14. Campus Policies on Information Resources, Internet Use, Web Pages, Information Security and Information Protection

14.1 General Use Policy on Information Resources

Purpose

The purpose of this General Use Policy on Information Resources (hereinafter the "Policy") is to establish a Dutchess Community College (hereinafter "DCC" or the "College") policy regarding the use and management of information resources. Every individual utilizing information resources of the College, accessing the DCC wireless network, accessing College websites off campus, or using College-owned communications devices on or off campus is expected to understand and follow this policy.

Definitions

For the purpose of this policy, the following definitions will apply:

"Communications Devices" includes telephones, computers, PDAs, and any other appliances where information is transmitted and/or received.

"Department of Information Technology" or "IT" is the College's department by this or another name, or its successor, charged with maintaining the College's information resources infrastructure.

"Supervisor" is defined as the dean or supervisor who oversees a particular user's area of the College, as established by the College organizational chart. For students, the Supervisor shall be considered the Vice-President and Dean of Student Services.

"Virtual Communities" are defined as social networks of individuals with a membership who interact through specific media in order to pursue mutual interests or goals.

"Wireless Infrastructure" refers to wireless access points, antennas,
cabling, power, and network hardware associated with the deployment of a wireless communications network.

State and Federal Law

All users of DCC Information Resources are subject to Federal and State law. No school computer or any other communications device may be used in violation of the laws of New York State or the federal laws of The United States of America, including, but not limited to the Family Education Rights and Privacy Act (FERPA) and the American Health Insurance Portability and Accountability Act (HIPAA).

General Use Policies

The College's Information Resources may only be used for purposes that are consistent with the educational mission of the College as defined in the Professional Staff Handbook of Dutchess Community College.

Nothing in this General Use Policy shall be construed or interpreted in such a way as to conflict with the College's policy on Academic Freedom (sec. 6.7 of the Professional Staff Handbook).

The College's Information Resources may not be used:

- to violate the laws of New York State or the United States of America;
- to create or disseminate software or data files that could be reasonably considered as viruses or malware;
- to intimidate, threaten or harass individuals, or violate any other College policies;
- to store, print, or transmit obscene, pornographic, slanderous, or threatening messages;
- for profit-making or commercial purposes, unless special arrangements have been made with the College;
- for partisan political lobbying.

A. Computers

The Department of Information Technology (IT) provides access to computing appropriate for the needs of particular users. IT is also responsible for maintaining on-site and off-site storage of data.

Access to computers may include Internet connections and access to local area networks and servers. Computer access is made available only to authorized individuals and organizations, according to the following guidelines:

1. Each Dutchess Community College staff or faculty member who has computing needs which support the overall goals of the College will be assigned an account by IT.

2. Each account owner or manager is responsible for maintaining the account and files stored in the account. This maintenance includes removing old and unused files and changing the account password regularly to prevent other users from gaining access to the account.

B. Software

1. No user may copy, or attempt to copy, any proprietary or licensed software provided or installed by IT.

2. Pirated software or software programs copied without authorization may not be stored or used on College-owned Information Resource systems.

3. All shareware programs must be registered in accordance with their license and use provisions.

4. No person may store or use programs on College-owned systems which violate or hamper another person's use of Information Resources.

5. Programs that attempt to obtain another user's password, acquire another user's files, circumvent

system security measures or crash the computer are prohibited.

6. The devising or spreading of computer viruses is expressly forbidden.

C. User Access

Users gain access to computer systems by being assigned an account on the College's network. Possession of an account may allow the owner to use storage space on servers or computers, and also utilize services of peripheral devices such as printers. Users should take reasonable precautions to insure that such programs and files do not cause consequent damage to the computing systems at the College or the files or accounts of other users.

A user should only access, or attempt to access, files in his or her own accounts, files which have been made accessible to him or her by the files' owner, or files which have been made publicly accessible by the files' owner. No person may use, or attempt to use, any computer accounts other than his or her own assigned account. The negligence of a user in revealing an account name and password does not confer authorization to use the account.

D. Internet Use

Users should be aware that the Internet is not a secure medium. Third parties may be able to obtain information regarding users' activities.
The Internet does not guarantee the privacy and confidentiality of information. Sensitive material transferred over the Internet may be at risk of detection by a third party. Therefore, care should be taken when transmitting highly confidential material.

Pursuant to the procedures and limitations as described in The Internet Acceptable Use Policy Enforcement section, the College reserves the right to monitor access to information resources and inspect files and documents stored or transmitted via College computers

and networks for the purposes of investigating whether a violation of this policy has occurred.

