

Computer Ethics Terms

1. Acceptable Use Policy – a set of guidelines or rules adopted by a school or other organization that governs Internet, network, and information technology use.
2. Computer crime – a crime committed using a computer, usually to gain access to restricted files, systems, or information. These crimes can resemble trespassing, vandalism, or theft.
3. Computer virus – a small, intentionally, created computer program that causes damage to computer workstations, personal computers, or computer networks. This is a generic term that also includes worms, Trojan horses, and bombs.
4. Data privacy – the concept that an individual has a right to say who has personal information about him or her and how that information is used. With the spread of digital information gathering and recordkeeping, data privacy is becoming more difficult to maintain.
5. Flame – an emotionally, often profane, response to an action or statement in a chat-room, electronic discussion group, or newsgroup.
6. Hacker/Cracker – an individual who gain unauthorized access to computerized information or computer systems. The term “cracker” implies there is malicious intent to the access.
7. Intellectual property rights – the concept that a person’s ideas, writings, and constructions (like computer software) that may not exist in a physical sense should be treated as property and the creators or owners of this property have rights to its sale, use, and control.
8. Netiquette – a term taken from a combination of “network” and “etiquette” that means a code of polite, thoughtful, or respectful behaviors to be followed while using networks, including the Internet.
9. Newbie – a new user of networked resources who may not yet know the rules of “netiquette” and runs a risk of being “flamed” for rude behavior.
10. Peer-to-peer (P2P) file sharing – a type of file sharing that allows computer users with the same program to connect with each other and access files from one another’s hard drives rather from a central server. Napster, Gnutella, KaZaA, and Limewire are examples of peer-to-peer software.
11. Plagiarism – the use of another’s ideas or words as one’s own.
12. Pornography – material, usually of a sexually explicit nature, that is inappropriate for use under certain conditions, such as in a school, with children, where unlawful, or where its presence can be considered a form of harassment.
13. Spoofing – the use of another’s identity when online.
14. Virtual space – the environment created by computer networks in which data is stored and communication transpires. Also termed “cyberspace.”

Ethical use is the most generic term that applies to actions that may be considered right or wrong.
Safe use applies to situations in which physical harm may come to a user or user’s property.
Moral use applies to situations to which religious or spiritual values apply. (Is the action good or evil?)
Appropriate use applies to actions which may be right or wrong depending on when, where, and with whom they happen.
Legal use applies to situations in which established laws are violated.