

Authorization for Electronic Network Access-Staff AUP

Each staff member must sign this Authorization as a condition for using the District's Electronic Network connection. Please read this document carefully before signing.

All use of the Internet shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. This *Authorization* does not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. **The failure of any user to follow the terms of the *Authorization for Electronic Network Access* will result in the loss of privileges, disciplinary action, and/or appropriate legal action.** The signatures at the end of this document are legally binding and indicate the parties who signed have read the terms and conditions carefully and understand their significance.

Terms and Conditions

Acceptable Use - Access to the District's electronic network must be: (a) for the purpose of education or research, and be consistent with the District's educational objectives, or (b) for a legitimate business use.

Privileges - The use of the District's electronic networks is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The system administrator will make all decisions regarding whether or not a user has violated the terms of access privileges and may deny, revoke, or suspend access at any time. His or her decision is final.

Unacceptable Use - The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:

- a. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any State or federal law;
- b. Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused;
- c. Downloading copyrighted material for other than personal use;
- d. Using the network for private financial or commercial gain;
- e. Wastefully using resources, such as file space;
- f. Hacking or gaining unauthorized access to files, resources or entities;
- g. Invading the privacy of individuals, that includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature including a photograph;
- h. Using another user's account or password;
- i. Posting material authored or created by another without his/her consent;
- j. Posting anonymous messages;
- k. Using the network for commercial or private advertising;
- l. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and
- m. Using the network while access privileges are suspended or revoked.

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

- a. Be polite. Do not become abusive in your messages to others.
- b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
- c. Do not reveal the personal information, including the addresses or telephone numbers, of students or colleagues.
- d. Recognize that electronic mail (e-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
- e. Do not use the network in any way that would disrupt its use by other users.
- f. Consider all communications and information accessible via the network to be private property.

No Warranties - The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the users own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Indemnification - The user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any violation of this *Authorization*.

Security - Network security is a high priority. If you can identify a security problem on the Internet, you must notify the system administrator or Building Principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account without written permission from that individual. Attempts to log-on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

Vandalism - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

Telephone Charges - The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.

Use of Electronic Mail - The District's electronic mail system, and its constituent software, hardware, and data files, are owned and controlled by the School District. The School District provides e-mail to aid students and staff members in fulfilling their duties and responsibilities, and as an education tool.

- a. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student or staff member to an electronic mail account is strictly prohibited.
- b. Each person should use the same degree of care in drafting an electronic mail message as would be put into a written memorandum or document. Nothing should be transmitted in an e-mail message that would be inappropriate in a letter or memorandum.
- c. Electronic messages transmitted via the School District's Internet gateway carry with them an identification of the user's Internet "domain." This domain name is a registered domain name and identifies the author as being with the School District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of the School District. Users will be held personally responsible for the content of any and all electronic mail messages transmitted to external recipients.
- d. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.
- e. Use of the School District's electronic mail system constitutes consent to these regulations.

Internet Safety

Internet access is limited to only those "acceptable uses" as detailed in these procedures. Internet safety is almost assured if users will not engage in "unacceptable uses," as detailed in this *Authorization*, and otherwise follow this *Authorization*.

Staff members shall supervise students while students are using District Internet access to ensure that the students abide by the Terms and Conditions for Internet access contained in this *Authorization*.

Each District computer with Internet access has a filtering device that blocks entry to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee.

The system administrator and Building Principals shall monitor student Internet access.

Web Publishing Guidelines

General Requirements

All material published on the District Web site must have educational value and/or support the District guidelines, goals, and policies. Material appropriate for Web publishing includes information about the District and its Board Members, agendas, policies, appropriate administrative procedures, Department activities or services, schools, teachers or classes, student projects, and student extracurricular organizations. Personal information, not related to education, will not be allowed on the District Web site.

