

IJNDB TECHNOLOGY RESPONSIBLE USE GUIDELINES (TRUG)

The TRUG provides parents/guardians, students, and staff with a statement of purpose and explanation of the use of technology within the learning community. This procedure is reinforced by practice, responsible use guidelines and is required to be read before accessing the technology devices, digital resources, and network infrastructure. Students, parents/guardians and all staff members must also read and sign the accompanying statement of responsibilities in the handbook.

These guidelines are based on the Children's Internet Protection Act (CIPA) and its four guiding principles of: respect, privacy, sharing, and safety. These guidelines are appropriate for all technology users and we encourage parents to follow these guidelines in their own homes.

Orange Elementary, Petersham, and Ralph C. Mahar Districts (OES\PCS\RCM) provide access to electronic resources that promote educational excellence, sharing of information, innovative instruction, and online communication to enhance today's learners' ability to live and work in the 21st century. Online communication constitutes but is not limited to email, Internet, blogging and any use of network resources. OES/PCS/RCM electronic resources include, but are not limited to all hardware, software, data, communication devices, printers, servers, filtered Internet access, and local and wide area networks.

Online communication is critical for today's learners to apply 21st Century Skills and employs tools such as interactive websites, blogs, video conferencing, podcasts, which offer authentic opportunities for students to express and share information. To keep students safe and comply with the Children's Internet Protection Act (CIPA), the TRUG is put in place and updated to accommodate for the many educational and global changes to date. This TRUG is written for all those who use electronic devices in our schools. These electronic devices may be used for classroom blogs, student emails, podcast projects, interactive websites, and any other occasion by students, teachers, and staff or community members.

The following is a statement of rules and guidelines for the responsible use of electronic devices. These are provided to help understand what is responsible behavior regarding the use of technology. While these rules and guidelines detail responsible use of electronic information resources anywhere, these are rules and guidelines under which all members of the OES/PCS/RCM community (students and staff) will be held accountable.

USAGE GUIDELINE

OES/PCS/RCM provide students and staff access to various electronic resources including a wide range of educational materials through Internet and computer online services.

Content Filtering

The OES/PCS/RCM Schools use software designed to block access to certain sites and filter content as required by the Children's Internet Protection Act, 47 U.S.C. §254 (CIPA). The OES/PCS/RCM Schools are aware that not all inappropriate information can be filtered, and the district will make an effort to correct any known gaps in the filtering of information without unduly inhibiting the educational use of age appropriate content by staff and students. Users will inform teachers or administrators of any inadvertent access to inappropriate material, in order that there is appropriate modification of the filtering profile. OES/PCS/RCM Schools educate students about appropriate online behavior, including interacting with other individuals on social networking web sites and in chat rooms as well as cyberbullying awareness and response.

Student Safety. Do not send any message that includes personal information such as: home address, personal phone numbers and/or last name for yourself or any other person. Likewise, the staff is not permitted to post this information to public domains (i.e. class web page or Internet). Student pictures and/or work may only be included on district/ school/ classroom websites with parent/guardian permission and without identifying captions unless the site is password protected.

Extended Safety PK 6. Teachers of students in grades PK-2 will access appropriate websites for their students. Students in grades 3-6 may not attempt to access any Internet resource without the prior consent and supervision of staff.

Password Protection. Passwords are provided for each user's personal use only and are, therefore, confidential. Never share your password, steal or use another person's password. If you suspect that someone has discovered your password, you should change it immediately and notify your teacher or administrator who in turn will notify the network administrator or the technology director. As words are easily hacked, when establishing a password one should keep in mind that strong passwords consist of a combination of upper and lowercase letters, numbers and symbols.

Privacy. Email is no more private than a postcard. Students and staff need to know that files stored on school computers are not private. Network and Internet access is provided as a tool for educational purposes only. The District has the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access including transmitted and received information. All information files are the property of the District and no user shall have any expectation of privacy regarding such files. Federal Law requires that all email sent and received be stored for a period of seven years.

Online Etiquette. Follow the guidelines of responsible behaviors within the school handbook. Use appropriate language and graphics. Swearing, vulgarities, suggestive, obscene, belligerent, harassing, threatening or abusive language of any kind is not acceptable. Do not use school online access to make, distribute, or redistribute cyber bullying, obscene material or material which is based on slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, gender identity or sexual orientation.

