PLESD systems, software and equipment from their appropriate supervisor (or the supervisor's delegate); if an employee has not received training or is still uncertain as to their comfort level, they should contact TD for additional support training.

18. All employees are required to log off their computers at least one time during the working day and at the end of the working day to assure that data is saved properly and that general system upgrades can run accordingly.

19. Use the PLESD network to store, record, download or otherwise procure and transfer music (such as streaming audio or Internet radio) or images (such as pictures and streaming video) for personal entertainment. Streaming audio and video is permissible for educational and training purposes. Employee files may be purged of excessive audio and video data at any time at the discretion of the Superintendent or the Director of Technology. It is permissible to request installation if iTunes and to play music from a portable device should as an iPod or an MP3 player provided that the files are not transferred to the PLESD network or any PLESD computer.

PLESD WIRELESS INTERNET

It is permissible to access the PLESD wireless Internet network where available using any personal computing device. However, access of the wireless Internet by a user means that the user agrees to all the rules and guidelines set forth in this document including adherence to the limitations of the CIPA Content Filter.

INTERNET USE

The Internet is an electronic network connecting millions of computers and individual users worldwide. The purpose of the Internet is to support world-wide access to a broad variety of information and data, and to allow the sharing of content created by a multitude of users. The use of an assigned PLESD account must be in the application and support of educational and instructional technology, and must be consistent with the educational objectives of PLESD and the standards that have been established by the School Board and Administration.

1. Internet access may be provided to employees for research, reporting and educational activities relating to their duties (and not for entertainment purposes). Employees may also use the Internet access for access to:

- Electronic mail
- World Wide Web
- Various discussion groups and social networks (which may be restricted by CIPA filtering)
- Bulletin Boards
- LIMITED Streaming Audio and Video content
- Web-based educational applications
- PLESD Sites (web pages, blogs, training, etc.)

2. Network Etiquette – You are expected to abide by the generally accepted rules of network etiquette. These include but are not limited to the following:

- Be polite. Do not be abusive in your messages to others.
- Use appropriate language. Do not swear, use vulgarities or any other inappropriate or suggestive language. Illegal activities are strictly forbidden.
- Do not reveal your personal address or phone number or that of other employees or students, except in your normal course of duties.

- Note that PLESD-provided e-mail accounts are not guaranteed to be private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.
- Do not disrupt the use of the network by other users.

3. Inappropriate use of an account -- The use of the Internet is a privilege, not a right. Inappropriate use will result in cancellation of privileges. The following are examples of inappropriate use.

- Attempting to bypass the CIPA Content Filter
- Accessing streaming audio and video for entertainment purposes, whether it is from the Internet or via electronic mail.
- The use of (or an attempt to use) another person's log-in and/or password.
- Copying, transferring, or duplicating software owned by or registered to PLESD.
- Transmission of, or downloading any material in violation of any national, state, or district regulation is prohibited. This includes, but is not limited to, copyrighted documents, material that is threatening, and/or obscene/pornographic material.
- Using the network for commercial, political, personal, or private gain.
- Communication whose sole intent is not for the purpose of education or school-related research/activities.

CONSEQUENCES FOR INAPPROPRIATE USE

The Director of Technology will deem what is inappropriate use and, after consulting with the Superintendent or appropriate supervisor, may close an account. Administrators may request the Director of Technology to deny, revoke, or suspend specific employee accounts. If an employee has failed to comply with this policy, he/she may be:

A. Removed from the system for a specific period of time or permanently, depending on the nature of the offense.
B. Required to pay for damages, technician time, computer resources, or other fees.
C. Criminally charged under local, state, or federal laws.
D. Subject to employee disciplinary action, up to and including termination or discharge in accordance with existing Board policies and applicable law.

Plumas Lake Elementary School District Technology
Acceptable Use Contract for PLESD Employees

As an employee of the Plumas Lake Elementary School District, here in after referred to as "PLESD", I,_____, recognize and understand that the district's email systems are to be used for conducting the district business only. I understand that use of this equipment for private purposes is strictly prohibited. Further, I agree not to access a file or retrieve any stored communication or data other than where authorized unless there has been prior clearance by an authorized PLESD representative. I am aware PLESD reserves the right to review, audit, intercept, access, and disclose all matters on the district's e-mail systems and serves at any time, with or without employee notice or consent, and that such access may occur during or after working hours. I am aware that use of an PLESD provided password or code does not restrict the district's right to access electronic communications. I am aware that violations of this policy may subject me to disciplinary action, up to and including termination or discharge from employment. I agree that it is not permissible to store personal files (including audio and image files) on my computer or network account and such files may be deleted at any time without notice. I acknowledge that I have read and that I understand the PLESD Technology Acceptable Use Policy regarding e-mail, computer hardware usage, computer software usage, and Internet access. I acknowledge that I have read and that I understand this notice and that a copy of the entire policy has been provided to me. Refusing to sign does not negate my responsibility to abide by the policies and procedures as set forth above and in the policy as revised. Choosing not to adhere to the policies set forth above is cause for suspension of all computer and Internet privileges.

_____ _____

Signature Date