on-line at www.ccc.edu

RESPONSIBLE COMPUTER USE POLICY

(ADOPTED AUGUST 3, 2006)

I. INTRODUCTION

All users shall abide by the following provisions contained herein, or otherwise may be subject to disciplinary action or referral to the appropriate legal authorities for failing to comply.

II. SCOPE OF POLICY

This policy is applicable to all users of CCC information resources. This policy refers to all CCC "information resources" which means all computer and communications equipment installed on CCC property or otherwise furnished by CCC, whether individually controlled or shared, stand-alone or networked, and whether owned, leased, operated, or controlled by CCC, and including networking devices, personal digital assistants, wireless devices, personal computers, work stations, mainframes, minicomputers and any associated peripherals and software regardless of whether used for administrative, research, teaching or other purposes. No one, other than authorized personnel for authorized purposes, shall attempt to modify or remove CCC information resources or any other computer equipment, software or peripherals that are owned by others without proper authorization from CCC or the owner.

III. LEGAL COMPLIANCE

All users of CCC's information systems must comply with all federal, Illinois, and other applicable law; all generally applicable CCC rules and policies, including, but not limited to those which apply to personal conduct and those specific to computers and networks; and all applicable contracts and licenses. Users are responsible for ascertaining,

understanding and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

IV. AUTHORIZED USES

All users of CCC's information systems shall use only those computing resources that they are authorized to use and use them only in the manner and to the extent authorized. Ability to access computing resources does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding. Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by CCC. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information violate CCC's policy and may violate applicable law. All users must use systems and resources in ways that do not interfere with or disrupt the normal operation of these systems, nor interfere with the access and use of these systems and resources by others allowed to do so.

V. PROHIBITED CONDUCT

A. Harassment

No user may, under any circumstances, use CCC's computer systems or networks to libel, slander, or harass any other person.

B. Capacity Used

All users of CCC's information systems shall respect the finite capacity of those resources and limit use so as not to consume an unreasonable amount of those resources or to unreasonably interfere with the activity of other users. Although there is no set bandwidth, disk space, CPU time, or other limit applicable to all uses of CCC computing resources, CCC may require users of those resources to limit or refrain from specific uses in accordance with this principle. The reasonableness of any particular use will be judged in the context of all of the relevant circumstances and may

be deemed in violation of this policy. Users must be good stewards of the computing and network resources offered by CCC. Users rely on shared computing and networks simultaneously and, therefore, each user must consider the needs of other users when using these resources. Examples of poor stewardship of information resources include, but are not limited to: excessive personal use in a lab facility; excessive game playing; excessive personal use at staff and faculty workstations; continuous running of background programs and reception of large files or running intensive multi-media network applications (digital radio or other media) during high-use times.

C. Illegal File Sharing

Sharing copyrighted materials without a license (i.e., P2P file sharing which is often automatically shared) is against the law and also prohibited under this policy and subject to discipline. Copyright abuse can subject both the user and CCC to legal sanctions. Federal law requires CCC to take action when it is notified that someone on its network is distributing copyrighted materials. CCC will not protect any individual users, faculty, staff or students who distribute copyrighted material without license, nor will it protect or defend individuals who have improperly used CCC information resources.

D. Personal Gain or Benefit

All users shall refrain from using CCC information systems resources for personal commercial purposes or for personal financial or other gain without proper authorization. All users shall refrain from seeking personal benefit or permit others to benefit personally from any confidential information that has come to them by virtue of their work assignments. Personal use of CCC computing resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other CCC responsibilities and is otherwise in compliance with this policy. Further limits may be

imposed upon personal use in accordance with normal supervisory procedures.

E. Software License Abuse

CCC requires strict adherence to software vendors' license agreements. Copying of software in a manner not consistent with the vendors' license is strictly forbidden on CCC information resources. Questions regarding copying should be referred to OIT.

VI. PRIVACY

All users of CCC's information systems shall respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Ability to access other persons' accounts does not, by itself, imply authorization to do so. Users should be aware that their uses of the CCC computing resources are not completely private. The normal operation and maintenance of CCC's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the rendition of service. CCC may also specifically monitor the activity and accounts of individual users of CCC computing resources, including individual login sessions and communications, without notice, when (a) the user has voluntarily made them accessible to the public, (b) it reasonably appears necessary to do so to protect the integrity, security, or functionality of CCC or other computing resources or to protect CCC from liability; (c) there is reason to believe that the user has violated, or is violating, this policy or any CCC policy; (d) an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or (e) it is otherwise required or permitted by law or for any other legally permitted reasons associated with the evaluation, testing, repair or general operation of the CCC information resources.