The College provides access to the Internet for staff, faculty, students and authorized guests. Access to the Internet is limited to purposes consistent with the educational mission of the College. In order to ensure the equitable and orderly use of Information Resources, the College reserves the right to allocate Internet usage and availability on its library, laboratory, classroom, and other computer terminals on campus. The College does not control access to Internet sites; users assume said responsibility.

E. Virtual Communities

Any virtual community using DCC information resources should be consistent with the educational mission of the College, published in the Rights and Responsibilities Handbook, and the community's membership should reflect the College's goals.

Moderators of DCC virtual communities should publish clear guidelines detailing acceptable behavior for the virtual community. Participants must be made aware of who has access to the virtual community that they are participating in. The moderators should make provision for appropriate Dutchess Community College staff to have access to the virtual community. Student-created virtual communities must have a faculty or staff moderator and members must be current students, faculty, staff, or trustees, and members of these groups cannot be excluded from a virtual community on an *a priori* basis.

F. Information Security

IT makes strong efforts to maintain the security of account names, numbers, passwords, directories, and files. However, users should not assume or expect privacy while using College-owned Information Resources. No computer system is completely secure, and it is possible that some user could gain access to another user's accounts through actions or accidents beyond reasonable control. It is the responsibility of

the college and IT to maintain the highest level of information security appropriate to the needs of the College. Furthermore, it is the responsibility of IT to inform users of security upgrades and proper protocols that may impact use of the College's Information Resources. In the event that there is a breach of security of DCC's informational resources, IT will notify affected users.

G. Communications Devices

Telephone services and wiring must not be modified or extended beyond the area of their use. Unauthorized use of an individual's telephone extension number or voice mailbox and any attempt to gain access to a voice mailbox other than your own is prohibited. Voice mailbox passwords should be used and should never be exchanged.

H. Wireless Infrastructure

The purpose of Wireless Infrastructure at Dutchess Community College is to support the academic and administrative work of the College. Users of the Wireless Infrastructure are subject to the same rules and policies that govern all other information resources at the College. Users of the campus wireless network should be aware that information sent wirelessly is susceptible to unauthorized examination. For this reason, wireless devices should not normally be used for connecting to College systems containing sensitive or confidential information such as payroll, student information, or financial information. In order to maintain a secure and reliable wireless network, IT, in consultation with affected administrative offices and divisions of the College, shall:

1. set standards regarding user access and authentication at wireless access points;

2. resolve conflicts regarding the allocation of radio spectrum (prioritizing instructional needs over other uses);

3. monitor and incorporate new technologies to enhance

the performance and security of campus wireless networks.

I. Personal Use

Dutchess Community College permits its faculty and staff to use College Information Resources for some personal use, subject to certain limitations. Such use must be reasonable and may not be:

1. associated with any activity that violates state or federal law;

2. associated with any activity that violates College policies, rules, or regulations;

3. detrimental to the main purpose for which the Information Resource in question is provided.

4. associated with the transmittal, retrieval, or storing or any communications of a defamatory or harassing nature or contain materials that are obscene or pornographic;

5. associated with harassment of any kind which is prohibited by College practice or policy;

6. associated with derogatory or inflammatory remarks about an individual’s sex, sexual orientation, race, age, disability, religion or national origin;

Enforcement of General Use Policy on Information Resources

A. Inspection of User's Files

If, in the course of investigating a potential violation of this policy, IT deems it necessary to inspect a user’s files or information stored on college computers, it must first seek and obtain written authorization from the Dean of Academic Affairs if the user is on the faculty, the Director of Human Resources if the user is on staff, or the Dean of Student Services if the user is a student. A user whose computing information has been examined will be notified of the reason for the examination and of any

actions taken by IT as a consequence of that examination.

B. Limit on Use of Examined Files

Any information or documents so obtained by IT, under the authority of the user's Supervisor, may be used only to ascertain whether there has been a violation of written policy or law, and may not be disseminated or used for any other purposes.

C. Disciplinary Process

Violations of this Policy may subject the user to disciplinary action consistent with existing College practices, policies, and procedures. Disciplinary actions should also adhere to the policy on Academic Freedom in section 6.7.1 in the Professional Staff Handbook.

D. Possibility of Prosecution

It should be understood that the above policies do not preclude prosecution in cases of criminal misconduct and that all users are subject to local, state and federal laws.

(DCC Board of Trustees Resolution #2011-66, August 9, 2011)