

California Montessori Project Staff Technology Usage & Professional Communication Policy

The California Montessori Project (CMP) Technology Usage & Professional Communication Policy will, through the use of a variety of technology resources, support all students in receiving a quality education and all employees in working in a professional and intellectually stimulating environment. The creation of a large and varied technology environment demands that technology usage and staff communications be conducted in legally and ethically appropriate ways, consistent with the Mission Statement and instructional goals of CMP.

Thus, it is the intention of CMP that all technology resources will be used in accordance with any and all school system policies and procedures as well as local, state, and federal laws and/or guidelines governing the usage of technology and its component parts. Additionally, it is implied that all students and employees of CMP will use the provided technology resources so as not to waste them, abuse them, interfere with or cause harm to other individuals, institutions, or companies. Further,

- All CMP technology resources, regardless of purchase date, location, or fund, are subject to this policy. During scheduled work hours (excluding scheduled lunch breaks and shift breaks), all personal technology resources, including personal computers, cell phones, handheld devices, etc., are subject to this policy.
- Any questions about this policy, its interpretation, or specific circumstances shall be directed to the Campus Principal, Technology Advisor, Human Resources, and/or Executive Director.
- Violators of this policy will be handled in a manner consistent with comparable situations requiring disciplinary and/or legal action.

POLICY STATEMENT:

The primary goal of the technology environment is to support the educational, instructional, and school business endeavors of students and employees of CMP. Use of any and all technology resources is a privilege and not a right.

CMP considers any and all information on the CMP network to be private, confidential and not open to the public.

I. ACCESS:

- A. The use of all CMP technology resources is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges.
- B. Individuals may not allow someone else to use their passwords to access the network, electronic mail (e-mail), or the Internet (i.e., Aeries, APTA, calendar, etc.).

- C. Individuals must take all reasonable precautions to prevent unauthorized access to accounts and data (i.e., Aeries, APTA, e-mail, calendar, etc.) and any other unauthorized usage within and outside CMP.
- D. Use of technology resources that reduces the efficiency of use for others (i.e., unauthorized software downloads and/or video data streaming) is prohibited. For instructional purposes, CMP staff may request permission regarding software downloads and/or video data streaming via the CMP "MyTechDesk" ticket process.
- E. Individuals must not modify technology resources, utilities, or configurations, or change the restrictions associated with their accounts, or attempt to breach or circumvent any technology resources or security systems, either with or without malicious intent.
- F. The Technology Advisor, Campus Principal or Executive Director will determine when inappropriate use has occurred and may recommend the denial, revocation, or suspension of a specific user's access. The Executive Director or designee will have final review and authority over such a decision.

II. PRIVACY:

- A. To maintain network integrity and to ensure that the network is being used responsibly, the Executive Director, Human Resources, Campus Principal and/or Technology Advisor reserve the right to monitor all CMP equipment, computers, network communications, and any files within such equipment, at any time, with or without notice.
- B. Any files stored on any CMP equipment or networks will not be private if passwords are compromised. The Campus Technology Mentor and/or the Technology Advisor may also access files stored on CMP equipment or networks during troubleshooting and problem resolution activities.
- C. CMP reserves the right to monitor personal devices approved for CMP network access.
- D. Because communications on the Internet are often public in nature, all users should be careful to maintain appropriate, responsible and professional communications at all times, both during and outside of scheduled work hours.
- E. CMP cannot guarantee the privacy, security, or confidentiality of any information sent or received via the Internet, cell phones, or by other electronic means. Staff should understand that such information may also be subpoenaed in the event of litigation.

- F. Users should be aware that the Technology Advisor and Technology Mentors routinely monitor and perform maintenance on file servers, e-mail, workstations, the Internet, user accounts, and telephones. During these procedures, it may be necessary to review e-mail and/or files stored on the network.
- G. CMP equipment is to be used only for job related functions and use of such equipment for personal purposes is prohibited.
- H. At this time, CMP does NOT perform routine backups. Therefore, all users are encouraged to back up any critical files (i.e., digital student information, accounting information, etc.) and any other data on the campus network storage device. In addition, the use of flash drives and CD's (which should be stored in a secure location) are encouraged.

