YSO Policy: Appropriate Use of Technology

This is a policy from an independent public school district for high school and middle school-aged youth. For this policy, BE SAFE recommends the following:

- **Specify the disciplinary or legal action that will result from violation of this policy.**

<u>Policy:</u>

Students may use the Technology Resources for educational purposes. The Technology Resources are defined as the Program's network, servers, computer workstations, telephones, peripherals, applications, databases, library catalog, online resources, Internet access, email, online class activities and any other technology designated for use by the Program for students. With this educational opportunity comes responsibility. Inappropriate system use of the Program's Technology Resources will result in the consequences below, including loss of the privilege to use this educational tool.

The Internet is a network of many types of communication and information networks, which are used frequently in program assignments and include access to library materials and purchased online databases. Some material accessible via the Internet may contain content that is illegal, inaccurate, or potentially offensive to students (or their parents/guardians). It is possible for students to access (accidentally or otherwise) these areas of content. While the Program uses filtering technology and protection measures to restrict access to such material, it is not possible to absolutely prevent such access. It will be each student's responsibility to follow the rules for appropriate and acceptable use.

<u>RULES FOR APPROPRIATE USE:</u>
- Students must only open, view, modify, and delete their own computer files, unless they have specific permission from a teacher or staff member to do otherwise.
- Internet use at the Program must be primarily related to program assignments and projects.
- Students may be assigned individual accounts to Program resources and must use only those accounts and passwords that they have been granted permission by the Program to use. All account activity should be for educational/programmatic purposes only.
- Students are responsible at all times for their use of the Program's Technology Resources and must assume personal responsibility to behave ethically and responsibly, even when technology provides them the freedom to do otherwise.

<u>INAPPROPRIATE USES:</u>
- Using the Program's Technology Resources for illegal purposes (e.g., gambling, pornography, computer hacking).
- Disabling, bypassing, or attempting to disable or bypass any system monitoring, filtering or other security measures.
- Sharing/borrowing usernames, passwords, account access or logging in for someone else.
- Purposefully opening, viewing, using, or deleting files belonging to another system user without permission.
- Electronically posting confidential personal information about yourself or others (i.e. addresses, phone numbers, pictures).
- Downloading or plagiarizing copyrighted information without permission from the copyright holder.
- Intentionally introducing a virus or other malicious programs onto the Program's Technology Resources.

- Electronically posting messages or accessing materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
- Wasting or abusing program resources through unauthorized system use (e.g., online gaming, streaming music and/or video, unauthorized chatting or abuse of student e-mail, etc.).
- Gaining unauthorized access to restricted information or network resources.

PERSONAL WIRELESS/MOBILE DEVICES:
Personal wireless and mobile devices will be provided filtered access to the Internet as well as access to any web-based student applications that would normally be accessible to students from home. The Program is not responsible for the loss or theft of a personal device, nor for damage, nor unauthorized access to the device nor the data that resides therein. In addition:

- The student must take full responsibility for setting up and maintaining their personal wireless and mobile devices. The Program will not provide technical support for these devices.
- When personal wireless and mobile devices are not in the student's possession, they must be secured by the student. Laptops must never be left unattended. Laptops may not be left at school over vacations. Laptops must go home with students daily.
- The playing of games, music, or other entertainment on personal wireless and mobile devices is prohibited at the program. Electronic communication such as e-mail, instant messaging, chat, blogs, etc are also prohibited at the program unless an approved and monitored application is being used for educational purposes by the teacher.
- Sound on personal wireless and mobile devices must be turned off except when it is being used as part of instruction.
- Student selection of appropriate, tasteful screensavers and wallpaper is expected.
- The Program may examine any personal wireless or mobile device and search its contents, if there is a reason to believe that program policies, regulations, or guidelines have been violated.
- All students with personal wireless or mobile devices being used for instruction or other Program business must use the Program provided wireless network which is filtered according to the Children's Internet Protection Act (CIPA) requirements.
- Personal laptops and wireless devices are permitted for use by all staff and students, however, they are never to be plugged into the wired network (i.e., computers, wall jacks, other Program equipment, etc.).
- If a student uses a personal device in an inappropriate manner, they will lose their privilege of bringing a personal laptop to school.

CONSEQUENCES FOR INAPPROPRIATE USE:
- Suspension of access to the Program's Technology Resources;
- Revocation of the Program's Technology Resources account(s); and/or
- Other appropriate disciplinary or legal action in accordance with the Code of Conduct and applicable laws.