KECK GRADUATE INSTITUTE
ACCEPTABLE USE POLICY for
COMPUTING, INTERNET and NETWORK RESOURCES

OVERVIEW

In support of the mission of Keck Graduate Institute (the Institute) of education and research aimed at translating into practice, for the benefit of society, the power and potential of the life sciences, the Institute makes available computing, Internet and network resources including, but not limited to, local area network (LAN), wide area network (WAN or Internet), wireless local area network (WLAN), secure shell (SSH), virtual private network (VPN), electronic mail (e-mail), computers, printers, scanners, network drives, and other resources which may be used by its students, faculty, staff and other authorized users. The use of these resources is a nontransferable, revocable privilege, not a right arising from employment or association with the Institute community.

The computing, Internet and network resources of the Institute are administered by the Information Technology (IT) Department under the direction of the Director of IT, and the Vice President for Finance and Operations. All such resources are to be used to promote education and learning and to carry out the administrative services of the Institute. The Institute reserves the right to change its use policy and procedures at any time, without advance notice, subject to approval by the VP of Finance and Operations and/or President.

Use of the Institute's computing, Internet and network resources is governed by federal and state laws as well as the Institute's own behavioral standards expressed in its community standards, policies and procedures and as outlined in this document. While the Institute does not routinely inspect, monitor, read, retrieve, or disclose user communications, nevertheless, as a condition of using the Institute's computing, Internet and network resources each user consents and authorizes the Institute to conduct such activities without users prior consent and/or notification.

Users of the Institute's computing, Internet, and network resources should not expect that their use will be private or confidential. No user should have any expectation of privacy in any message, file, image or data created, sent, retrieved, received, or posted using the Institute's equipment and/or access. It is the responsibility of each user to know and to comply with applicable laws, standards, policies and procedures. The following information is provided to help all users understand what acceptable use is, what unacceptable use is, what their responsibilities are, and what the consequences of misuse are.

ACCEPTABLE USE

The following represents a guide to acceptable use of computing, Internet and network resources. It is not intended to identify all acceptable uses, but to indicate those uses which are clearly consistent with the purposes of these resources at the Institute.

1. Communication regarding the Institute's business purposes.

2. Communication regarding the educational, academic, and professional activities of faculty, students, and staff that are relevant to the Institute.

3. Communication regarding official Institute work performed by offices, departments, recognized campus organizations, and other constituencies of the Institute.

4. Personal use incidental to the primary purposes of promoting education and learning and/or carrying out the administrative functions of the Institute.

5. Business related communication intended for Institute-wide distribution. Distribution lists are to be secured and maintained for the express purpose of notifying the Institute community at large or its designated constituencies of announcements and information relating to the conduct of Institute business.

6. Communication to known constituencies for the purpose of conducting business relating to the Mission of the Institute.

Content generated by the use of the resources must be in keeping with the Institute's Code of Conduct, as well as federal and state laws.

Acceptable use always includes:

1. Respect for the rights of others including the rights of privacy and freedom from harmful and/or offensive intrusions.

2. Respect for intellectual property rights as legally protected by copyright and license to programs and data as well as contractual obligations.

3. Respect for the integrity of the computing, Internet, and network systems.

Questions as to what is or is not an acceptable use should be directed to the Director of IT and/or the Vice President for Finance and Operations. The Director of IT and the Vice President for Finance and Operations may at any time make a determination as to the whether or not a particular use is or is not consistent with the purposes of the Institute's computing, Internet and network resources and is therefore acceptable or unacceptable.

UNACCEPTABLE USE

The following list characterizes unacceptable use. It is not intended to identify all unacceptable uses, but to indicate the types of uses that are clearly inconsistent with the purposes of these resources at the Institute. Such use is subject to consequences.

1. Damage to or destruction of equipment, software or data belonging to the Institute or others.

2. Disruption or unauthorized monitoring of electronic communications.

3. Creating and/or willfully disseminating computer viruses and turning off installed security software on Institute provided computers, e.g., antivirus, anti-spyware, etc.

4. Violation of computer system security.

5. Use of peer-to-peer (P2P) or related file sharing program for anything other than official Institute business

6. Attempt to gain unauthorized access, whether successful or not.

7. Access or retrieval of any stored information without authorization to do so and the storing of Institute data on offsite servers.

8. Unauthorized use of computer accounts, access codes and/or passwords assigned to/by others. At no point should employees share usernames or passwords with other employees.

9. Misrepresenting your identity and/or account in any matter.

10. Use of obscene, vulgar, foul or abusive language and/or disinformation.

11. Posting on electronic bulletin boards anything that violates the Institute Code of Conduct.

12. Academic dishonesty (plagiarism, cheating, et al).

13. Use for the purpose of promoting, viewing, or obtaining pornography and/or sexually explicit text or graphics.

14. Use of visuals and sounds which may be offensive and/or disruptive to others.

15. Any violation of federal and/or state laws.

16. Use of e-mail, chat rooms on the Internet or any other network resource as pranks or in a threatening or harassing manner.

17. Use of e-mail or any other network resource to malign the reputation or integrity of any individual, and/or to libel, and/or to slander others.

18. Violating the privacy of another user, including, but not limited to, unauthorized disclosure of student academic and disciplinary matters and/or employee personnel matters.

19. Individuals, offices, and departments may not independently send large group or Institute-wide e-mail unless approved in advance by a Dean or Vice President.

20. Electronic eavesdropping on electronic communication facilities.

21. Violation of copyrights, software license agreements, and/or patent protections.

22. Sending of copyrighted material, proprietary financial information, or confidential personnel information without prior authorization.