I acknowledge the need to backup critical files.

Initials: _____

- I. All files and network communications stored on or sent through CMP's technology resources shall be and remain the property of CMP.
- J. Users should be aware that the technology staff logs and records all Internet and network access for all CMP network users.
- K. Users are prohibited from violating the privacy of others using hand-held devices such as cell phones, camera phones, and video cameras, to record voice, images, data, etc.
- L. Confidential staff, student or family information (i.e., special education information, behavior reports, grades, progress reports, etc.) should be under guarded care at all times. Leaving such information unattended, whether on the desk, the computer screen, the fax or the printer for anyone to inadvertently see, is strictly prohibited and potentially a breach of confidential information. For example, staff should invoke their password protection screen before leaving their computer unattended. (See also: CMP Personnel Policy regarding Confidential Information – Staff and Confidential Information – Students.)

III. COPYRIGHT:

- A. Illegal copies of software may NOT be created or used on CMP equipment.
- B. The legal and ethical practices of appropriate use of technology resources will be taught to all students and employees. Any questions about copyright provisions should be directed to the Technology Advisor.

- C. Copyright is implied for all information (text, data, and graphics) published on the Internet. Web page authors will be held responsible for the content of their pages to include adherence to all applicable copyright and usage laws.
- D. Duplication of any copyrighted software is prohibited unless specifically allowed under the license agreement.
- E. System-wide software originals will reside with the Technology Advisor and/or Technology Mentor
- F. If a single copy of a software package is purchased, it may only be used on one computer at a time. Multiple loading or "loading the contents of one disk onto multiple computers" (1987 Statement on Software Copyright) is NOT allowed.
- G. If more than one copy of a software package is needed, a site license, lab pack, or network version must be purchased. The Technology Advisor and Technology Mentor will validate the type of licensing that should be purchased.
- H. The Technology Advisor and/or Technology Mentors are responsible for installation of all authorized software in use on the local area network and/or individual workstations within CMP.

I agree to request that any and all software installation be conducted by the Technology Mentor or Technology Advisor according to the above policy.

Initials: _____

IV. ELECTRONIC MAIL:

Collaborative Group Norms:

“Honor the sanctuary of others’ work environment and workflow.”

“Don’t muddle another’s work environment by forgetting e-mail etiquette.”

“Remember that ‘Reply to All’ can be easily overwhelming.”

“E-mails should be saved for FACTS, not feelings.”

“Keep a prepared work environment.”

CMP provides access to e-mail accounts for all credentialed employees and other administrative staff as designated by the Executive Director. Please remember that each classroom may have responsibility for more than one e-mail account: 1) the classroom account (an avenue for parent/guardian communications), and 2) the teacher account (for internal communiqué).

- A. Requests for new e-mail accounts will be initiated by the Campus Principal or Human Resources upon initial employment or change of employee status.

- B. Access to e-mail is for conducting educational, instructional and/or school business activities.
- C. Electronic mail should reflect professional standards at all time. As such, employees are reminded to practice e-mail etiquette (see Appendix A).
- D. When any e-mail correspondence with students, parents, and/or guardians has potential to escalate, the e-mail communication should immediately be discontinued and any further communication should take place through a personal phone call or meeting.
- E. CMP's e-mail accounts may not be used for political or personal gain.
- F. CMP's e-mail accounts may not be used for attempting or successfully sending anonymous messages.
- G. CMP e-mail accounts are for communicating with parents, guardians or students on an individual basis. E-mails to more than one parent, guardian or student are considered mass e-mails and should be handled through the campus administrative office.
- H. Each campus administrative office may send mass e-mails with respect to parent, guardian and student communication. The campus administrative offices will maintain classroom e-mail distribution lists so that timely e-mail communications can be processed through the campus office. Processing mass e-mail through the administrative office ensures:
 - a. Administrative review and approval,
 - b. Communication consistent with CMP Policies and Procedures,
 - c. Consistency with prior communications,
 - d. Maintenance of student and family confidentiality,
 - e. A check and balance in regard to timely communication.

In such cases, mass e-mails will be sent using blind recipient techniques.

