SNOW COLLEGE

Policy # 225
Former Policy #12.1
Date Approved: 5-18-2000
Date Amended: 1-27-2017

SUBJECT: INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

1.0 GENERAL STATEMENT

1.1 Snow College makes available to its community members technology resources, including email and internet, to support the educational, instructional and administrative activities of Snow College. These resources are to be used to advance the mission of the College. These resources are to be used in a manner consistent with College Policy, Law and Rules. Every user bears the responsibility for knowing and complying with applicable Policy, Laws, and Rules; for appropriately securing their computers and other electronic devices from misuse or theft by others; and for avoiding any use that interferes with others' legitimate access to and use of College Technology Resources.

2.0 TERMS

2.1 "User" or "Users" are the students, faculty, staff and authorized visitors, guests, affiliates and others to whom Technology Resources are made available.

2.2 "Technology Resources" are the College owned devices and systems, College contracted systems and services, and privately owned or publicly provided devices using the College's networks and resources. Included are College owned facilities such as computer hardware, multimedia hardware, video equipment, software, documentation, communications support, on-line account administration, support services, Internet access and instructional materials.

2.3 "Policy, Law and Rules" includes this Policy, the Information Security Policy, Technology Resource Guidelines, specialized policies created by specific departments, programs and offices of the College, and federal and state laws and rules including copyright laws.

2.4 "Electronic Messages or Traffic" includes emails, texts, voicemails, instant messages, internet use and other electronic communications transmitted sent or received using College Technology Resources.

3.0 APPLICABILITY

3.1 This Policy applies to all Users and all technology administered within the College Internet domain by individual departments or members of the faculty or staff or by campus organizations, to information services hosted by dorm-resident students or by authorized resident visitors on their own hardware connected to the campus network; to the resources administered by central administrative departments such as the College Library or IT; to authorized collaborative devices connected to

the campus network and using College Internet addresses; to personally-owned devices connected by wire or wireless service to the campus network from College owned housing or via campus locations providing mobile wired access or wireless access; and to actions originating from computer systems or mobile devices maintained or used by members of the campus community off-campus but connecting remotely to the College's network services and under the aegis of the College's name. It applies to websites bearing the College credentials, even when hosted outside the College's Internet domain.

4.0 POLICY

4.1 Acceptable Use. Use of all College Technology Resources, information technology and digital resources should be for purposes that are consistent with the College's educational mission and the Policy, Law and Rules (including license agreements and terms of service) of the College, and not for commercial purposes.

4.2 Personal Use. Users may also use College Technology Resources for appropriate incidental personal use so long as those activities are legal and do not violate College policies; contractual obligations; the safety, security, privacy, reputational and intellectual property rights of others; or other restrictions.

4.3 Prohibited Use. Use of the College's Technology Resources should not violate applicable Policy, Law and Rules and may not be used to transmit malicious, harassing or defamatory content.

4.4 Use Is a Privilege and May Be Revoked. The use of the College Technology Resources, including networking and the internet, is a privilege, not a right. Inappropriate use, including any violation of Policy, Law and Rules, may result in cancellation of the privilege.

4.5 College Access

4.5.1 College Access to All Use of Technology Resources. In the event the College has reasonable suspicion that a User has violated any civil or criminal law, the College Code of Conduct, this Policy, or any other Policy, Law and Rule, the College reserves the right to and the User agrees that the College may monitor, access, inspect, remove, copy, take possession of, or surrender to civil or criminal authorities the offending Content, with or without notice or consent of the User. The includes monitoring and accessing Electronic Messages or Traffic. Further, the College may monitor the Technology Resources to ensure that they are secure and being used in conformity with this Policy, Law and Rule. Information that the College gathers from such permissible monitoring or examinations may also be used in disciplinary actions.

4.5.2 College Access to Employee Generated Content. Employees are notified that the College owns all data and files in any computer, network, or other information system used by the College and to all data and files sent or received by employees using any College Technology Resources. This includes Electronic Messages or Traffic sent or received using College Technology Resources. The above are not private or confidential, and are the property of the College, and may be accessed or monitored as determined by the College.

