Purpose
California Institute of Integral Studies (the “Institute”) relies on its computer network to conduct its business. To ensure that its computer resources are used properly by its students, the Institute created this Computer Use Policy (the “Policy”).

The rules and obligations described in this Policy apply to all users (the “Users”) of the Institute’s computer network, wherever they may be located. Violations will be taken very seriously and may result in disciplinary action and civil and criminal liability initiated by the Institute, or its employees, students, independent contractors, agents, and other computer users.

It is every student’s duty to use the Institute’s computer resources responsibly, professionally, ethically, and lawfully.

Definitions
From time to time in this Policy, we refer to terms that require definitions:

The term Computer Resources refers to the Institute’s entire computer network. Specifically, Computer Resources includes, but are not limited to: host computers, file servers, application servers, communication servers, mail servers, web servers, databases, workstations, stand-alone computers, laptops, software, data files, and all internal and external computer and communications networks (for example, Internet, commercial online services, value-added networks, email systems) that can be accessed directly or indirectly from our computer network.

The term Users refers to all students and other persons or entities who use our Computer Resources.

Policy
The Computer Resources are the property of the Institute and may be used only for legitimate business and academic purposes. Users are permitted access to Computer Resources to assist them in their academic career. Use of the computer system is a privilege that may be revoked at any time.

In using or accessing our Computer Resources, Users must comply with the following provisions.
A. ACADEMIC FREEDOM

CIIS strives to promote an atmosphere of academic freedom through its Academic Freedom Policy. The pursuit of academic freedom may include the expression of conflicting opinions and critical discourse which may be perceived as a prohibited activity under this policy. Therefore, the Academic Freedom Policy will take precedence over Section C, Prohibited Activities, of the Student Computer Use Policy for technology that is implemented expressly for creating a method of dialogue among the Institute’s faculty, or for a particular class, cohort, or other such academic classification. The Student Computer Use Policy will take precedence over all other matters.

B. NO EXPECTATION OF PRIVACY

No expectation of privacy. The computers and computer accounts given to Users are to assist them in their academic career. Users should not have the expectation of privacy in anything they create, store, send, or receive on the computer system.

Waiver of Privacy Rights. Users expressly waive any right of privacy in anything they create, store, send, or receive on the computer or through the Internet or any other computer network. Users consent to allowing personnel of the company to access and review all materials Users create, store, send, or receive on the computer or through the Internet or any other computer network. Users understand that the Institute may use human or automated means to monitor use of its Computer Resources, and that members of the IT Services department have full administrative access to everything that is stored on the computer system, and may access items as part of their normal maintenance routine, or as mandated by internal or external investigations or court subpoena. Users also understand that regular backups of the data stored on the computer system are kept for up to 1 year, and may be accessed during internal and external investigations, as well as submitted as evidence in a court of law.

C. PROHIBITED ACTIVITIES

Inappropriate or unlawful material. Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent by email or other form of electronic communication (such as bulletin board systems, newsgroups, chat groups, intranets, or listservs) or displayed on or stored in the Institute’s computers. Users encountering or receiving this kind of material should immediately report the incident to the Dean of Students.

Prohibited Uses. The Institute’s Computer Resources may not be used for dissemination or storage of commercial or personal advertisements, solicitations, promotions, destructive programs (that is, viruses or self-replicating code), political material, or any other unauthorized use.
Waste of Computer Resources. Users may not deliberately perform acts that waste Computer Resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time in the computer lab, attaching large files to emails, peer-to-peer file sharing, downloading large files that take up bandwidth, or otherwise creating unnecessary network traffic.

Misuse of Software. Users may not do any of the following: 1) Copy software for use on their home computers; 2) provide copies of software to independent contractors or clients of the Institute or to any third person; 3) install software on any of the Institute’s workstations or servers; 4) modify, revise, transform, recast, or adapt any software; or 6) reverse-engineer, disassemble, or decompile any software. Users who become aware of any misuse of software or violation of copyright law should immediately report the incident to IT Services.

D. PASSWORDS

Responsibility for passwords. Users are responsible for safeguarding their passwords for access to the computer system. Individual passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their passwords. No User may access the computer system with another User’s password or account.

Passwords do not imply privacy. Use of passwords to gain access to the computer system or to encode particular files or messages does not imply that Users have an expectation of privacy in the material they create or receive on the computer system. The Institute has global passwords that permit it access to all material stored on its computer system—regardless of whether that material has been encoded with a particular User’s password.

E. SECURITY

Access to other user’s files. Users may not alter or copy a file belonging to another User without first obtaining permission from the owner of the file. Ability to read, alter, or copy a file belonging to another User does not imply permission to read, alter, or copy that file. Users may not use the computer system to “snoop” or pry into the affairs of other users by unnecessarily reviewing their files and email.

Accessing other computers on the network. A User’s ability to connect to other computer systems through a network or by modem does no imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operators of those systems.
Computer security. Each User is responsible for ensuring that use of outside computers and networks, such as the Internet, does not compromise the security of the Institute’s Computer Resources. This duty includes taking reasonable precautions to prevent intruders from accessing the company’s network without authorization and to prevent introduction and spread of viruses.

F. VIRUSES

Virus detection. Viruses can cause substantial damage to computers systems and data. Each user is responsible for taking reasonable precautions to ensure he or she does not introduce viruses to the Institute’s network. To that end, all material received on floppy disk or other magnetic or optical medium and all material downloaded from the Internet or from computers or networks that do not belong to the Institute MUST be scanned for viruses and other destructive programs before being placed onto the computer system. Users should understand that their home computers and laptops may contain viruses. All disks transferred from these computers to the Institute’s network MUST be scanned for viruses.

Accessing the Internet. To ensure security and avoid the spread of viruses, Users accessing the Internet through a computer attached to the Institute’s network must do so through the Institute’s Internet firewall. Accessing the Internet directly by modem is strictly prohibited unless the computer you are using is not connected to the Institute’s network.

G. ENCRYPTION SOFTWARE

Use of encryption software. Users may not install or use encryption software on any of the Institute’s computers without first obtaining written permission from IT Services. Users may not use passwords or encryption keys that are unknown to the Institute.

Export Restrictions. The federal government has imposed restrictions on export of programs or files containing encryption technology (such as email programs that permit encryption of messages and electronic commerce software that encodes transactions). Software containing encryption technology is not to be placed on the Internet or transmitted in any way outside the United States.
H. MISCELLANEOUS

Compliance with Applicable Laws and Licenses. In their use of Computer Resources, Users must comply with all software licenses; copyrights; and all other state, federal, and international laws governing intellectual property and online activities.

Other policies applicable. In their use of the Computer Resources, Users must observe and comply with all other policies and guidelines pertaining to Computer Resources.

Amendments and revisions. This policy may be amended or revised from time to time as the need arises. All amendments and revisions will be made available to the Users.

No additional Rights. This policy is not intended to, and does not grant, Users any contractual rights.