I agree to send e-mail communications addressed to more than one parent, guardian or student to the administrative office for review, approval and blind copy distribution according to the above policy.

Initials: _____

- I. Users should routinely purge unnecessary e-mail correspondence.

V. INTERNET:

Introduction: CMP provides students and staff access to the Internet, which may include services such as e-mail, web sites, and other authorized services. This access is provided solely for the purposes of internal communications, educational instruction and research, as well as CMP's administrative operations. CMP requires responsible use of this technology.

For students, the ultimate responsibility in using the Internet lies with each student and the student's parent or guardian. Access to the Internet is a privilege, which may be restricted or denied in the event an individual abuses any of the terms of the CMP Technology Usage & Responsibilities contract. This contract must be read and acknowledged in writing by each student and the student's parent or guardian.

In an effort to provide safeguards for staff and students, CMP fully complies with current and pending State and Federal Law relative to the Children's Internet Protection Act (CIPA). Even so, CMP cannot provide 100% assurance that all materials accessed by students are appropriate for children.

Filtering and Monitoring: Filtering software is used to block or filter access to visual depictions that are obscene in accordance with the Children's Internet Protection Act. Other objectionable material is also being filtered. The determination of what constitutes "other objectionable" material is based on categories as defined in CMP's content filter: St Bernard, iPrism.

- A. Filtering software is not 100% effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites.
- B. Any attempts to defeat or bypass CMP's Internet filter or conceal Internet activity are prohibited: proxies, https, special ports, modifications to CMP's browser settings and any other techniques designed to evade filtering.
- C. Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.
- D. Staff members who supervise students, control electronic equipment or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of CMP.
- E. CMP will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by students to inappropriate material on the Internet is deliberate and consistent monitoring of student access to CMP computers.

- F. Staff members may request access to filtered sites and blocked services as may be applicable to the mission and objectives of the school and in support of CMP's business operations and academic program. The Technology Advisor shall act on such requests using the standard of care outlined in this Technology Usage Policy. The Campus Principal and/or Executive Director will provide final review and authorize action as necessary.

Acceptable Use: Access to the Internet is for the purpose of supporting internal communication, educational instruction and research, and CMP's administrative operations. All Internet usage must be consistent with these purposes, the terms of the policy, and all provisions of law governing these actions.

Uses Not Acceptable: The following are examples of specific types of conduct that are not acceptable Internet uses (additional examples are included in Appendix B):

- A. The transmission or reception of any material in violation of any United States or California Law or regulation, including the unauthorized transmission or reception of copyrighted material, the transmission of any harassing or threatening material, the transmission of material protected by trade secret, and/or the transmission of any vulgar or obscene material.
- B. The use of the Internet for any non-school, commercial purpose (unless pre-approved by the Campus Principal or Executive Director and relative to the school's administrative and/or programmatic operations).

Network Etiquette: Use of technology should be consistent with CMP's mission to be respectful, be safe and be responsible. Users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

- A. Be respectful. Use appropriate language. Abusive language/ tone is inappropriate and will not be tolerated.
- B. Be safe. Keep student, parent and staff information confidential at all times.
- C. Be responsible. Use the network in such a way that it is not disruptive to others.

Privileges: The use of the Internet is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The Technology Advisor, Human Resources, and/or the Campus Principal will deem what is inappropriate use and will make recommendations when inappropriate use is identified. Final review and decision on such a recommendation will be made by the Executive Director. Staff members who are aware of inappropriate use by authorized users are encouraged to report such abuses to their Campus Principal or Executive Director.

Privacy: CMP reserves the right to monitor, inspect, copy and review, at any time and without prior notice, any and all Internet usage and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of CMP and no user shall have any expectation of privacy in such material (i.e., Internet usage and e-mail).

Security: Security on any computer system is a high priority, especially when the system involves many users. This includes, but is not limited to: Virus warnings, compromising passwords, and modification of computer systems. Staff should notify the Technology Mentor, Technology Advisor and/or Campus Principal immediately when a security problem on the network or Internet is suspected. Do not demonstrate the problem to other users. Do not use another individual's account.

Vandalism: Vandalism can be deemed as any malicious attempt to harm or destroy data of another user. Vandalism will result in cancellation of privileges, termination and/or legal action.

