Acceptable Information Technology Use Policy

A. Introduction

This policy is established to make users of Gonzaga University’s computing resources aware of their privileges and responsibilities, and to maximize the value of those resources to the Gonzaga community, while permitting maximum freedom of use consistent with the law, Gonzaga University’s Mission statement, the Student Handbook, the Gonzaga University Policies and Procedures Manual, the Faculty Handbook, and a productive environment. Any use of Gonzaga University computing resources that violates policies contained in these manuals and handbooks also violates this policy.

B. Definitions

1. **Gonzaga Computing Resources**: the physical network media and the attached computers and software owned or controlled by Gonzaga University. Gonzaga computing resources includes ZagNet, the student network connecting the residence halls to the campus network.

2. **Mobile Data Devices**: any device used to access or store Gonzaga University data including: cell phones, smart phones, thumb drives, or portable electronic devices of any kind.

3. **Internet**: the global computer network composed of millions of computers and thousands of networks.

4. **Logged on**: connected to a service through a non-public, user identification (e.g., personal account).

5. **Resource**: any computing device, peripheral, software, or related consumable (e.g., paper, disk space, central processor time, and network bandwidth) owned or controlled by Gonzaga.

6. **Service**: any software that makes a computer’s files or other locally stored information available for use by another computer or facilitates the transfer of data between two remote computers. Services include, but are not limited to, web, file, and e-mail server software.

7. **Spam**: unsolicited mass e-mail for the purpose of advertising a service, personal gain, or other inappropriate use.

8. **Mass Mailing**: electronic mail sent unsolicited to a large number of employees or students or to a campus-wide distribution list.

9. **Internet Cloud Based Services**: digital services, applications, storage, and data that are provided remotely and delivered and consumed in real-time over the Internet.

C. Staff and Faculty User Responsibility

1. Gonzaga computing resources are provided primarily to support the Mission and operations of Gonzaga University. Users may occasionally use Gonzaga computing
resources for personal needs as long as such use is consistent with established Gonzaga University policy and does not inhibit academic or administrative use of Gonzaga computing resources.

2. Gonzaga University uses electronic mail (e-mail) and morning mail as official means of communication and to conduct Gonzaga business. Employees and students are responsible for checking and maintaining their email accounts.

3. Gonzaga University cannot provide, and will not be responsible for, software kept on personally owned computers, nor is it responsible for the installation, repair, maintenance or upgrade of personally owned hardware.

4. Employees are required to ensure that Gonzaga University-related information contained in e-mail/Internet messages is accurate, appropriate, and lawful.

5. Users must secure their computer when they will be away from their computer. Data on local hard drives must be secured either through password protection or physical security (e.g., locked office) when a user is not present.

6. Personal accounts are confidential and must not be shared with others. Passwords must be changed as required. Users must not store or transmit passwords.

7. Employees, students, and other authorized users may post electronic materials for public access, provided those documents conform to policies contained within the Student Handbook, Gonzaga University Policies and Procedures Manual, the Faculty Handbook and relevant laws.

8. It is the employee’s responsibility to report to their immediate supervisor, HR or Information Technology Services any e-mail that is received from a member of the Gonzaga staff, faculty or student body that is believed to be in violation of this policy.

9. Announcements for events to all staff, faculty or students should be sent through Morning Mail. If an employee or student believes s/he has an exception (e.g., safety, security, breaking news of high importance, etc.) s/he should contact her/his area Vice President or the Vice President for Student Life. If an exception is granted, the email should be sent from the area Vice President’s email account. Electronic mail sent by faculty members to students for purposes of facilitating academic work and faculty member use of the Faculty-l list do not require prior approval.

10. All users should log-off at the end of their shift in order to facilitate patching and upgrading computers with minimal impact to users.

11. Personally-Owned Computers or Mobile Data Devices: Users are responsible for protecting confidential data on personally owned computers, mobile data devices or on internet-cloud based services.

12. Connecting Remotely
   a. An employee wishing to use Gonzaga University’s remote access systems must obtain permission from his/her direct supervisor prior to first use of the remote access systems.
b. All security policies applied in the Gonzaga office environment must also be applied when using or connecting to Gonzaga computing resources outside the Gonzaga office environment. Workstations, laptops and other devices that connect to the Gonzaga University Network must have up-to-date virus protection and personal firewall software enabled where available.

c. Participation in a remote access program may not be possible for every employee. Remote access is meant to be an alternative method of meeting Gonzaga University needs. Gonzaga may refuse to extend remote access privileges to any employee or terminate a remote access arrangement at any time.

d. Work done at a remote location is considered official Gonzaga business. All work product such as files, tables, reports, databases, programs and other content created while remotely accessing data or services are considered official records.

13. Staff and Faculty should reference the following policies, found in the Gonzaga University Policies and Procedures Manual, as they relate to acceptable information technology use: Professional Conduct Standard, Cell Phone Policy, Social Media Policy, Harassment and Discrimination, and Confidential Information Policy.

14. All employees agree to apply safeguards to protect Gonzaga University information assets from unauthorized access, viewing, disclosure, alteration, loss, damage or destruction. Appropriate safeguards include use of discretion in choosing when and where to use remote access tools or services, prevention of inadvertent or intentional viewing of displayed or printed information by unauthorized individuals, use of local encryption on devices, use of passwords for controlling access, and use of antivirus software on remote computers. Employees will immediately report to their supervisor and Information Technology Services all incidents involving suspected or actual unauthorized access, disclosure, alteration, loss, damage or destruction of data, including data stored or accessed from Gonzaga University or a remote location.

D. Unacceptable Uses

1. Using Gonzaga computing resources for unlawful activity or in violation of any Gonzaga Policy.

2. Using Gonzaga computing resources for sending inappropriate emails or accessing websites that are contrary to Gonzaga’s Mission and professional conduct standards (pornography, profanity, harassing or discriminatory jokes, degrading or offensive content, etc.).

3. Sending spam or creating or retransmitting chain e-mail messages.

4. Sending e-mail from another user’s account.

5. Altering the header of an e-mail message to prevent the recipient from determining the actual sender of the e-mail.

6. Logging into or using any computer account or accessing, modifying, or creating any files without the account owner’s permission.
7. Introducing new services or resources (e.g., personal web server) or altering existing services or resources (e.g., registering personal domain name) on Gonzaga computing resources without the approval of Information Technology Services.

8. Bypassing internal security technology controls and ITS protocols and protections.

9. Using Gonzaga University resources, including Gonzaga computing resources, for political gain or exclusive personal gain.

10. Transmitting, without authorization, Gonzaga University proprietary information.

11. Wasting resources such as print services, disk space, and network bandwidth.

12. Intercepting network traffic without authorization.

13. Using Gonzaga computing resources for any activity that degrades Gonzaga University provided services, denies services to other Gonzaga computing resources users, or jeopardizes the security or capabilities of Gonzaga computing resources.

E. Privacy

1. Gonzaga computing resources are intended for Gonzaga business and academic purposes. All e-mail, electronic communication, and electronic files or documents that are transmitted, received, accessed, or stored using Gonzaga computing resources are considered Gonzaga records and are subject to review by authorized Gonzaga representatives, disclosure to law enforcement or government officials, or third parties through subpoena or other processes.

2. Individual Gonzaga web pages, phone number and e-mail may be listed on Gonzaga directories.

F. Violations

A violation of this policy may result in corrective action up to dismissal from employment or the university.