

Internet Safety Policy

Fiddlehead School recognizes that Internet access is essential to the mission of the School. Inherent in Internet access is the potential for viewing information or content that is contrary to the mission of the School. The School Network—computers, network, and Internet (the “Network”)—brings many resources to our school communities and allows communication on a previously unheard-of scale. The Network is a resource from which all users—students, staff, parents and community members—will pursue learning with the same set of standards for behavior and intellectual effort.

At the same time, the unregulated availability of information and communication on the Internet requires that the School establish reasonable controls for lawful, efficient, and appropriate use of this technology.

To minimize risk of harm to Network users, the School is implementing a policy to:

- i. Prohibit access by users to inappropriate matter on the Internet and World Wide Web through the use of filtering software;
- ii. Promote the safety and security of users when using electronic mail, chat rooms, and other forms of direct electronic communications;
- iii. Prohibit unauthorized access, including so-called “hacking,” and other unlawful activities by users online;
- iv. Prohibit unauthorized disclosure, use, and dissemination of personal information regarding users; and
- v. Promote measures designed to restrict users’ access to materials harmful to minors.

To minimize risk of harm to Network users, the School shall provide the following:

1. **Supervision:** Whenever possible, classroom, library, and lab computer screens should be visible to the teacher if students are using them for Internet or e-mail access. All lab computers should be visible from the front of the room. In classrooms, where computer placement is more difficult, teachers should develop procedures so students know the teacher could be walking by at any moment.
2. **Training:** A staff development program will be established to ensure staff members are current on Internet policy and use. The primary focus will be for staff to assist students in achieving the School’s mission. Students will be trained in appropriate use, provided with strategies to evaluate the material they locate on the Internet (including interacting with other individuals via social networking websites and the like), and taught cyberbullying awareness and response.
3. **Internet Acceptable Use Policy:** All Network users are required by policy to read and abide by our Internet Acceptable Use Policy. This places the responsibility for abuses on the

shoulders of the abuser, rather than the teacher or the school, but does not remove the need for adequate supervision.

4. **Internet Filtering:** The School will employ an Internet security appliance with the content filtering subscription which will at minimum filter 1) visual depictions of obscenity, (2) visual depictions of child pornography, and (3) materials otherwise harmful to minors.

The Executive Director will designate an authorized person(s) to disable the blocking or filtering measure during any use by an adult to enable access for bona fide research or other lawful purpose on a single machine.

Legal References: Children's Internet Protection Act (CIPA)

Adopted: September 20, 2016

Reviewed: October 17, 2020