Controversial or Offensive Material: While CMP abides by the Children's Internet Protection Act, staff, students, parents, and/or guardians are advised that use of the Internet has the potential for access to materials that are inappropriate. It is the responsibility of each individual staff member and student to use the system in an appropriate manner and to avoid access to or use of inappropriate material at all times. Any staff member becoming aware of the access to such material by any other person shall immediately report the inappropriate and unauthorized access to the Campus Principal or Executive Director.

Social Networking: Staff members are prohibited from using **CMP** resources for the purpose of Social Networking. Staff members are also prohibited from using **personal** resources for the purpose of Social Networking during scheduled work hours. This includes, but is not limited to: MySpace, Facebook, Twitter, social forums/blogs, etc. Staff members are reminded that there is a greater standard of care for professional educators and those employees should carefully consider their social activities and special interests, both within and outside of their employment with CMP. Staff members who choose to engage in activities and social communication that conflict with the professional educator's role in the classroom, and/or impact the educator's ability to be successful in the classroom, may create personal and organizational liabilities.

- A. Teachers and staff members should refrain from requesting of or accepting 'friend requests' from students, parents and/or guardians.
- B. Personal blogs are just that, personal and do not represent the views of CMP. Staff, students, parents and guardians shall not act as a spokesperson of CMP.

- C. References to staff, students and/or families on social networking sites are discouraged. Staff is reminded that their online presence is a public venue and is a reflection on CMP. Staff should be aware that their actions captured via images, posts, or comments, both during and outside of scheduled work hours, may create a liability upon CMP as well as the staff member's credibility as a professional educator and/or other CMP employees, families and students, and can also be disruptive to CMP operations.

Online Applications: Online applications are tools on the Internet used to support academic learning. Examples are Accelerated Reader, Rosetta Stone, and K to the 8th. If teachers find other useful online applications to accommodate student activities, a proposal should be prepared and presented to the Campus Principal, Technology Advisor, and/or the CMP Administrative Leadership Team for review and approval prior to implementation. The proposal should be prepared utilizing the Web Application Request Form.

I agree to abide by the above Internet Usage Policies, including the policy on Social Networking.

Initials: _____

VII. WEB PUBLISHING:

- A. All information in posted work must be of publishable quality with regard to spelling, usage, and mechanics.
- B. All information in posted work must maintain the confidentiality of staff, students, parents, and/or guardians. This includes all information related to full names, addresses, contact numbers, family status, health, and progress information (see Confidential Information section of CMP Personnel Handbook).
- C. Information on behalf of CMP shall only be published by appointed individuals and shall be reviewed and approved by the Campus Principal and/or Executive Director (or an appointed designee) prior to publishing.
- D. All materials prepared by staff to be posted on CMP's website and associated pages shall be in good taste and respectful of CMP, other employees, families and students of CMP.
- E. All links should be checked regularly to make sure they are current and working.
- F. Pages that are not updated in a timely fashion, that contain inaccurate or inappropriate information, or contain links that do not work may be removed and the author will be notified.

- G. A media release must be on file prior to public postings reflecting identifiable information or images. Pictures and other personally identifiable information shall only be used with written permission from the staff member, or the parent/guardian of the student involved. For safety reasons, only first names of students shall be used in publicly posted information.
- H. For safety reasons, student posting of personal information of any kind is prohibited.
- I. Written permission is not required to list faculty/staff and their school contact information such as phone extension, e-mail address, etc.
- J. The CMP web server shall not be used for profit (except for any and all sponsored CMP activities and fundraisers), commercial purposes, to express personal opinions, or to editorialize.
- K. Infringement of copyright laws, as well as the posting of obscene, harassing or threatening materials on web sites and through other electronic means are against the law/school policy and are subject to prosecution.

I agree to abide by the above Web Publishing Policy and will ensure confidentiality as outlined above.

Initials: _____

VIII. PARENTAL PERMISSIONS:

Staff members are required to verify written parental permission when posting student information on the web, requesting videos, designing publicity or public relations information, or supervising student media projects.

