
COMMUNITY COLLEGE OF PHILADELPHIA

COLLEGE POLICIES AND PROCEDURES MEMORANDUM NO. 307

ACCEPTABLE USE POLICY FOR INTERACTIVE SYSTEMS

Revised: March 2012
July 25, 2007

Original Date of Issue: May 15, 1997

*Revised by the Technology Coordinating Committee and approved by IWC and the President
xx.xx.2012*

*Revised by the Technology Coordinating Committee and approved by IWC and the President
6.19.07*

Introduction

In support of its mission, Community College of Philadelphia provides access to computing and information resources for students, faculty, staff, members of the Board of Trustees and other parties that may be given access to the College's interactive systems through a contractual association with the College within institutional priorities and financial capabilities. All members of the College community who use the College's computing and information resources¹ are responsible to safeguard the integrity of these resources, respect the rights of other computing users, and abide by all pertinent license and contractual agreements. It is the policy of Community College of Philadelphia that all members of its community act in accordance with these responsibilities, any relevant laws and contractual obligations, and the highest standard of ethics.

Social networking services/sites can provide a virtual community external to the College.. Members create their own online "profile" with biographical data, pictures, likes, dislikes and any other information they choose to post. They communicate with each other by voice, chat, instant message, videoconference and blogs, and the service typically provides a way for members to contact friends of other members. Examples include but are not limited to Facebook, MySpace, Friendster, Plaxo, LinkedIn, Ryze.

The use of information technology must remain in keeping with the philosophy and mission of Community College of Philadelphia. Usersⁱ must abide by this and any other relevant policies, procedures and guidelines. These policies and guidelines include but are not limited to:

- **College Policies and Procedures Memorandum #3** – Plagiarism, Classroom Cheating, Electronic Cheating, and Non-Print Product Misrepresentation
- **College Policies and Procedures Memorandum #305** – Policy Governing the Use and Duplication of Software
- **College Policies and Procedures Memorandum #309** – Hardware and Software Support Policies On-Campus
- **Guidelines for Responsible Computing**
- **Student Code of Conduct**
- **Equal Employment Opportunity and Affirmative Action Policies**
- **Applicable collective bargaining agreements**
- **Guidelines for Using the Faculty/Staff Access Centers**
- **College Policies and Procedures Memorandum #352-** Discriminatory Harassment Prevention

The College also recognizes federal, state, and local laws in regard to copyright, privacy, or any other statutes that relate to the online environment, as binding upon users of the College's interactive system as well as employees identifying an affiliation with the College when using any social networking service.

Community College of Philadelphia's interactive system is intended for use as an educational tool, and as such supports the teaching, learning, research, and campus activities of the College community and facilitates the management of administrative functions. The College, therefore, provides students, faculty and staff access to the technology resources and interactive systems of the College. This policy applies to all users of the College system, as listed above and any others to whom the College wishes to make the system available.

The College makes no guarantees of any kind, either express or implied, that the functions or the services provided by or through the College's system will be error-free or without defect. The College will not be responsible for any damage users may suffer, including, but not limited to, loss of data or interruptions of service. The College is not responsible for the accuracy or quality of the information obtained through or stored on the system. The College will not be responsible for financial obligations arising through the unauthorized use of the system.

The Executive Officer for Information Technology Services will oversee the College's system by working with other College officials, government agencies and appropriate regional, state and national organizations as necessary.

The use of the College's interactive systems is a privilege, not a right, and inappropriate use can result in a termination or suspension of some or all of those privileges. Users will be expected to abide by generally accepted rules of network etiquette.

Privacy

While the College does not intend to routinely review the contents of files on the system, the College will engage in routine maintenance and monitoring of the system. Accordingly, system users should have no expectation of privacy using the College's system, including personal e-mail messages and other data files.

Routine maintenance and monitoring of the system may lead to the discovery that a particular user has or is violating the College's Acceptable Use Policy, or applicable law. The College will cooperate fully with local, state, and federal officials in any investigation concerning or relating to any illegal activities conducted through the College system.

An individual search will be conducted if there is reasonable suspicion that a user has violated the law or the College's Acceptable Use Policy. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation.

College employees should be aware that their personal files (including personal e-mail messages) may be discoverable in court or agency proceedings and possibly elsewhere.

Use of the College system to access or attempt to access student or employee information for any use not job-related violates College policy along with state and federal laws. Confidential information, whether it relates to students, employees, or others shall not be disclosed or distributed using the College system or by employees identifying an affiliation with the College when using any social networking service. Exceptions are activities which are in accordance with College policy and federal laws, such as the Family Education Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach Bliley Act. Federal Laws pertaining to confidentiality of information can be accessed by each federal law's web-site.

Users must not post, transmit, re-post, or re-transmit private information about another person or organization on the College's system without first obtaining the permission of that person or organization.

Employees are prohibited from using a College-provided or personal cell phone or Smartphone camera or video recorder to take, transmit, download, or upload to social networking or video sites either for business reasons or for non-business purposes any photos or videos of College employees, vendors, officials or students without their consent.

Unacceptable Use

Under no circumstances may users attempt to gain unauthorized access to the College's interactive system or to any other computer system through the College's system, or to go beyond their authorized access. This includes attempting to log in through another person's account or accessing another person's files.

Users must not make deliberate attempts to disrupt the College's computer systems' performance or destroy data by introducing or spreading computer viruses or by any other means.

