

CLEARWATER U.S.D. 264
TECHNOLOGY POLICY FOR INFORMATION SERVICES
STUDENTS AND STAFF
(Approved 7/30/2012)

Access to computer and network services is a privilege; not a right. On a global network, it is impossible to control all material and at times, users may obtain access to inappropriate information or material. However, the Clearwater Unified School District (U.S.D. 264) has taken available precautions, including but not limited to enforcing the use of filters that block access to materials deemed harmful to minors.

It is the responsibility of all staff members to monitor students' online activity for appropriate behavior. Additionally, it is all staff members' responsibility to educate students about appropriate online behavior, including interactions with other individuals on social networking sites/chat rooms, and cyberbullying awareness and response.

The Board of Education reserves the right to modify and update this Technology Policy for Information Services (TPIS) and Acceptable Use Policy (AUP) at any time. It is the policy of U.S.D. 264 to expect that all technologies and electronic communications should be used in accordance with the district TPIS and AUP. The district retains the right to discipline any student, up to and including expulsion, and any employee, up to and including termination, for violations of this policy. Specific violations will be dealt with in the manner outlined in the appropriate personnel and student handbooks. Technology Expectations are outlined below.

PERSONAL RESPONSIBILITY: Each user shall accept personal responsibility for reporting any misuse of information services to the building principal or the Director of Technology.

ACCESS APPROPRIATE SITES: All Internet access by both students and staff passes through a Barracuda filtering solution that is updated frequently to reflect newly defined inappropriate content. The Barracuda attempts to block access to inappropriate sites and keeps a log of inappropriate sites that users' attempt to access. The internet filter may occasionally block a legitimate research site. Users may send an unblock request (helpdesk@usd264.net) if they feel a site has been inappropriately blocked. Each request will be reviewed by the Director of Technology for approval. Likewise, if a student or staff member inadvertently reaches a site that he/she feels should be blocked but is not, he/she should let his/her teacher or supervisor know. The teacher/supervisor will then send the URL to mdoud@usd264.org for immediate consideration to be blocked.

Users will access, save, or use only “school-appropriate” language, pictures, text, or any other data on/from the Internet. The following uses of district-provided Internet, network and e-mail are not permitted:

- To access, upload, download, or distribute pornographic, obscene, or sexually explicit material;
- To transmit obscene, abusive, insulting, harassing, sexually explicit, or threatening language;
- To use another’s password or allow someone to use your password;
- To intentionally introduce malicious code or viruses into any computer resource.
- Inappropriate use and/or transmission of any material via the Internet or any other method of violation of any United States or state law or regulation are prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material or material protected by a trade secret.

USE FOR LEARNING PURPOSES: Users will agree to use the Internet only for lawful and primarily school related purposes. School computer networks and Internet access are provided to support the educational mission of the school. Incidental personal use of school technologies must not interfere with the student’s learning function or the employee’s job performance, must not violate any of the rules contained in this policy, and must not damage the school’s hardware, software or computer systems.

ELECTRONIC COMMUNICATIONS: May include, but are not limited to email, chat, phone, and other Internet communications. Users shall have no expectations of privacy when using district electronic communications. Any email, computer application or information in district computer systems is subject to monitoring by the administration at any given time. All user communications, including text and images, that may indicate a violation of law or policy could be disclosed to law enforcement or other third parties without prior consent of the sender or receiver.

PASSWORDS: Users will protect their passwords and help to maintain the security of the network.

- Passwords should not be posted on computers because this undermines network security.
- The user shall not give personal information of students or staff, including name, password, etc., to others.
- A teacher giving his/her password to a student may be denied future Network privileges and may be disciplined, and possibly terminated, in addition to losing his/her privileges of access and use of the system.
- A teacher shall not give access to students to the Student Information System

(PowerSchool) for any reason for student confidentiality.

PERSONAL ELECTRONIC DEVICES: Electronic devices have become a common means of communication and information access. These devices have the potential of disrupting the orderly operation of the school. The school district has created a policy to govern the possession and use of electronic devices on school premises, during school hours, at school-sponsored activities, and on school transportation.

DEFINITION: Personal Electronic Device is defined as a privately owned wireless and/or portable electronic handheld equipment. This includes, but is not limited to, laptops, tablets and emerging mobile communication systems. Personal Electronic Device also includes any current or emerging wireless handheld technologies or portable information technology systems that can be used for word processing, wireless Internet access, image capture/recording, sound recording and information transmitting/receiving/storing, etc.

