Computing Guidelines of The College

Executive Summary

Columbia College, The School of Engineering and Applied Science, The Division of Student Affairs, and The Center for Career Education (The College) encourage the use of computing and network resources to enhance and support the learning and working environment of The College's computing community. Access to the computing and network environment is to be used in effective, ethical, and lawful ways that support the values of The College and the functions of its component units.

The College endeavors to create an atmosphere that balances respect for individual computer users and College resources in a manner that is designed to yield the greatest benefit for all users while maintaining the ethical and community standards of The College and Columbia University. This policy pertains to information technology systems, computing resources, and technologies made available in support of the activities of The College.

It applies to any devices and/or computers owned by the College as well as those owned by individuals who have been authorized to install or connect personal equipment either on the premises or to the network (e.g. remote-connections via home equipment).

In this context, The College's computing community includes: students, employees, temporary employees, consultants, contractors (and their employees), volunteers, and such visitors as are granted temporary user status by The College.

College Computing Resources

College computing resources are defined as those that are used to access The College's information technology systems. Such devices include (but are not limited to) personal desktop computers, laptop computers, monitors, hard drives, printers, scanners, network devices, networking equipment, servers, software developed by The College, and software acquired by The College. Any computer system that is owned or managed by The College, regardless of its location is a College computing resource.

All relevant data and information acquired by, managed, stored, transmitted, or maintained for administrative purposes is considered a computing resource.

University computing resources include those devices used for the activities of The College but not maintained by CCIT. Such devices include, but are not limited to, University-issued mobile device (e.g. Blackberrys, Treos, iPhones, Mobile phones), campus computer kiosks, or the University's VPN.

Support

Columbia College Information Technology (CCIT) is available to assist, advise, and consult with users on the proper use of College computer resources and interpretation of this policy. If users have any questions or uncertainty about this policy, they are encouraged to contact the Director of Columbia College Information Technology or his/her designate for clarification.

CCIT and its team members are charged with maintaining The College's computing resources. In addition to being bound by the policies of this document, they have been given additional privileges and responsibilities in order to accomplish their tasks.

A separate document called the "Code of Conduct for CCIT Team Members" regulates the activities of CCIT Team Members.

Principles

- Computing and network resources are provided primarily to support and further The College's mission.

- All members of The College's computing community who share in the benefits of its computing environment are partners and stakeholders in maintaining and protecting this environment, its resources, and the interests of other community members.

- Individuals using College-owned computer technology resources are expected to comply with all applicable University, local, state, and federal guidelines, policies, regulations, statutes, and procedures pertaining to confidentiality and privacy, including, but not limited to, the Family Educational Rights and Privacy Act of 1974 (FERPA), and the University's computing &

security policies.

- Some of the material used at the College is copyrighted, protected by intellectual property law, and/or license agreements. Community members should undertake reasonable efforts to ensure that they do not violate the various laws, policies, procedures and license agreements.

- Members of The College community are responsible and accountable for their actions and statements in the electronic working and learning environment, according to the University's Rules of Conduct.

- Community members are expected to use reasonable restraint in consumption of these valuable shared resources, and to use them in ways that do not interfere with the study, work or working environment of other users.

- Community members entrusted with computing resources are responsible for the safety and security of The College's property and information. This includes physical security (e.g. the locking of equipment when unattended), locking one's workstation when unattended and using appropriate password security

- The College's computing resources should primarily be used for College educational and administrative purposes.

- Any data stored by or transmitted to members of the College community is confidential and will not be accessed by The College without just cause and due process.

  In any circumstances of alleged impropriety, formal procedures permit persons responsible for computers or networks to request specific institutional authorization to examine directories, files, email or other electronic records that are relevant to the investigation of the allegation. More information can be found within the "Code of Conduct for CCIT Team Members".

- Members of The College community must follow prescribed procedures for accessing systems, maintaining account security, storing information, and transmitting information.

- College users accessing and using non-College computing resources are bound by the policies of the external resource, and the more restrictive applicable policy applies.

- Anyone who observes actual or apparent use which appears to violate The College's Computing Guidelines or another applicable policy is encouraged to bring the matter to the attention of CCIT.

Unacceptable Uses

Below are presented illustrative, but not exhaustive, examples of unacceptable uses of College computing resources. Some of these unacceptable uses also constitute criminal offenses.

- **Unauthorized access (hacking):** This may include a) using unauthorized user names, passwords, computer addresses, or identities, b) modifying assigned settings to gain access to computer resources and/or data, c) using unauthorized interfaces or procedures, or d) otherwise attempting to evade, disable or "crack" security provisions of The College or external systems.

- **Unauthorized Distribution and Disclosure of Information:** Every effort must be made to prevent the unauthorized disclosure and distribution of information that is the property of The College.

- **Installation or alteration of systems, peripherals, or software:** The College's computing resources have been designed to provide a stable, highly available, and secure computing environment in keeping with The College's mission in a cost-effective, secure, and supportable information technology delivery structure. The introduction or reconfiguration of computing resources can be unintentionally detrimental and is not permitted.

  As computing technologies and capabilities change over time – users are encouraged to work with CCIT in identifying, researching, and selecting new computing resources, extending the existing computing environment, or improving the existing computing environment.

