EMPLOYEE ACCEPTABLE COMPUTER USE POLICY

Gogebic Community College provides internet/intranet/extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, FTP, PDA devices, and cell phones are the property of Gogebic Community College. These systems are to be used for furthering the mission of Gogebic Community College and in serving the educational interests of our students.

The purpose of this policy is to outline the acceptable use of computer equipment at Gogebic Community College. These rules are in place to protect the employee and Gogebic Community College. Inappropriate use exposes GCC and the employee to risks including virus attacks, compromise of network systems and services, and legal issues.

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

General Use and Ownership

1. While Gogebic 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 remain the property of GCC, subject to intellectual property rights of faculty.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and there is any uncertainty, employees should consult their supervisor or manager.
3. For security and network maintenance purposes, authorized individuals within Gogebic Community College may monitor equipment, systems and network traffic at any time.
4. Gogebic Community College reserves the right to audit networks and systems at any time.

Security and Proprietary Information

1. The majority of information contained on Gogebic Community College databases is protected under FERPA and employees should take all necessary steps to prevent unauthorized access to confidential information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
3. All PCs, laptops, and workstations should be secured with a password when unattended, or by logging off when the host will be unattended.
4. Because information contained on portable computers is especially vulnerable, special care should be exercised.
5. Postings by employees from a Gogebic Community College email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Gogebic Community College, unless posting is in the course of business duties.
6. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

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 have a need to disable the network access of a host if that host is disrupting production services).

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

The list below is by no means exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

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 Gogebic 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 Gogebic Community College or the end user does not have an active license is strictly prohibited.
3. Intentional introduction of malicious programs into any workstation, network or server.
4. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home, along with work-study students.
5. Using a Gogebic Community College computing resource to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws, along with local, state, and federal laws.

6. Making fraudulent offers of products, items, or services originating from any Gogebic Community College account.

7. 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, pingoed floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

8. 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.

9. Circumventing user authentication or security of any host, network account.

10. Interfering with or denying service to any user other than the employee’s host (for example, denial of service attack).

11. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, anyone’s computing activity, via any means, local or via the Internet/Intranet/Extranet.

12. Providing information about, or lists of Gogebic Community College employees and students to parties outside Gogebic Community College.

Email and Communication Activities

1. Sending unsolicited email messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone, cell phone, or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster’s account, with the intent to harass or collect replies.

Blogging/Social Media

1. Blogging/social media by employees, whether using Gogebic Community College’s property and systems or personal computer systems, is also subject to terms and restrictions set forth in this policy. Social media includes LinkedIn, Twitter, Facebook, YouTube, My Space, Pinterest and others as they evolve. Limited and occasional use of Gogebic Community College’s systems to engage in blogging/social media is acceptable,
provided that it is done in a professional and responsible manner, does not otherwise violate Gogebic Community College policy, is not detrimental to Gogebic Community College’s best interests, and does not interfere with an employee’s regular work duties. Blogging/social media from Gogebic Community College’s systems is also subject to monitoring.

2. Gogebic Community College’s Confidential Information policy also applies to blogging/social media. As such, employees are prohibited from revealing any confidential information related to the college, employees, and students when engaged in blogging/social media.

3. Employees shall not engage in any blogging/social media that may harm or tarnish the image, reputation and/or goodwill of Gogebic Community College and/or any of its employees and students. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging/social media engaging in any conduct prohibited by Gogebic Community College.

4. Employees may also not attribute personal statements, opinions or beliefs to Gogebic Community College when engaged in blogging/social media. If an employee is expressing his or her beliefs and/or opinions in blogs/social media, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Gogebic Community College. Employees assume any and all risks associated with blogging/social media.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Date of Adoption: 5/27/08

Revised: 5/26/15