IX. PERSONAL EQUIPMENT:

- A. CMP is not responsible for personal equipment brought onto the CMP campus (for example, computers, cameras, cell phones, handheld devices, etc.). Further, CMP is not responsible for personal equipment connected to the network or the damages/changes made to that equipment as a result of the policies of the CMP network.
- B. All personal equipment used within the CMP network is bound by the same policies and rules as CMP school-owned equipment.

C. Use of personal cell phones/handheld devices on campus shall be guided by the following provisions:

1. While personal cell phones/handheld devices are allowed on campus, staff members are encouraged to model school policy and should have them turned off during school/work hours. These devices can cause disturbance to the classroom as well as emit frequencies which may cause interference with wireless access. Special circumstances may warrant a need to have a personal cell phone on during work hours in "muted" mode, but must be pre-approved by the Campus Principal or Executive Director.
2. The use of school telephones and 2-way radios provided by the school are the preferred method for communicating with other classrooms or the administrative office.
3. Personal calls, texting, social networking or any other personal business or Internet activity should not be conducted during scheduled work hours, and most especially while the employee is responsible for the supervision of students in the classroom, on the playground or on field trips. (See also: Personnel Policy and Student Policy regarding Cell Phone Usage.)

X. SOFTWARE:

Teachers, other staff members, parents, guardians and/or students may not load non-authorized software on the CMP network. The Technology Advisor and/or Technology Mentors are not responsible for non-authorized software and will remove all non-authorized software from the network.

I agree to abide by the above Technology Usage Policy, including the following appendices.

Print Name: _____

Campus: _____

Signature: _____

Date: _____

Appendix A

EXAMPLES OF E-MAIL ETIQUETTE:

1. Be concise and to the point.
2. Use a meaningful subject line.
3. Use proper spelling, grammar and punctuation.
4. Personalize your message appropriately.
5. Use "CONFIDENTIAL" in the subject line when any confidential information is being transmitted.
6. Respond in a timely manner.
7. Use the "cc:" field sparingly.
8. Use Reply to All only as necessary.
9. Do not attach unnecessary files.
10. Refrain from emailing large attachments.
11. Use professional stationary and signature blocks.
12. Use the high priority option with care.
13. Do not write in CAPITALS.
14. Take care with abbreviations and emotions.
15. Be careful with formatting.
16. Keep your language gender neutral.
17. Maintain the message threads to ensure clarity.
18. Do not copy a message or attachment without permission.
19. Avoid using URGENT and IMPORTANT.
20. Do not forward chain letters.
21. Don't reply to spam.
22. Proofread the e-mail before you send it.
23. Include your name, title, grade, classroom and campus in your closing.
24. Stay away from endorsing your favorite vendor link, quote, clip art or paper color in your closing.
25. Include the California Montessori Project's PRIVILEGED & CONFIDENTIAL statement in all e-mail correspondence.

Appendix B

EXAMPLES OF INAPPROPRIATE USE OF RESOURCES:

The following are examples of inappropriate activities for any CMP network, e-mail system, or the Internet. This list is not all-inclusive. Anything that would be considered inappropriate in "paper form" is also considered inappropriate in electronic form.

1. Using another user's password or attempting to find out another user's password.
2. Sharing your own password.
3. Modifying another user's files, folders, home directory, or work.
4. Harassing, insulting, bullying, or attacking others via technology resources, including handheld devices.
5. Vandalizing computers, computer systems, or computer networks (this includes changing workstation configurations such as screen savers, backgrounds, printers, BIOS information, preset passwords, etc.).
6. Intentionally wasting limited resources such as disk space, print toner and paper.
7. Attempting to access inappropriate web sites.
8. Sending, displaying, or downloading offensive messages or pictures.
9. Using obscene, racist, profane, discriminatory, threatening, or inflammatory language.
10. Posting any false or damaging information about other people, the school, or other organizations.
11. Posting of any personal information about another person.
12. Broadcasting network messages and/or participating in sending or perpetuating chain letters.
13. Violating copyright laws.
14. Plagiarism of materials that are found on the Internet.
15. Use of technology resources to create illegal materials (i.e., counterfeit money, fake identification, etc.).
16. Use of any CMP technology resources for personal gain, commercial or political purposes.