Title: Technology Use Policy

Control Information

Control Item	Details
Owner/Curator	Melissa Harris
Document #	PolicyS00045a
Supersedes	None
File Location	www.muddycreekcharterschool.org
Board Approval Date	9/11/2014
Consult and Notify	ICP, ED, HT, AA, T

Revision History

Revision	Date	Revision Description	Originator
A	9/11/2014	Initial Release	Melissa Harris

1.1. Objective:

The objective of this policy is the following:

1.1.1. To set forth guidelines for staff and student access to the school computer system and acceptable and safe use of the Internet, including electronic communications.

1.1.2. To provide guidelines for the use of technology in the educational setting.

1.2. Acceptable Use of Technology

1.2.1. Access to the school computer system and to the Internet enables students and employees to explore thousands of libraries, databases, bulletin boards, and other important resources. The school expects that faculty will blend thoughtful use of the school computer system and the Internet throughout the curriculum and will provide guidance and instruction to students in their use.

1.2.2. The use of the Internet during school hours has a limited educational purpose, which includes use of the system for classroom activities, educational research, and professional or career development activities. Users are expected to use Internet access to further educational and personal goals consistent with the mission of the school district and school policies. Uses which might be acceptable on a user's private personal account on another system may not be acceptable on this limited-purpose network.

1.3. General School Responsibilities

The school will:

1.3.1. Designate staff as necessary to ensure coordination and maintenance of the school's electronic communications system that includes all school computers, e-mail, and Internet access.

1.3.2. Provide staff training in the appropriate use of the school's system including copies of school policy and administrative regulations. Staff will provide similar training to authorized system users.

1.3.3. Cooperate fully with local, state or federal officials in any investigation relating to misuse of the school's system.

1.3.4. Use only properly licensed software, audio, or video media purchased by the school or approved for use by the school. The school will comply with the requirements of law regarding the use, reproduction, and distribution of copyrighted works and with

applicable provisions of use or license agreements.

1.3.5. Install and use desktop and/or server virus detection and removal software.

1.3.6. Provide technology protection measures that protect against Internet access by both adults and minors to visual depictions that are obscene, child pornography; or with respect to the use of computers by minors, harmful to minors. An administrator, supervisor, or other individual authorized by the superintendent may disable the technology protection measures to enable access for bona fide research or other lawful purposes, as deemed appropriate.

1.3.7. Prohibit access by minors, as defined by CIPA and this regulation, to inappropriate matter on the Internet and World Wide Web.

1.3.8. Provide staff supervision to monitor the online activities of students to prevent unauthorized access, including “hacking” and other unlawful activities online, and ensure the safety and security of minors when authorized to use e-mail, chat rooms, and other forms of direct electronic communication.

1.3.9. Provide student education about appropriate online behavior, including cyberbullying awareness and response, and how to interact with other individuals on social networking sites and in chat rooms.

1.3.10. Notify appropriate system users that:

1. The school retains ownership and control of its computers, hardware, software, and data at all times. All communications and stored information transmitted, received, or contained in the school’s information system are the school’s property and are to be used for authorized purposes only. Use of school equipment or software for unauthorized purposes is strictly prohibited. To maintain system integrity, monitor network etiquette and ensure that those authorized to use the school's system are in compliance with Board policy, administrative regulations and law, the Executive Director may routinely review user files and communications. The school will inform system users that files and other information, including e-mail, generated or stored on district servers are not private and may be subject to such monitoring.
2. Files and other information, including e-mail, sent or received, generated, or stored on district servers are not private and may be subject to monitoring. By using the school’s system, individuals consent to have that use monitored by authorized school personnel. The school reserves the right to access and disclose, as appropriate, all information and data contained on district computers and school-owned e-mail system.
3. E-mail sent or received by a Board member or employee in connection with the transaction of public business may be a public record and subject to state archivist rules for retention and destruction.
4. Information and data entered or stored on the school’s computers and e-mail system may become discoverable evidence if a public records request is made or a lawsuit is filed against the school. “Deleted” or “purged” data from school computers or e-mail system may be retrieved for later public records disclosure or

disciplinary purposes, as deemed necessary by the school.

5. Transmission of any materials regarding political campaigns is prohibited. Providing general information is permitted, without advocacy for a position or candidate.

1.3.11. Ensure all staff and non-school system users complete and sign an agreement to abide by the school's electronic communications policy and administrative regulations. All such agreements will be maintained on file in the information services office.

1.4. Filters, Internet Protection and Supervision

The Executive Director will ensure that the school's computer system complies with the following provisions of the Children's Internet Protection Act:

1.4.1. Technology protection measures installed and in continuous operation that block or filter Internet access by both adults and minors to inappropriate content.

1.4.2. Education of minors about appropriate online behaviors, including cyberbullying awareness and response, and how to interact with other individuals on social networking sites in chat rooms.

1.4.3. Monitoring of all online activities of minors.

1.4.4. Denying access by minors to inappropriate content on the Internet.

1.4.5. Prohibiting the unauthorized access, "hacking" and other unlawful activities by minors online.

1.4.6. Prohibiting the unauthorized disclosure, use and dissemination of personal information regarding minors.

1.5. System Access

1.5.1. Access to the school's system is authorized to Board members, school employees, students with parent approval and when under the school supervision of staff; school volunteers, district contractors, or other members of the public as authorized Executive Director consistent with the school's policies.