CCC, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual

communications, to appropriate CCC personnel or law enforcement agencies and may use those results in appropriate CCC disciplinary proceedings. Communications made by means of CCC computing resources are also generally subject to the Illinois Public Records Statue to the same extent as they would be if made on paper. Authorized system administrators may access computer users' files at any time for maintenance purposes. System administrators will report suspected unlawful or improper activities to the proper authorities.

VII. SECURITY

CCC employs various measures to protect the security of its computing resources and of their users' accounts. Users should be aware, however, that CCC cannot guarantee such security. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts and guarding their passwords.

VIII. ADDITIONAL USER-SPECIFIC PROVISIONS

A. Website Reproduction

In addition to fully complying with this policy's general provisions identified in sections I through IX, inclusive, all users that have their own websites housed on CCC web servers (i.e., colleges, departments, faculty, etc.) which reproduce material available over the internet must be done in compliance with all applicable copyright laws. In addition, all CCC information that a school, department or employee desires to post on their websites should only be done with appropriate permission and authority.

B. Third-Party Connections to the CCC Network (vendors, contractors, consultants and external entities)

In addition to fully complying with this policy's general provisions identified in sections I through IX, inclusive, all third-party connection users are subject to the following additional provisions:

1. **Information and Systems Protection**
   Protect the security of CCC systems, the confidentiality and privacy of CCC students, employees and records.

2. **Equipment and Resource Inspection**
   All information resources and equipment must be inspected by a CCC IT employee. The inspection is intended to verify that the appropriate level of security is in place as well as verify the existence of proper communication equipment, technical settings, hardware compatibility and anti-virus protection. Any equipment deemed insufficient or risky to the CCC network may be denied access until deemed acceptable. Any external equipment and network devices not made available for the inspection may be disconnected from the CCC network until proper inspection is completed. If any equipment or network device is suspected of endangering network health, performance or security is subject to immediate disconnection.

3. **Intruded or Impaired Service**
   Any intrusive security audits or tests which may impair the connectivity, functionality and health of the CCC network must be scheduled and approved by the Vice Chancellor for Information Technology in advance of any such audit or impairment.

4. **Authorized Agency Connection**
   Generally, no direct connection to the CCC network from non-centrally-contracted third parties providing computing or network support is allowed. However, if any such connection is authorized, CCC cannot enable the outside agency to compete with any services already provided by agencies with exclusive agreements to provide such services to CCC. Instead, the connection must be limited solely to improving a service provided to CCC.

5. Terminated Connection

Agencies granted special connections must comply with CCC's computer use policy. A violation of the policy will cause immediate termination of connectivity.

6. Internal Connection to Outside Agency

Any CCC staff requiring a connection to outside agencies must provide a written request to OIT and shall explain the nature of the desired connection to outside agencies and the benefits expected therefrom.

C. Community at Large

In addition to fully complying with this policy's general provisions identified in sections I through IX, inclusive, all users without access to the CCC network but instead only accessing the internet via CCC's wireless internet service are subject to the following additional provisions:

1. Access to the Service

The service is a free public service provided by CCC. Your access to the service is completely at the discretion of CCC and your access may be blocked, suspended or terminated at any time for any reason including, but not limited to, violation of this policy, reasons that may lead to liability for CCC or its constituency, disruption of access to other users or networks, and any violation of applicable laws, policies, rules or regulations. All users are subject to the terms of this policy and any future revisions.

2. Acceptable Use of the Service

Your access to the service is conditioned on your legal and appropriate use of the service. Your use of the service and any activities conducted online through the service shall not violate any applicable law, policy, rule or regulation of the rights of CCC and its constituency.

IX. ENFORCEMENT

All users of CCC's information resources who are found to have violated any of these policies will be subject to disciplinary action up to and including (but not limited to) warnings, probation, suspension, discharge, dismissal, expulsion, and/or legal action. All users, when requested, are expected to cooperate with system administrators in any investigation of system abuse. Users are encouraged to report suspected abuse, especially any damage to or problems with their files. Failure to cooperate may be grounds for cancellation of access privileges, or other disciplinary actions. CCC employees should be aware that e-mail on their CCC account and files on CCC computers may be subject to public disclosure under the Illinois Public Records Law. Further, CCC reserves the right to access employee e-mails and files on CCC computers when needed for work-related purposes.

CCC may temporarily suspend or block access to an account prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of CCC computing resources or to protect CCC from liability. CCC may also refer suspected violations of applicable law to appropriate law enforcement agencies.

A. Incident Response

The CCC Incident Response Team (IRT) will receive, review and respond to any and all computer security incident reports and activity including any real or suspected adverse event in relation to the security of CCC computer systems or computer networks. The IRT will review, reports, analyze and respond to incidents in accordance with its operating guidelines.