Possession of cell phones and other personal electronic devices on all school campuses and school buses, at school-sponsored activities and while the student is under the supervision and control of school district employees is permitted. These devices must be kept out of sight and powered off or silenced during the school day unless otherwise permitted by the district or school policy. Use of personal or district technology devices that disrupt the instructional day or includes possession, viewing, sending or sharing video or audio information having sexual, violent or threatening content on school grounds, school events or school buses is prohibited and will result in disciplinary action and/or confiscation of the personal technology device. The district retains the right to discipline any student, up to and including expulsion, and any employee, up to and including termination, for violations of this policy. By bringing personally owned devices to school, staff, students and their families accept that school authorities may inspect the device and its contents to ensure compliance with school and District codes of conduct, policies, and guidelines.

The student or staff member who possesses a personal technology device is responsible for its care. The district is not responsible for preventing theft, loss, damage, or vandalism to personal technology devices brought onto its property.

SPECIFICATIONS FOR PUBLISHING WEB PAGES TO THE DISTRICT WEB SERVER:

Identifiable student images shall not be posted on district or school websites without prior written permission from the student, and, if under 18, the student's parent or guardian. No personal student information shall be published on a school/district website (e.g., mailing address, telephone number, or other personally identifiable information). Any original materials created by students, such as poems, short stories, or art, are owned by those students. Original materials will not be posted on the district websites without prior written permission of the student who created the work, and, if under 18, the student's parent or guardian.

EMPLOYEE CREATED WEB PAGES AND/OR BLOGS: Employees may create or link to individual Web pages and/or blogs on an external site provided these external sites meet the District's specifications for publishing web pages as stated in the district policy. Any links to external sites that fail to meet the policy requirements will be removed.

1. Each external site must be on record with the district Information Technology Services department.
2. Each employee will be responsible for maintaining his/her Web pages or site blogs.

PARENTAL PERMISSION: In order for a student to gain access to the Internet and use of a computer, he/she must have parental permission as demonstrated by a signed Acceptable Use Policy on file with his/her school.

KEEP LAB/COMPUTER AREAS IN GOOD CONDITION

- Users will use the equipment with care.
- Report equipment or software problems to Information Services as helpdesk@usd264.org
- Remember to keep all food and drinks out of the computer area.
- Take the initiative to keep the lab or computer area clean and orderly by recycling unwanted paper, picking up personal items, etc.

EQUIPMENT AND SUPPLIES DISPOSAL: On a bi-monthly basis USD 264 will evaluate our current inventory and make necessary recommendations to eliminate obsolete equipment. Excess or unusable district-owned technology equipment and supplies will be disposed of at the discretion of the Director of Technology.

GIFT TO SCHOOLS: Any organization or individual making a technology gift to the district shall require the approval of the Director of Technology. All gifts will be regarded as district property.

Acceptable Use of Computers and Networks: Guidelines for Students



Available precautions, including but not limited to enforcing the use of filters that block access to obscenity, child pornography and other materials harmful to minors. On a global network, it is impossible to control all material and at times, users may obtain access to inappropriate information or material. It is all staff members' responsibility to educate students about appropriate online behavior, including interactions with other individuals on social networking sites/chat rooms, and cyberbullying awareness and response. It is also the responsibility of all staff members to monitor students' online activity for appropriate behavior. All users must share the responsibility for seeing that our computer facilities are used in an effective, efficient, ethical, and lawful manner. It is a privilege to have access to the resources, and therefore; all users must agree that they will comply with these guidelines.

When using the network or Internet:

- I will use appropriate behavior.
- I will be courteous to others on the network and on the Internet.
- I will use the equipment with care.
- I will use only software, which my teacher has assigned to me.
- I will connect only to sites, which have been allowed by the teacher
- I understand that the computer systems have been set up for me and may not be changed in any way.
- I will use only "school appropriate" language, pictures, and other data on the computer or network.
- I will follow the copyright laws, which protect programs, data books, and pictures. I will report problems to a teacher.
- I will leave all materials and equipment in good working order for the next user.
- I will remember to keep all food and drinks out of the computer area.
- I will help keep the computer area clean and orderly by recycling unwanted paper, picking up personal items, etc.
- I will have a teacher's permission for using the Internet, computer or lab.

Any user's computer privileges will be suspended for violating these guidelines. I understand and accept my responsibilities detailed above as a user of the Internet at any of the USD 264 facilities and I am aware that if I choose not to follow the guidelines, I will lose my Internet or network privileges.

Student Name (please print) _____ School _____

Student Signature Date _____

Teacher's Name _____ Teacher's Signature _____

I have read and understand the guidelines regarding appropriate use of the Internet by students. I also understand that there is objectionable material available on the Internet and by following these guidelines above, my child should not be exposed to this material. I further understand that precautions have been taken to restrict access to sites where the language, photos, text, etc. may be offensive. I agree to support and uphold the guidelines.

Parent/Guardian (please print) _____

Parent/Guardian Signature Date _____