Kalamazoo College

Acceptable Use Policy

August 2016

1. Overview

Kalamazoo College provides and maintains information technology resources to support its academic programs and administrative operations. This Acceptable Use Policy ensures the integrity of information technology resources and prevents disruption to academic and administrative needs. Kalamazoo College is committed to protecting its employees, partners, and the College from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, and network accounts, are the property of Kalamazoo College. These systems are to be primarily used for business purposes in serving the interests of the College, and of our employees and students in the course of normal operations. Please review Human Resources policies for further details.

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

2. Purpose

The purpose of this policy is to outline the acceptable use of technology resources at Kalamazoo College. These rules are in place to protect the users and the College. Inappropriate use exposes Kalamazoo College to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Kalamazoo College business owned, managed, leased, or otherwise provided by Kalamazoo College.

This policy applies to employees, contractors, consultants, temporaries, and other workers at Kalamazoo College.
3.1 General Use and Ownership

3.1.1 Kalamazoo College proprietary information stored on electronic and computing devices, whether owned or leased by K, the employee, or a third party, remains the sole property of Kalamazoo College. Users must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.

3.1.2 Users have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Kalamazoo College proprietary information.

3.1.3 Users may access, use, or share Kalamazoo College proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

3.1.4 Users are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, users should consult their supervisor or manager.

3.1.5 For security and network maintenance purposes, authorized individuals within Kalamazoo College may monitor equipment, systems, and network traffic at any time.

3.1.6 Kalamazoo College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

3.2 Security and Proprietary Information

3.2.1 All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.

3.2.2 System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

3.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

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

3.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.
3.3 Unacceptable Use

The following activities are, in general, prohibited. Users 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 a user of Kalamazoo College information technology resources authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing College owned resources.

The lists below are not exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

3.3.1 System and Network Activities

The following activities are strictly 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 Kalamazoo 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 Kalamazoo College or the end user does not have an active license.

3. Accessing data, a server, or an account for any purpose other than conducting Kalamazoo College business, even if you have authorized access.

4. Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

6. 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.

7. Using a Kalamazoo College computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

8. Making fraudulent offers of products, items, or services originating from any Kalamazoo College account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. 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.

11. Port scanning or security scanning, unless prior notification to the Chief Information Officer is made.

12. 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.

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

14. Introducing honeypots, honeynets, or similar technology on the K network.

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

16. 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.

17. Providing information about, or lists of, Kalamazoo College employees to parties outside K, except as required by one’s job (e.g. Human Resources) or with prior authorization of the Chief Information Officer.

3.3.2 Email and Communication Activities

When using College resources to access and use the Internet, users must realize they represent the College. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the college." Questions may be addressed to the Chief Information Officer. The following actions are prohibited:

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 or paging, whether through language, frequency, or size of messages.

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

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

5. Creating or forwarding "chain letters," "Ponzi" or other "pyramid" schemes of any type.

3.3.3 Blogging and Social Media

1. Employees must abide by the Social Media policy.

4. Policy Compliance

4.1 Compliance Measurement
The Information Services team may verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 Exceptions
Any exception to the policy must be approved by the Chief Information Officer in advance.

4.3 Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Related Standards, Policies and Processes

- Data Classification Policy
- Data Protection Standard
- Social Media Policy
- Minimum Access Policy
- Password Policy