Messaging. Teachers may incorporate: email, blogs, podcasts, video conferencing, online collaborations, electronic devices, IMing, texting, social media, Virtual Learning Environments and other forms of direct electronic communications or Web 2.0 applications for educational purposes. Although teachers monitor student online activity, it is the direct responsibility of the user to comply with this TRUG.

Web 2.0 Tools. Uses of blogs, podcasts, or other Web 2.0 tools are considered an extension of the classroom. Whether at home or in school, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, podcasts, or other Web 2.0 tools. Students using blogs, podcasts or other Web 2.0 tools are expected to act safely and responsibly by keeping all personal information out of their posts. Comments made on school related blogs should follow the rules of online etiquette detailed above and will be monitored by school personnel. If inappropriate, they will be deleted. Never link to web sites from a blog without reading the entire article to make sure it is appropriate for a school setting.

Student Emails to Staff

Students are encouraged to email staff concerning school-related content and questions. However, there will be no requirement or expectation for staff to answer student email outside of their regular work day, although they certainly may if they choose. For example, an unanswered email to a teacher would not excuse a student from turning in an assignment.

General Email and Online Chat Guidelines

Below is a general summary of guidelines related to email and any form of online chat or instant messages:

Email and online chat is to be used for school related communication. Do not send harassing email or instant messages or content.

Do not send offensive email or instant messages or content. Do not send spam email or instant messages or content.

Do not send email or instant messages containing a virus or other malicious content.

Do not send or read email or instant messages at inappropriate times, such as during class instruction.

Do not send email or instant messages to share test answers or promote cheating in any way. Do not use the account of another person.

Plagiarism/Copyright/Licensing. Plagiarism is the act of using someone else's words or ideas as your own. Students are required to give proper credit to all Internet sources used in academic assignments, whether quoted or summarized. This includes all forms of media on the Internet, such as graphics, movies, music, and text. Plagiarism of Internet resources will be treated in the same manner as any other incidences of plagiarism, as stated in the school handbook. In addition, all students and faculty must adhere to the copyright laws of the United States (P.L.94553) and the Congressional Guidelines that delineate it regarding software, authorship, and copying information. All students and faculty should also adhere to the Creative Commons licenses where the author/artist denotes what media may be shared, remixed, or reused.

Proxies. The use of anonymous proxies to get around content filtering is strictly prohibited and is a direct violation of this agreement.

Illegal Activity. Use of any electronic devices for any illegal activity is prohibited. Illegal activities include, but are not limited to: (a) tampering with computer hardware or software, (b) software piracy (c) unauthorized entry into computers and files (hacking), (d) knowledgeable vandalism or destruction of equipment, (e) deletion of computer files belonging to someone other than oneself, (f) uploading or creating of computer viruses, (g) distribution of obscene or pornographic materials, (h) sexting and (i) cyber bullying.

Such activity is considered a crime under state and federal law. Users must be aware that any illegal action carried out over the Internet will be reported to law enforcement officials for possible prosecution. Please be advised, it is a federal offense (felony) to break into any security system. Financial and legal consequences of such actions are the responsibility of the user (staff, guests, and student) and student's parent or guardian.

Social Media. In accordance with OES/PCS/RCM school district policies, the use of social media sites as a method for staff to push information out to students, parents, and community members is allowed. Below are **examples** of minimum information required for faculty to provide to building Principals and/or their designees (i.e., IT department).

Twitter:

Must submit username and page URL to Principal.
Account needs to be created with your district email address.
Can not follow student accounts.

Facebook:

Must be a business page where users can only “Like” the page.
Account needs to be created with your district email address.
Must submit page URL to the Principal.

Google+:

Account needs to be created with your district email address.
Can only follow student accounts created with their district email address.

TERMS OF AGREEMENT

The OES/PCS/RCM Schools reserve the right to deny, revoke or suspend specific user privileges and/or to take other disciplinary action, up to and including suspension, expulsion (students), or dismissal (staff) for violations of these Guidelines. The Districts will advise appropriate law enforcement agencies of illegal activities conducted through the OES/PCS/RCM Internet connection. The Districts also will cooperate fully with local, state, and/or federal officials in any investigation related to any illegal activities conducted through the network. The school districts and its representatives are not responsible for the actions of the users or the information they access.

Adopted:

4/1/2015 Orange Elementary

Orange Elementary, Orange, MA