23. Representing, giving opinions, or otherwise making statements on behalf of the Institute unless authorized to do so.

24. Commercial purposes of any type.

25. Unsolicited advertising.

26. Personal financial gain in any form.

27. Using computing, Internet or network resources for fundraising for non-Institute organizations.

28. Transferring use to another individual or organization.

29. Personal uses of the resources that may cause interference with the operation of the Institute's information technologies, or burden the institute with incremental costs.

30. Use of Institute resources for online game paying.

31. Creating, sending, and/or forwarding electronic chain letters.

32. Unnecessarily impeding the computing activities of others.

33. Turning off any security application installed on an Institute computer, e.g., anti-virus, anti-spyware, or anti-spam software.

All unacceptable uses are also a violation of your responsibilities as a user.

USER RESPONSIBLITIES

By using the Institute's computing, Internet and network resources, you are agreeing as a condition of use to accept personal responsibility for considerate, ethical, and responsible behavior in your use of the available resources.

1. You are responsible to use the resources only for acceptable uses such as those identified above.

2. You are responsible to use the resources in compliance with applicable laws and Institute Code of Conduct standards, policies and procedures. It is your responsibility to determine what restrictions apply and to review the Institute's on-line policies and procedures that will be updated continually.

3. You are responsible to use the resources with sensitivity to the rights of others. It is your responsibility to avoid intrusions into the privacy of others and/or to avoid creating an atmosphere of discomfort or harassment for others.

4. You are responsible for the security of your account/s. It is your responsibility to access your account/s with a password that will protect it from unauthorized use and to change that password at a minimum of every six (6) months. If you discover that someone has made an unauthorized use of your account/s, you are to report the intrusion to the Institute's IT Department and to change your password. The Institute assumes no responsibility for the security of your account/s.

5. The Institute assumes no responsibility for lost or corrupted data. You are responsible to make any back-ups of such data that you have created or maintain.

6. You are responsible to report any weakness you discover in the security of the computing, Internet, and network resources to the Institute's IT Department at 909.607.0387. You are not to explore a weakness on your own as this may be interpreted as intentionally tampering with the Institute's resources and be treated as a violation of criminal law as well as this policy. If you wish to assist in resolving a security weakness in the system, contact the Institute's IT Department.

7. You are responsible to identify clearly and accurately any on-line communication including messages, sentiments and declarations as coming from you. If you are acting as the authorized agent of the Institute, the communication must be identified as coming from the Institute.

8. You are responsible to take steps to avoid being a victim or an unwitting distributor of computer viruses or other destructive computer programs. The Institute assumes no responsibility for avoidance of or for the impact of computer viruses or other such destructive programs.

9. You are responsible for the confidentiality and security of any personal information that you store or disclose, such as your credit card number. The Institute assumes no responsibility for any loss you incur as a result of any such storage or disclosure.

CONSEQUENCES AND MISUSE

Misuse of Institute computing, Internet, and/or network resources may result in one or more of the following consequences which may be implemented at the discretion of the Director of Human Resources, the Associate Vice President for Business and Finance, or the Vice President for Finance and Operations.

1. A written warning to the user.
2. A restriction on use privileges.
3. A revocation of all use privileges.
4. Implementation of the Institute's procedures for responding to alleged violations of community standards which could result in suspension or expulsion from the Institute and/or termination of employment by the Institute.
5. Immediate suspension or termination from employment by the Institute.
6. Financial restitution to the Institute for funds owed and/or expended because of misuse.
7. Referral to civil or criminal authorities for prosecution.
8. A demand for indemnification for any loss or damage suffered by the Institute.

WARNINGS

1. The Institute reserves and intends to exercise its right to inspect, monitor, read, retrieve, and/or disclose all messages created, received, or sent over its resources, and all files, data or information stored on its resources when violation of this or any other Institute policy is suspected or alleged or for any other reason. The Institute may provide the results of the exercise of this right to appropriate government authorities or other third parties. The contents of electronic communications files data or other information may also be disclosed within the Institute without notice or the permission of the students, faculty, staff, and other authorized users.
2. Notwithstanding the Institute's right to inspect, monitor, read, retrieve, and disclose any electronic communication, such messages should be accessed only by the intended recipients and/or authorized Institute personnel. Any exception to this must receive prior

approval by the Vice President for Finance and Operations or the Director of Human Resources.

3. The use of passwords for security does not guarantee confidentiality. Therefore, the confidentiality of any message should not be assumed. Remember that the recipient of your message may forward it to others. Also, when a message is deleted, it is still possible to retrieve and read that message, and it may be subject to disclosure under federal or state law.

4. Any electronic mail and any account assigned and/or associated with the resources provided by the Institute are the property of the Institute.

5. Some of the resources available through the network may contain objectionable material and/or potentially offensive material. The Institute neither assumes responsibility for the content of those resources unrelated to the Institute and over which it has no control, nor endorses any of their contents.

6. The Institute cannot guarantee that an electronic communication received was actually sent by the purported sender. In case of doubt, validate the authorship and authenticity of any electronic communication.

7. Security for electronic communications is not provided by the Institute. Therefore, disclosure of personal information is discouraged especially through e-mail. The Institute assumes no responsibility for any consequences incurred because of disclosure of personal information.

The Institute reserves the right to change this policy and its procedures at any time, without advance notice, subject to approval by the Vice President for Finance and Operations. Questions related to the Institute IT policies should be directed to the Institute's Director of IT.

IT CONTACT
KGI - Information Technology Department
535 Watson Drive
Claremont, CA 91711
helpdesk@kgi.edu

_____
Employee's Name (Print)

_____ _____
Employee's Signature Date

Effective Date: November 14, 2014 Amendment Date: September 14, 2015
Administrator: Human Resources/ IT Department
Approval Authority: Cabinet