

Acceptable Use Policy

The school provides electronic information resources (including, but not limited to, computers, computer accounts and services, networks, software, electronic mail services, electronic information servers, web pages, and related services) to assist members of the Flintridge Prep community in the pursuit of education, and to serve as an information resource for past and potential members of that community. As general rule, acceptable use of school-provided technology will further those goals and will be consistent with the school's Honor Code, which requires every member of the community to be honest, kind, generous, and respectful. Further, acceptable use follows community standards of appropriateness and decorum; obeys school policy, local, state, and federal laws; and does not compromise the school's mission or its educational or legal status.

The following are examples of prohibited uses:

1. Use in violation of any applicable local, state, or federal law, including (but not limited to) infringement of copyright laws.
2. Use that is inconsistent with the non-profit status of the school. This includes support of non-school-related commercial activities.
3. Presenting material that represents, or purports to represent, an official school position or policy without specific authorization to do so.
4. Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others.
5. Harassing or threatening use. This includes making or posting photos, or video or sound recordings, of any member of the community that embarrass, insult, denigrate, or harass that person, without that person's express permission.
6. Making or posting recordings of any instructional activity, such as classes, lectures, rehearsals, coaching sessions, practices, or tutoring sessions, without the express permission of the faculty member in charge and the knowledge of student participants.
7. Misrepresenting the identity of the provider of information, the person responsible for providing information, or the fraudulent use of a user's authorization to access school systems or to distribute information.
8. Accessing the school network, or using school systems, using another user's login account, even if it is done with that user's knowledge and permission. The login-account owner will be considered to be equally as responsible for any harm caused by an account as the person who actually caused the harm.
9. Knowingly distributing viruses, trojans, worms, or other malicious programs.
10. Connecting any computer that does not have anti-virus software installed to the school network.
11. Unauthorized installation of any software on school computers.
12. Use of peer-to-peer file-sharing applications (such as bittorrent); operation of an unauthorized server, either on school computers or on personal computers that are connected to the school network.
13. Use of any software that compromises security or degrades network, server, or client-system performance.
14. Unauthorized access of any network or computer-based resource, including but not limited to files, drives, applications, or devices.