Users must not use the College system to access material that advocates illegal acts, or that advocates violence or discrimination towards other people.

Employees identifying an affiliation with the College may not post content or conduct activities that fail to conform to local, state, and federal laws when using any social networking services.

Under no circumstances will users access the College system to engage in any other illegal act.

System Security

Users are responsible for the use of their individual account and must take all reasonable precautions to prevent others from being able to access or use their account. Under no conditions should a user provide his/her password to another person.

Users must immediately notify the system administrator if they have identified a possible security problem. Users will not attempt to investigate or correct a security problem. Such activity may be construed as an illegal attempt to gain access.

Users must not knowingly post, transmit, re-post or re-transmit information on the College's system that, if acted upon, could spread a virus, cause damage or a danger of disruption.

Inappropriate Language

Members of the College community, as individuals and groups, have the right to exercise their full freedom of expression and association. The College neither sanctions nor censors individual expression of opinion on its systems. The College is committed to creating an educational environment that is free from intolerance directed towards individuals or groups. Respect for rights, privileges, and sensibilities of each other are essential in preserving the College community. There is a wide range of material available on the Internet, some of which may conflict with the particular values of students and employees. The College cannot accept responsibility for any individual user's accessing offensive materials through its computer systems.

Users must not engage in libel, slander, or harassment in violation of College policies, or the use of threatening language.

Users must not knowingly or recklessly post, transmit, re-post, or re-transmit false or defamatory information about a person or organization on the College's system.

The College discourages the use of language that embarrasses or intimidates others.

Inappropriate Activities

Users must not use the College system to access material that is profane or obscene (including pornography). For students, a special exception may be made for potentially inappropriate material if the purpose of such activity is to conduct research and access is approved by the instructor. College employees may access the above material only in the context of legitimate research.

Users must not look at, copy, alter or destroy anyone else's personal files without express permission. The ability to access a file or other information does not imply permission to do so.

Users may not use the College system for commercial purposes, defined as offering or providing goods or services for sale or barter to others or purchasing goods or services for personal profit. The College acquisition policies will be followed for purchasing online any goods or services for the College.

Users may not use the system for political lobbying that is, to express their opinion on political issues to their elected representatives, or to urge others do so, unless this communication is in support of the academic mission of the College. Students may also use the system to express their opinions to elected officials on political issues if those communications are made in connection with an educational assignment.

Use of College Name, Logo or Seal

Users of the College system, as well as employees identifying an affiliation with the College when using any social networking service, may not use the College's name, logo, or seal in their Pages in any way that implies College endorsement of other organizations, products or services, without first obtaining written permission from the Office of Communication.

Users may not use College logos or trademarks, including the College seal, without first obtaining written permission from the Office of Communications.

Social Networking

Employees identifying an affiliation with the College when using electronic social networking services are also bound by all provisions of this policy.

The College recognizes that some employees may, for personal reasons, access, view, operate, and post, download, or upload content to external social networking sites and video sites on their own time via their own computer equipment.

Employees identifying an affiliation with the College when using electronic social networking services must post the following disclaimer; “The opinions expressed on this social networking profile (video site) are my own personal opinions. They do not reflect the opinions of my employer, Community College of Philadelphia.”

Oversight (Enforcement)

Individuals who have a complaint or a grievance on matters related to this policy, should contact the College’s Chief Information Officer. The CIO will determine the appropriate College office or department to hear and/or investigate the complaint or grievance.

Original date: May 15, 1997

Last modified 17 September 2003

July 25, 2007

December, 2010

March 2012

Community College of Philadelphia Web Team

TCC subcommittee 12/04

¹ Interactive systems are defined as those devices that are connected to the College network infrastructure whether directly or remotely. This is to include all equipment connected to the College network for the use of data transmission or processing using the College infrastructure. Remote connection may be accomplished via dial-in, VPN or other secure methods.

IWC questions for Clarification

1. At some points in the document the term "employees" is used versus "users" in other sections of the document. An example is p. 4 under "Unacceptable use." Other groups mentioned are: Board members, students, advisory committee members, groups like student clubs.

We had specific reasons for using the terms Employee and User. The User term reflects those that are using the system but may not be employees.

2. If question #1 applies to employees only, is there language that is needed for Board members?

We can now include them with the Employee statements; Trustees. All have recently signed the AUP. I suggest the following change within the revised AUP. (1) Unacceptable Use section: 4th paragraph change "Employees" to "Users" and (2) if desired the term "Board of Trustee members" can be added as a group designation on Page 1 in the opening paragraph where the term user is defined.

3. Should the term "users" be updated to members of the College community since "users" seems to be somewhat limited.

We disagree that the term "users" is limited since many users of our system may not be members of the College community.

4. Is there any expectation that the College police or enforce the policy (esp. when individuals are using their own systems)?

The College cannot monitor the policy and will react only when a complaint is filled as has been past practice.

5. Could the College get the same benefit by posting something on our web page to cover general members of the College community?

We provide the AUP link on multiple locations throughout the ccp.edu domain.

6. Should there be a separate policy versus adding to the current policy?

This has already been debated. The Social Media section within AUP is intended to handle the broad issues that pertain to legal and responsible computing within the campus environment. A separate policy specific to SM may be developed at some point which would in my opinion be more of a set of Guidelines.