Acceptable Use of Information Technology Resources
Policy Number (TBD)

FULL POLICY CONTENTS

Scope
Reason for Policy
Policy Statement
Procedures
Definitions
Exceptions
Sanctions
Related Policies, Documents & Forms
Archival

Effective: October 1, 2016
Last Updated: March 8, 2017

Responsible University Office:
Information Technology Services

Policy Contact:
Chief Information Officer

Scope

This policy applies to all users of university IT resources, whether or not they are affiliated with the university, and whether or not they are on campus or connect from remote locations.

This policy applies to all IT resources of the university, including:

- All facilities, computers, systems, equipment, software, networks, databases and other electronic information resources, and computer facilities owned, leased, managed, or maintained on behalf of the university for the handling of data, voice, television, telephone, cellular, microwave, or related signals or information;

- Any access or use of the university's electronic resources, including the university Internet connections, from a computer, device or other system not controlled or maintained by the University.

- Access to the university computing resources from personal equipment is covered under this policy.

Reason for Policy

Gonzaga information technology (IT) resources are provided to support the mission and operations of Gonzaga University. This policy is established to make users (see Section C, Definitions) of Gonzaga University's IT resources (see Definitions), aware of their privileges...
and responsibilities related to those resources. IT resources are provided or allowed to interact with university systems solely in order to enable the university to fulfill its academic, service, and administrative purposes, and they must be used in a manner supportive of a productive work environment and consistent with the law, Gonzaga University’s Mission Statement, and other institutional policies.

Access to university IT resources is revocable. Users must abide by all applicable restrictions, whether or not the restrictions are integrated into the IT resources or can be circumvented by technical means. Acceptable use of IT resources must always be ethical, demonstrate academic honesty and show restraint in the consumption of shared resources. Acceptable use supports respect for intellectual property rights, maintains the confidentiality of information, ensures the privacy and security of information, and promotes freedom from intimidation and harassment. All users are expected to demonstrate these values at all times in their use of university IT resources.

Gonzaga recognizes the value of privacy as a condition for academic freedom and the benefits that privacy and autonomy bring to the individual, to groups, and to the culture of the institution. When involving the acceptable use of university IT resources, IT personnel may engage in activities authorized by this policy, respectful of and consistent with the requirements for academic freedom expressed in the Faculty Handbook and to community members’ professional and legal obligations to protect others’ information, to ensure that any use is consistent with this policy. Users of IT resources are urged to review and understand the contents of this policy.

Policy Statement

User Responsibilities

All users of Gonzaga University’s IT resources are expected to conform to the following responsibilities:

1. Personal use of university resources is only permitted if the usage does not interfere with the performance of work duties, compromise the security, integrity or performance of university property, information, or software, and does not incur a cost to the university.

2. Use university data only for approved academic and administrative purposes.

3. Respect the finite capacity of the university's IT resources; this means limiting use so as not to consume an unreasonable amount of those resources or to interfere with the activity of other users;

4. Know that your Gonzaga email account and Morning Mail are official means of university communication;
5. Maintain sole responsibility for supporting and maintaining personally-owned devices;
6. Respect the rights of others, e.g. refrain from accessing others’ files, conducting denial of service attacks, misrepresentation, forgery, or attacking university IT resources;
7. Do not circumvent, ignore, or attempt to break information security mechanisms and controls;
8. Obey local, state, federal, copyright, and other applicable laws;
9. Secure devices used to fulfill job responsibilities, including those that store or transmit university information;
10. Securely store and transmit data and information;
11. Use only those IT resources you are authorized to use and only in the manner and to the extent authorized;
12. Protect your account and passwords;
13. Use passwords appropriately;
14. Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected;
15. Report security breaches, loss of data, or other violations of this policy to the Office of the CIO;
16. Use only licensed software, in compliance with vendor’s/owner’s license terms of use;
17. Do not engage in prohibited activities (see below);
18. Follow any other related university policies and procedures.

**Prohibited Activities**

Gonzaga University IT resources may not be used for any of the following purposes (this list is illustrative, not exhaustive):

1. **Unlawful Activity or Violation of University Policy:** Gonzaga IT resources may not be used to engage in behavior or communications that violate the law or university policy, including but not limited to:
   a. Discrimination
   b. Fraudulent activity
   c. Harassment
   d. Obscene materials
e. Threats of violence or harm
f. Child pornography
g. Copyright infringement

2. Political Use: Gonzaga IT resources may not be used for partisan political activities except with the prior written approval of the user’s divisional Vice President.

3. Commercial Use: University’s systems or networks may not be used for personal financial gain or benefit, for example, by engaging in a commercial enterprise or selling access to your User ID, university systems, or networks. Faculty may engage in work such as consulting only in accordance with the Faculty Handbook and university policy.

4. Personal Use: Except as otherwise provided in this policy, Gonzaga IT resources may not be used for personal purposes, except limited incidental use (see D1, above). Users may not use any university data (see Definitions) for any personal purposes.

