

APPROPRIATE USE OF TECHNOLOGY POLICY (ALL GRADES AND PERSONNEL)

Acceptable uses of the Internet are activities that support learning, collaborative work, and teaching. It is expected that every user will show respect for other people at all times. Acceptable uses include, but are not limited to, the following:

- Using the Internet to research assigned school projects;
- Respecting and upholding copyright laws and all other applicable laws and regulations;
- Respecting the ideas and work of others and giving credit appropriately when using another's words and/or ideas in a research project or any other assignment;
- Respecting the rights and privacy of others by not accessing private files or personal information;
- Following all regulations posted in the computer lab or other room where computers are in use.
- Following the directions of the adult in charge of the computer lab or other room where computers are in use
- Report any inappropriate use of data or violation of policy immediately upon discovery.

Unacceptable uses of computers and the Internet include, but are not limited to, the following:

- Accessing inappropriate material (material that is sexually explicit, pornographic, or obscene) using the Internet;
- Swearing, using vulgarities, and/or any other inappropriate language, pictures, or gestures on the Internet in any form;
- Pursuing or passing on materials from the Internet that are demeaning to others or inherently inappropriate for student possession in an educational setting (material that advocates violence or discrimination against any person or group, humor of an offensive or sexually explicit nature);
- Changing any computer configuration, password, or file that does not belong to the user;
- Using the network for commercial use, financial gain, or illegal activity;
- Using an account other than your own or misrepresenting your identity;
- Attempting to "hack" or "mining" into any computer;
- Creating and/or distributing a computer virus or spam;
- Using the network to illegally transfer software (i.e. "pirating") in violation of copyright law;
- Internet surfing for personal purposes such as shopping, banking, research for personal purposes, online auctions (e.g. Amazon), chats, gaming, etc.
- Downloading unacceptable materials;
- Revealing any Personally Identifiable Information of students or staff;

- Causing damage to computer equipment or assisting others to cause damage;
- Installing or storing any software on any Cotter computer without permission from the Cotter Tech Department;
- Using any computer without permission of the teacher or staff member responsible for that computer;
- The following E-mail activities are not permitted: (1) sending chain letters and/or annoying, unnecessary messages to large numbers of people; (2) sending harassing, obscene, or threatening messages or pictures; (3) forging messages to make them appear to originate elsewhere; (4) using someone else's user name and/or password.

Personal Safety: Personal contact information concerning students, if shared inappropriately, may jeopardize personal safety. Students should not reveal any Personally Identifiable Information. They should not agree to meet someone they have met on-line. Under no circumstances should a student reveal his or her password to anyone.

Respecting Technology Resources: Student folders and E-mail should be checked frequently and unwanted messages and files deleted. Students should conserve technology resources (paper, toner, file storage space, etc.) Any attempt to damage/destroy school equipment, including but not limited to: hardware and software, the files of another user, creation and/or spreading of computer viruses, tampering with security or unauthorized files, and removing or exchanging any hardware or software component violates acceptable use of technology policy.

Consequences/Disciplinary Actions: Failure to abide by these guidelines will result in consequences that may include paying for damages, restitution, withdrawal of computer privileges, loss of E-mail and file server privileges, detention, suspension, or expulsion. When applicable, law enforcement may be involved.

Privacy Expectations: Users should expect only limited privacy in the contents of personal files in the school network. Files and E-mail are subject to routine maintenance and monitoring by designated staff. Cotter Schools reserves the right to delete any files that are inappropriate or may contain a virus. Requests for access to a user's account must be made to the IT Lead and HR Manager.

Off Campus Infractions: Cotter reserves the right to discipline a student for actions associated with media that occur off campus if the actions are intended to have an effect on another student or they adversely affect the safety and well-being of a student while in school.

Limitation of School Liability: Use of Cotter's network is at the user's own risk. The network is provided on an "as is, as available" basis. The school will not be responsible for any damage users may suffer, including, but not limited to: (1) loss, damage or unavailability of data; (2) delays or changes in or interruptions of service; (3) mis-deliveries or non-deliveries of information or materials, regardless of the cause.

The school is not responsible for the accuracy or quality of any advice or information obtained through the school computer network. The school will not be responsible for financial obligations arising from unauthorized use of the school computer network. Any financial obligation incurred by a student through activity on the network is the sole responsibility of the student or the student's parents. All

provisions of the acceptable use policy are subordinate to local, state, and federal laws. It is expected that each student and their parent/guardian read and comply with this Computer Acceptable Use Policy. Parents are expected to sign the Parent/Guardian Computer Responsibility Form during the annual enrollment/re-enrollment process.