All content published on the District Web site must:

1. Comply with all State and federal law concerning copyright, intellectual property rights, and legal uses of network computers.
2. Comply with Board policies, administrative procedures, these Guidelines, and other District guidelines provided for specific levels of publishing. This specifically includes the Board's *Access to Electronic Networks* policy and the District's procedures on *Acceptable Use of Electronic Networks*.
3. Due to limited storage space and varying network speeds, file sizes must be kept under 50 kilobytes unless the District Webmaster approves otherwise.
4. Comply with the publishing expectations listed below.

Material that fails to meet these Guidelines or is in violation of Board policy and/or procedures shall not be published on the District Web site. The District reserves the right to remove any material in violation of its policy or procedures. Failure to follow these Guidelines or Board policy and/or procedures may result in loss of privileges, disciplinary action, and/or appropriate legal action.

Publishing Expectations

The following are minimum expectations for all District Web pages:

1. The style and presentation of Web published material should be of high quality and designed for clarity and readability. Material shall not be published in violation of the District's procedures on *Acceptable Use of Electronic Networks*, including material that is defamatory, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or harassing or material that invades the privacy of any individual. Anonymous messages are prohibited.
2. Correct grammar and spelling are expected.
3. All information must be verifiable.
4. Publications must include a statement of copyright when appropriate and indicate that permission has been secured when including copyrighted materials.
5. Publications must identify affiliation with the District, school and/or department.
6. Widespread use of external links to non-District Web sites is discouraged, but if used, the external sites must contain appropriate educational materials and information as exclusively determined by the District. Every effort should be made to insure all links are operational. Every link to an external Web site must open a new browser window.
7. Relevant dates are required on all publications, including the date on which the publication was placed on the District Web site. Each site should contain the date the page was last updated.
8. All publications must include the District e-mail address of the staff member responsible for the page. This provides a contact person for questions or comments.
9. Use of the District's Web site for personal or financial gain is prohibited. No commercial or private accounts should be listed on any District Web pages.
10. All documents should be previewed on different Web browsers before being posted on the District Web site.

For more information about these expectations or other issues related to Web publishing, please contact the System Administrator.

Protecting Student and Staff Privacy

Personal information concerning students or staff members, including home addresses and telephone numbers, shall not be published on District Web pages.

A student's last name, last name initial, and grade level shall not be published on District Web pages. In addition, student records shall not be disclosed. In special circumstances (e.g., where accolades are warranted), the sponsoring staff member should contact the Building Principal who may seek permission from the student's parents/guardians. Web pages shall not display student pictures with a student identified by his or her name unless written parental permission was first granted (e.g., by executing the form *Using a Photograph or Videotape of a Student*). Student e-mail addresses, whether a personal or District account, shall not be listed on any District Web page.

Submitting Material to Be Published

Everyone publishing information on the District's Web site shall have signed an *Authorization for Electronic Network Access*. All material posted by a teacher or other staff member on the District's Web site is deemed "work for hire," and the copyright in those works vests in the District.

Copyright Web Publishing Rules - Copyright law and District policy prohibit the re-publishing of text or graphics found on the Web or on District Web sites or file servers, without explicit written permission.

- a. For each re-publication (on a Web site or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the Web address of the original source.
- b. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the Web site displaying the material may not be considered a source of permission.
- c. The "fair use" rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.
- d. Student work may only be published if there is written permission from both the parent/guardian and student.

Authorization for Electronic Network Access Signature Form

Submit this form to the Technology Director after reading the Authorization for Electronic Network Access document.

I understand and will abide by the above *Authorization for Electronic Network Access*. I understand that the District and/or its agents may access and monitor my use of the Internet, including my e-mail and downloaded material, without prior notice to me. I further understand that should I commit any violation, my access privileges may be revoked, and school disciplinary action and/or appropriate legal action may be taken. In consideration for using the District's electronic network connection and having access to public networks, I hereby release the School District and its Board members, employees, and agents from any claims and damages arising from my use of, or inability to use the Internet.