4.6 Violations of this Policy may result in disciplinary action, including dismissal from employment, expulsion from the College, suspension or termination of Technology Resources use and privileges.

4.7 Utilization of any College Technology Resources constitutes acceptance of the terms of this Policy. Users acknowledge they have read and understand this Policy and they shall be personally responsible for their acts or omissions in connection with utilization in derogation of this policy.

4.8 Guidelines. The Snow College Office of Information Technology may from time to time publish and update "Guidelines to the Information Technology Acceptable Use Policy." Such Guidelines are binding upon Users.

4.9 The College makes no warranties of any kind, whether expressed or implied, for the services it provides, in connection with the use of the Internet. The College will not be responsible for any damages an employee or other user suffers. This includes loss of data resulting from delays, non-deliveries, or service interruptions caused by the College's negligence, by the user's errors or omissions or by any other cause. Use of any information obtained via the Internet is at the user's own risk. The College specifically denies any responsibility for the accuracy or quality of information obtained through this service. All users need to consider the source of any information they obtain, and evaluate how valid that information may be.

4.10 Unauthorized uses of the College information technology facilities include, but are not limited to:

- Any utilization infringing on the rights or liberties of another.
- Illegal or criminal use of any kind.
- Utilization involving communications, material, information, data or images prohibited by legal authority as obscene, pornographic, threatening, abusive, harassing, discriminatory, or in violation of any other College policies.
- Deliberately wasting or overloading computing resources.
- Accessing, viewing, printing, storing, transmitting, disseminating or selling any

information protected by law or subject to privilege or an expectation of privacy.

- Utilization that causes or permits materials protected by copyright, trademark, service mark, tradename, trade secret, confidential or proprietary data and information statutes, or communications of another to be uploaded to a computer or information system, published, broadcast, or in any way disseminated without authorization of the owner.

- Use of electronic communication systems to create or transmit unsolicited bulk messages (commonly known as 'spam'), content intended for commercial gain, or content which violates applicable state or federal laws.

- Any attempts to access any resources, features, contents, or controls of the information technology facilities that are restricted, confidential or privileged.

- Intentional or reckless utilization of resources causing damage to or altering the operation, function or design of the information technology facilities or content.

- Granting access to persons not authorized by the College to any College information facility, either by intentional action such as disclosure of account information or unintentional action such as failure to log off.

- Commercial, profit-motivated or partisan political use not related to College programs.

- Any violation of applicable school policy or public law by such use.

- Any activity that is contrary to the high moral standards which must be maintained in an educational setting.

- The transmission to others of profane, defaming, harassing or offensive language.

- Any commercial use, product advertisement or improper promotion of political candidates.

- Any attempt to disrupt or interfere with use of the Internet system.

- Any attempt to access improper information to which the account holder does not have right to access.

4.11 Vandalism is defined as any malicious attempt to harm, modify, or destroy data of another user, the College data systems, Internet, or other networks. This includes, but is not limited to, the uploading or creating of computer viruses. Harassment is

defined as the persistent annoyance of another user, or the interference of another users' work. Harassment includes, but is not limited to, the sending of unwanted mail. Vandalism and harassment may result in cancellation of user privileges and possible disciplinary action.

4.12 Security on any computer system is a high priority, especially when the system involves many users. Users must never allow others to use their password. Users should protect their password to ensure system security and their own privilege and ability to continue to use the system. The College is not responsible for individual password security.

- If you identify or suspect a security problem on the Internet, you must notify a system administrator. Do not demonstrate the problem to other users.
- Do not use another individual's account without express written permission of the account holder and system administrator.
- Any user identified as a security risk for having a history of problems with other computer systems may be denied access to the Internet by the College.

4.13 Due to the inherent lack of security in most Internet communications, and due to the right and need for the College to monitor compliance with civil or criminal law, the College Code of Conduct, the IT Acceptable Use Policy, or any other College policy, procedure, or regulation, any user utilizing any College information technology, understands and agrees they are specifically waiving any expectation or right to privacy in their communications, data, programs, or other personal information stored, displayed, accessed, communicated, published or transmitted on the facilities.