1.5.2. Students, staff, Board members, volunteers, school contractors, and other members of the public may be permitted to use the school's system for personal use, in addition to official district business, consistent with Board policy, general use prohibitions/ guidelines/etiquette, and other applicable provisions of this administration regulation. Personal use of school-owned computers, including Internet and e-mail access by

employees, is prohibited if it interferes with employee's duties during the employee's work hours. Additionally, Board member and employee use of school-owned computers may be permitted only when such use does not violate the provisions of ORS 244.040 and use is under the conditions that access is provided to the general public under the district's policy governing use of district equipment and materials.

1.5.3. The following conduct is strictly prohibited:

1. Attempts to use the district's system for:
    - Unauthorized solicitation of funds;
    - Distribution of chain letters;
    - Unauthorized sale or purchase of merchandise and services;
    - Collection of signatures;
    - Membership drives;
    - Transmission of any materials regarding political campaigns.
2. Attempts to upload, download, use, reproduce, or distribute information, data, software, or file share music, videos, or other materials on the district's system in violation of copyright law or applicable provisions of use or license agreements.
3. Attempts to degrade, disrupt, or vandalize the school's equipment, software, materials, or data or those of any other user of the school's system or any of the agencies or other networks connected to the school's system.
4. Attempts to evade, change, or exceed resource quotas or disk usage quotas.
5. Attempts to send, intentionally access, or download any text file or picture or engage in any communication that includes material that may be interpreted as:
    - Harmful to minors;
    - Obscene or child pornography as defined by law or indecent, vulgar, profane, or lewd as determined by the school;
    - A product or service not permitted to minors by law;
    - Harassment, intimidation, menacing, threatening, or constitutes insulting or fighting words, the very expression of which injures or harasses others;
    - A likelihood that, either because of its content or the manner of distribution, it will cause a material or substantial disruption of the proper and orderly operation of the school or school activity;
    - Defamatory, libelous, reckless, or maliciously false, potentially giving rise to civil liability, constituting or promoting discrimination, a criminal offense, or otherwise violates any law, rule, regulation, Board policy, and/or administrative regulation.

6. Attempts to gain unauthorized access to any service via the school's system which has a cost involved or attempts to incur other types of costs without specific approval. The user accessing such services will be responsible for these costs.
7. Attempts to post or publish personal student contact information unless authorized by the system coordinator or teacher and consistent with applicable Board policy pertaining to student directory and personally identifiable information. Personal contact information includes photograph; age; home, school, work, or e-mail addresses; phone numbers; or other unauthorized disclosure, use, and dissemination of personal information regarding students.
8. Attempts to use the school's name in external communication forums such as chat rooms without prior district authorization.
9. Attempts to use another individuals account name or password, or access restricted information, resources, or networks to which the user has not been given permission.

1.5.4. Complaints regarding use of the school's Electronic Communications System may be made to the Executive Director, employee's supervisor, or system coordinator. The school's established complaint procedure will be used for complaints concerning violations of the school's Electronic Communications System policy and/or administrative regulation.

1.6. Violations/Consequences

1.6.1. Students:

- Students who violate general system user prohibitions shall be subject to discipline up to and including expulsion and/or revocation of school system access up to and including permanent loss of privileges.
- Violations of law will be reported to law enforcement officials and may result in criminal or civil sanctions.
- Disciplinary action may be appealed by parents, students, and/or a representative in accordance with established school procedures.

1.6.2. Staff

- Staff who violate general system user prohibitions shall be subject to discipline up to and including dismissal in accordance with Board policy and applicable provisions of law.
- Violations of law will be reported to law enforcement officials and may result in

criminal or civil sanctions.

- Violations of applicable Teacher Standards and Practices Commission (TSPC), Standards for competent and ethical performance of Oregon Educators will be reported to TSPC as provided by OAR 584-020-0041.
- Violations of ORS 244.040 will be reported to Government Standards and Practices Commission.

1.6.3. Others

- Other guest users who violate general system user prohibitions shall be subject to suspension of system access up to and including permanent revocation of privileges.
- Violations of law will be reported to law enforcement officials or other agencies, as appropriate and may result in criminal or civil sanctions.

Student Internet/Computer Use Agreement Form

Student Name_____ Grade_____

Teacher_____

Parent/Guardian Section

Please Check One:

[ ] I have read Muddy Creek Charter School Policy S00045 "Technology Use Policy" and discussed the policy with my child. I hereby give permission for my child to use the school computer system and the Internet for educational purposes, as outlined by the school and in accordance with school policy.

I hereby release the school and staff from any and all claims and damages of any nature arising from my child's use of, or inability to use the school system and Internet, including, but not limited to, claims that may arise from the unauthorized use to purchase products or services. I understand that I can be held liable for damages caused by my child's intentional misuse of the system.

[ ] I do not wish for my child to have access to the school computer system or the Internet. I am requesting an alternative education opportunity in place of educational activities requiring computer or Internet use.

Parent/Guardian Signature_____ Date_____

Parent/Guardian Printed Name_____ Phone_____

E-Mail_____