- **Vandalism of data:** One may not deliberately alter or destroy computer data. Under no circumstance may a user inspect, alter, delete, publish or otherwise tamper with files or file structures that the individual is not authorized to access.

- **The borrowing or theft of computing resources:** One must receive authorization prior to using or removing a computing resource outside of a formally authorized environment or process.

- **Interference with other users' work:** This includes use of any process that causes a user to be deprived of services or resources that they would normally expect to have available. It covers but is not limited to the creation of "spam (excessive email distribution)," the introduction of viruses or electronic chain letters, and the launching of processes that create a denial of service for others.

- **Squandering resources:** Resources are shared and no user may degrade the systems by: unwarranted data space, time and bandwidth consumption through resource-intensive programs or unattended network connections. As the use of College resources changes and the technology capabilities change over time, users are encouraged to work with CCIT in defining appropriate and efficient uses of computer resources.

- **Personal uses:** The College computer resources are to be used primarily for College business purposes (i.e. education and administration). All users have the responsibility to ensure that incidental personal use of College computer resources does not interfere with the normal course of their duties. Incidental personal use of computers would include but is not limited to personal email or instant messaging.

  The College strongly recommends that a degree of separation be maintained between personal and professional activities. Where applicable, it may be in one's best interest to maintain separations between one's roles within the University. CCIT can assist, advise, and consult in these matters.

- **Telecommuting/Remote Access:** Incidental personal use of College and/or any other computer systems that are used for telecommuting is permissible so long as the usage does not compromise or violate the network, computer, or data's security and/or the ethical principles set forth by the College.

  College issued computing resources in support of telecommuting/remote access remain the property of the College, are issued for job-related purposes, and must be maintained in keeping with all standards that apply to resources used within a traditional office environment.

  The College has developed approved solutions for working remotely that are detailed within its "Approved Solutions for Working Remotely" policy document.

- **Access, Storage, and Transmission of Information on or via Untrusted Systems:** Columbia College has invested in well-designed solutions ensuring continuity of access, authorization, integrity, and confidentiality controls for its computing resources. Data and information resources should not be accessed from, or stored on untrusted systems except via approved solutions. Nor should resources be transmitted between trusted and untrusted systems.

- **Sharing of account:** The College's computing resources are allocated to groups and individuals for specific academic and administrative purposes. It is not acceptable to give, sell, or otherwise provide computing resources to other individuals or groups that do not have explicit permission to use them. Users are not to share computer accounts.

- **Disclosure of security credentials:** It is important in a shared environment to maintain accountability and carefully control access to computing resources. The disclosure or distributions of passwords, key cards, authentication procedures, and cryptographic keys/information is prohibited. One is responsible for all activities that occur under the auspices of one's user accounts.

- **Breach of copyright:** This includes installing, reproducing, and/or distributing copyrighted materials such as proprietary software, publications, files, music, video, or other media without permission. College software is provided

under license agreements with various vendors and may not be copied or otherwise removed. Third party copyrighted information or software that the users do not have specific approval to store and/or use must not be stored on College systems or networks.

- **Use of computing resources in a manner that breaches Rules of University Conduct:** All members of the University community are responsible for compliance with the Rules of University Conduct.

Discipline, Jurisdiction, and Penalties

Columbia College extends to authorized users the privilege of using the College's computing resources. Along with this privilege comes responsibility to the College community to abide and be bound by the provisions of the applicable policies regarding its use.

All reports and incidents of inappropriate use of College computing resources will be properly investigated to ensure compliance with College and University policies, as well as state and federal laws. Violators of computing policies will be subject to the normal disciplinary procedures of the College and the University. The loss of computing privileges may also result.

Policy Changes

Should changes be made to this policy, all reasonable attempts will be made to communicate the changes to The College's computing community.

Definitions

- **Data**: the quantities, characters, or symbols on which operations are performed by computers and other automatic equipment and which may be stored or transmitted in the form of electrical signals, records on magnetic media,, etc.

- **Information**: knowledge acquired or derived from data. For the purposes of this policy, the term information refers to both information and data in all their forms, collected, maintained, accessed, modified, or synthesized by and for all members of the College community to perform the operations of the College.

- **Telecommuting:** Telecommunication work outside the traditional office or workplace, usually at home or in a mobile situation.

Relationship to Other Computing Policies

The College's computing policies are designed to be complementary and supportive of University policies and policies which the University must uphold.

Further, as many computing resources used by the College Community are provided by other University functions, it is important to understand that your computing usage is subject to other policies. You are encouraged to read and understand other applicable policies of the University. Below are links to applicable computing policies and rules of conduct.

Columbia University Computing and Network Use Policy
http://www.columbia.edu/cu/policy/network_use.html

Columbia University Copyright Policy
http://www.columbia.edu/cu/policy/copyright.html

Columbia University Information Policy Library
http://www.columbia.edu/cu/administration/policylibrary/responsible_office/cuit.html

FERPA
http://facets.columbia.edu/policy-access-student-records-ferpa

Rules of University Conduct
http://facets.columbia.edu/university-regulations/rules-university-conduct

University Telecommuting Policy
http://www.hr.columbia.edu/hr/policies/telecommuting/telecommuting/