Staff Name (*please print*)

Staff Signature

Date

Staff Laptop Agreement

Ownership of the Laptop

North Mac CUSD #34 retains sole right of possession of the laptop. The laptops are lent to the employee **for educational purposes only**. Using the laptop for personal matters such as personal social media sites, personal shopping or any other person use **is strictly prohibited**. Moreover, North Mac CUSD #34 Technology Director retains the right to collect and/or inspect laptops at any time, including electronic remote access to alter, add or delete installed software or hardware.

Responsibility for the Laptop

Employees are solely responsible for the laptop issued to them and must adhere to the following:

- Employee must comply with the District's Technology Policy and corresponding Authorization for Electronic Network Access.
- Employee must bring their laptop to school every day. **This laptop will be the main computer for staff.**
- Employee must treat their device with care and never leave it in an unsecured location.
- Employee must promptly report any problems with their laptop to the Technology Staff. (Technology Staff refers to J. Blankenship or J. Langellier)
- Employee may not attempt to install or run any operating system or programs on the laptop, unless prior approval from the Technology Director has been granted.

Responsibility for Electronic Data

Employees are solely responsible for any apps on their laptop that are not installed by a member of the North Mac CUSD #34 technology staff. Employees are NOT to be installing any apps or programs to the laptops without prior approval from the Technology Staff. Employees are responsible for backing up their data to protect from loss. Users of District Technology have no rights, ownership, or expectations of privacy to any data that is, or was, stored on the laptop, school network, or any school issued applications and are given no guarantees that data will be retained or destroyed.

Copyright and File Sharing

Employees are required to follow all copyright laws around all media including text, images, programs, music, and video. Downloading, sharing, and posting online illegally obtained media is against the Technology Policy.

Damage/Repair

The district will repair or replace damaged equipment resulting from normal use. Only Technology Staff are allowed to attempt any repairs or fixes to the equipment.

Digital Safety

Employee must be very careful when using their laptops online at home. Be careful to stay away from suspicious websites, downloading of files or other items from sites you are not sure of their credibility. Do not open emails or attachments from unknown sources. Use common sense when online to protect the District's Network.

Digital Citizenship

Employee must follow the six conditions of being a good Digital Citizen:

1. **Respect Yourself.** I will show respect for myself through my actions. I will select online names and profile pictures that are appropriate. I will consider the information and images that I post online. I will consider what personal information about my life, experiences, experimentation or relationships I post. I will not be obscene.
2. **Protect Yourself.** I will ensure that the information, images and materials I post online will not put me at risk. If I will not publish my personal details, contact details or a schedule of my activities. I will report any attacks or inappropriate behaviors directed at me. I will protect all passwords, accounts and resources.
3. **Respect Others.** I will show respect to others. I will not use electronic mediums to antagonize, bully, harass or stalk other people. I will show respect for other people in my choice of web sites, I will not visit sites that are degrading, pornographic, racist or inappropriate. I would not abuse my rights of access and I will not enter other people's accounts, private spaces or areas.

4. **Protect Others.** I will protect others by reporting abuse, not forwarding inappropriate materials or communications; I will moderate unacceptable materials and conversations, and not visit sites that are degrading, pornographic, racist or inappropriate.
5. **Respect Intellectual Property.** I will request permission to use resources. I will suitably cite any and all use of web sites, books, media, etc. I will acknowledge all primary sources. I will validate information. I will use and abide by the fair use rules.
6. **Protect Intellectual Property.** I will request to use the software and media others produce. I will use free and open source alternatives rather than pirating software. I will purchase, license and register all software. I will purchase my music and media, in refrain from distributing these in a manner that violates these licenses. I will act with integrity.

Signature

By signing below, the employee agrees to follow and accept:

- Technology Policy and corresponding Authorization for Electronic Network Access.
- The Laptop Agreement and Authorization for Electronic Network Access.
- North Mac CUSD #34 owns the laptop, software and issued peripherals.
- If the Employee ceases to be employed at North Mac CUSD #34 they will return the laptop in good working order or pay the full replacement cost of the computer.
- In no event shall North Mac CUSD #34 be held liable to any claim of damage, negligence, or breach of duty.

North Mac Staff Signature: _____ Date: _____