Greenfield Community College
Information Technology Department

Acceptable Use Policy

1.0 Overview

The Information Technology Department is committed to protecting Greenfield Community College's students, employees, partners and the college from illegal or damaging actions by individuals, either knowingly or unknowingly. Concurrently, the GCC Information Technology Department wants to preserve our culture of openness, trust and integrity.

GCCNET - Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and S/FTP, are the property of Greenfield Community College. These systems are to be used for business and academic purposes in serving the mission and principles of the college and of our students and employees in the course of normal operations.

Effective security is a team effort involving the participation and support of every Greenfield Community College employee, student and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and information technology systems at Greenfield Community College. These rules are in place to protect the employee, student and Greenfield Community College. Inappropriate use exposes Greenfield Community College to risks including virus attacks, compromise of network systems, non-public data, services, and legal issues.

3.0 Scope

This policy applies to employees, students, contractors, consultants, temporaries, and other users at Greenfield Community College, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Greenfield Community College.

4.0 Policy

4.1 General Use and Ownership

1. While Greenfield Community College's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the college systems remains the property of Greenfield Community College. Because of the need to protect Greenfield Community College's network, the Information Technology Department cannot guarantee the confidentiality of information stored on any network device belonging to Greenfield Community College.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. The Human Resources Department follows college guidelines concerning personal use of Internet/Intranet/Extranet systems that apply to all employees. If there is any uncertainty, employees should consult their supervisor or the Human Resources Department.

3. The Information Technology Department recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see Information Technology Department's Information Sensitivity Guidelines. For directions on how to encrypt email and documents, go to the Information Technology Department's Security Awareness webpage http://www.gcc.mass.edu/information-security/.

4. For security and network maintenance purposes, authorized employees of Greenfield Community College may monitor equipment, systems and network traffic upon request by the President.

5. Greenfield Community College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy and security.
4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by Information Sensitivity Guidelines and the Family Educational Rights and Privacy Act (FERPA). Employees should take all necessary steps to prevent unauthorized access to this information.

2. Authorized users are responsible for the security of their passwords and accounts and should keep passwords secure and not share accounts. System level passwords should be changed quarterly; user level passwords should be changed every six months.

3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 20 minutes or less, or by logging-off (control-alt-delete for Windows users) when the PC, laptop or workstation is unattended.

4. Because information contained on portable computers is especially vulnerable, special care for security should be exercised. Protect laptops in accordance with the “Laptop Security Tips” located at the Information Technology Department’s Security Awareness webpage http://www.gcc.mass.edu/information-security/.

5. Postings by employees from a Greenfield Community College email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Greenfield Community College, unless posting is in the course of business duties.

6. All hosts used by an employee, student or community user that are connected to the Greenfield Community College Internet/Intranet/Extranet, whether owned by the employee, student or community user or by Greenfield Community College, shall be continually executing approved virus-scanning software with a current virus database.

7. Employees, students or community users must use caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, Trojan horse code, or other such damaging material.

4.3. Limitations

1. Full GCC computer resources are available only to currently enrolled students and full and part-time faculty and staff of GCC. Guest access is available to the general public on wireless, on open-access kiosks and in the Library.

2. All users are responsible for deleting files which are no longer needed.

3. All use of the GCC Computer Network must comply with this GCC Acceptable Use Policy and applicable state and federal laws. These policies are available online on the Information Technology Department’s webpage (http://web.gcc.mass.edu/it).

4. The GCC Computer Network must not be used for private or commercial business activities or personal computing not connected with the college.

5. Individual accounts and passwords are not transferable. Usage is limited to the person to whom access was issued. Use of another person’s account or providing unauthorized access to your account constitutes grounds for termination of all access privileges.

6. Profanity, harassing, obscene, or sexually explicit materials may not be sent through, downloaded to or transmitted from the GCC system. Such use constitutes grounds for termination of all access privileges and possible legal action.

7. Any attempt to disrupt, interfere with, modify, or damage the operation of the GCC Computer Network constitutes grounds for termination of all access privileges and possible legal action. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer worms and viruses or other damaging material, and using the network to make unauthorized entry to any other machine accessible via the network.

8. Any attempt to acquire information stored on the GCC Computer Network other than public information and the user's own files constitute a violation of the Commonwealth's Confidentiality laws and could be subject to legal action.

4.4. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may need to
disable the network access of a host if that host is disrupting production services or requested by the President).

Under no circumstances is an employee or student of Greenfield Community College authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Greenfield Community College-owned resources.

Any disciplinary action associated with this policy is subject to the terms of collective bargaining agreements.

The lists below are not exhaustive and provide a framework and guidance for unacceptable use activities.

**System and Network Activities**

The following activities are prohibited:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Greenfield Community College.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Greenfield Community College or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate supervisor should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others.
6. Using a Greenfield Community College computing systems to engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any Greenfield Community College account.
8. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
9. Port scanning or security scanning is expressly prohibited unless prior notification to the Information Technology Department is made.
10. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
11. Circumventing user authentication or security of any host, network or account.
12. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
13. Providing information about, or lists of, Greenfield Community College employees or students to parties outside Greenfield Community College without authorized college agreement.

**Email and Communications Activities**

1. Refer to the Greenfield Community College e-communication policy.
This policy is not intended to interfere with rights under the First Amendment or the National Labor Relations Act.

5.0 Revision History
2/11/2011 – M.F. review
4/17/2011 – M.F. incorporation of edits for joint review with M.A.
4/20/11 – M.F. incorporation of edits from joint review with M.A.
8/3/2011 – M.A. Added Information Security Site Link
9/17/2012 – IRM Support of Policy
3/2014 – M.A. Added first amendment and disciplinary action clause.
3/2014 – Endorsed By College Council
3/2014 – Approved by College Assembly