

CAMBRIDGE RESCUE SQUAD Computer Use Policy

Section I: Purpose

The purpose of this document is three-fold. This document is intended to:

1. Guide, not govern, the use of computers and the network of the CAMBRIDGE RESCUE SQUAD.
2. Prohibit certain unacceptable uses of the CAMBRIDGE RESCUE SQUAD computers and network.
3. Educate users about their responsibilities.

Section II: General Information

1. Computer files are intellectual property under national and international law. Any copying of files without express permission from the owners is stealing.
2. All computers, networking equipment, and other peripherals are the property of the CAMBRIDGE RESCUE SQUAD and should be used with respect and not removed from the building without express permission.
3. Virtually all computers at the CAMBRIDGE RESCUE SQUAD have high-speed access to the Internet. Access is intended for research, education and communication, not for entertainment, shopping, or personal enrichment.

(For its own protection, the CAMBRIDGE RESCUE SQUAD reserves the right to block all Internet communications from sites involved in disruptive practices as well as the right to restrict access of individuals not following the CAMBRIDGE RESCUE SQUAD guidelines.)

4. Generally, the same ethical and professional conduct that applies to other CAMBRIDGE RESCUE SQUAD activities applies to use of electronic information resources.
5. Individuals making use of electronic communication are warned that they may willingly or unwillingly receive or discover material they find offensive. When sending electronic transmissions, users should realize that tone-of-voice, facial expressions and other usual communication cues are absent. Therefore, careful writing and judicious use of words is advised.
6. CAMBRIDGE RESCUE SQUAD will provide a username and password to all members to gain access to the computers and network. Furthermore, any members requiring an email account will be provided one whenever possible.

Section III: Guidelines

1. No one shall use and CAMBRIDGE RESCUE SQUAD computer without proper authorization.
2. No one shall connect any personal computer to the CAMBRIDGE RESCUE SQUAD network unless it has been approved by the network administration.
3. System administrators shall perform their duties fairly and respect the privacy of users as far as possible and refer all disciplinary matters to the appropriate authorities.
4. No one shall give any password for any CAMBRIDGE RESCUE SQUAD computer/network to any unauthorized means. No one except the network administrators are authorized to issue passwords for computers.
5. No one shall copy, install, or use any software or data files in violation of applicable copyrights or license agreements.
6. No one without authorization shall modify or reconfigure the software or hardware of any CAMBRIDGE RESCUE SQUAD computer or peripheral.
7. Users shall take full responsibility for messages that they transmit through the CAMBRIDGE RESCUE SQUAD network. No one shall use CAMBRIDGE RESCUE SQUAD computers to transmit fraudulent, defamatory, harassing, obscene, or threatening messages, or any communications prohibited by law.
8. No one shall use CAMBRIDGE RESCUE SQUAD communication facilities to attempt unauthorized use, nor to interfere with others' legitimate use, of any computer or network facility anywhere.
9. All users shall share computing resources and cooperate with other users of the same equipment.
10. No one without specific authorization shall use any CAMBRIDGE RESCUE SQUAD computers or network for non-CAMBRIDGE RESCUE SQUAD business.

11. No one shall misrepresent his/her identity or relationship to CAMBRIDGE RESCUE SQUAD when obtaining or using CAMBRIDGE RESCUE SQUAD computer privileges.
12. No one without specific authorization shall read, alter, or delete any other person's computer files or electronic mail.
13. Users shall not place confidential information in computers without protecting it appropriately. CAMBRIDGE RESCUE SQUAD cannot guarantee the privacy of files, electronic mail or other information stored by computer.
(Ordinary electronic mail is not considered private!)
14. No one shall knowingly endanger the security of any CAMBRIDGE RESCUE SQUAD computer or network, nor willfully interfere with others authorized usage.
15. No one shall create, install, or knowingly distribute a computer virus or other destructive program on any CAMBRIDGE RESCUE SQUAD computer or network, regardless of whether demonstrable harm results.

Section IV: Prohibited Behaviors

Prohibited behaviors include but are not limited to the following:

1. Sending harassing, intimidating and/or threatening messages through electronic mail or other means.
2. Intentionally intercepting, disclosing or using any electronic communication to which authorized access is not explicitly provided.
3. Providing others with access to one's personal computer account, or gaining or attempting to gain access to personal computer accounts, files, or electronic info of others.
4. "Hacking" or otherwise attempting to compromise CAMBRIDGE RESCUE SQUAD computer security.
5. Creating or releasing computer viruses or other destructive activities.
6. Interfering with normal operations of computer systems hardware or software.
7. Modifying, altering or otherwise tampering with systems or peripherals.
8. Copying or distributing commercial or other copyrighted software or proprietary data not in the public domain.
9. Use of CAMBRIDGE RESCUE SQUAD computers and/or services to perpetuate fraud, misrepresentation or illegal activity.
10. Use of CAMBRIDGE RESCUE SQUAD computers and/or services for commercial purposes or unauthorized financial gain.
11. Any act chargeable as a violation of local, state or federal law, whether or not charge are brought by civil authorities.

Section V: User Responsibilities

All users of CAMBRIDGE RESCUE SQUAD computers or networks have the following responsibilities:

1. learning how to use information technology
2. backup and security of your own work and files
3. use resources efficiently
4. use electronic equipment properly
5. abide by all security provisions
6. obey copyright law
7. recognize limitations to privacy in electronic communications
8. understand the limitations of our electronic resources
9. read and understand this computer use policy

All information contained in this document had been adapted fro use from the following computer use policies:

- University of Southern California
- Chemeketa Community College
- Earlham College
- University of Georgia