5. Harmful or Destructive Activity: Users may not engage in harmful or destructive activities. Such activities include, but are not limited to: creating or propagating malicious software, (except for academic purposes under the supervision of a faculty advisor supervisor in a controlled, isolated environment), accessing university information without appropriate authorization, disrupting services, damaging files, intentionally damaging or destroying hardware, software, or other data belonging to Gonzaga University or other users, or obtaining unauthorized resources.

6. Network Installations: Users may not, without authorization from ITS, connect any network equipment to the university campus network. Network equipment includes, but is not limited to: wireless access points, hubs, routers, firewalls, bridges, switches, network traffic monitoring/capture and analysis tools, and modems or any devices or applications that provide network connectivity to more than one individual computer system. Users may not connect to the network any computer that is configured to perform the functions of the aforementioned network equipment.

7. Anonymous Usage: Users may not run network services that allow the anonymous use of the Gonzaga network except as specifically provided by Gonzaga ITS (e.g. guest network access). Security must be provided through usernames and passwords that are traceable to individual users.

8. Sharing of Access: Users may not share any passwords or other types of authorization. Accounts are assigned to individual users who are responsible for any use of their accounts.

9. Unauthorized Access: Facilities, accounts, access codes, malicious software (e.g. keystroke logging software or password capture/decryption applications), privileges, or information may not be used without appropriate authorization. Users may not gain or attempt to gain unauthorized access to systems through the use of a special password, loopholes in computer security systems, or another user’s password. Authorized access
must not be used beyond need-to-know basis or the purpose for which access is granted. Information obtained through special access is confidential.

10. **Unlicensed Software:** No software may be installed, copied, or used on Gonzaga IT resources except as permitted by the owner of the software and the university. Software subject to licensing must be properly licensed, and all license provisions (e.g. installation, use, copying, the number of simultaneous users, terms of the license, etc.) must comply with this policy, as well as all applicable laws and contractual agreements.

11. **Degrading or Wasting of Resources:** Users may not overload networks with excessive data, degrade services, or waste IT resources, intentionally or negligently interfere with the proper operation of any system or its use by other users, cause congestion, overload or disruption of networks or systems, or create or knowingly disseminate unwanted and unsolicited emails or materials (SPAM).

12. **Alteration or Disposal of University IT Resources:** Users may not dispose of IT resources, or remove, transfer, disable or dispose of computer software licensed to the university without authorization from ITS.

13. **Falsifying Information:** Users may not knowingly or negligently falsify information stored or managed by the university.

14. **Transmitting or Storing Sensitive Information on Cloud Services:** Users may not store or transmit sensitive/confidential information using unapproved cloud services (see Definitions). Sensitive or confidential information includes but is not limited to FERPA-protected information, personally identifiable information, personal health information, confidential university business information, or personnel records, or other information that reasonably could be considered sensitive or confidential.

15. **Processing Payment Cards Without Authorization:** Users may not accept, transmit, or process payment cards or payment card numbers without prior authorization from the Controller’s Office.

16. **Sharing University Sensitive or Confidential Data with Third Parties:** Users may not share sensitive or confidential university data with any unauthorized third parties, including vendors, contractors, individuals, media organizations, regulators, law enforcement, and others without appropriate authorization (see Data Release Policy).
Security and Privacy

Gonzaga IT 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 IT resources, or are created and maintained to conduct university business, are considered Gonzaga records when it comes to compliance with this policy, and are subject to review by authorized Gonzaga representatives consistent with the need to protect academic freedom and the notification requirements set forth in the Faculty Handbook, disclosure to law enforcement or government officials, or third parties through subpoena or other processes, subject to community members’ professional and legal obligations to protect others’ information. This includes work performed from remote locations or personally owned devices.

Although the university does not routinely monitor email, data, software, or other online activity of users, it reserves the right to do so to assure acceptable use of its technology and as may be deemed necessary as set forth below. Only in extenuating circumstances, and to prevent risk to the university will the examination of the content of data be allowed. Every effort will be made to preserve professional confidences as required in the conducting of authorized professional services provided by university community members and subject to other external laws and obligations.

The university may be compelled by law to gather and/or disclose digital information of its users, such as pursuant to a subpoena, civil discovery hold or request, request of a governmental agency, or court order. Upon approval of General Counsel and one of the following: Academic Vice President, Assistant VP Human Resources, CIO; subject to the Faculty Handbook requirements and community members’ professional and legal obligations to protect others’ confidential information, the university may access, monitor, remove, or disclose a user’s communications or other data on university systems or personal devices. User(s) are required to cooperate in an investigation. In the event a user fails to cooperate, their user account credentials may be revoked, and they may be subject to other action or discipline. See “Enforcement” below.

The university may suspend access privileges of any individual user or device without prior notice for reasons relating to alleged or actual violation(s) of this or other university policies, threats of harm to IT resources or university data (see Definitions), performance degradation or interruption of IT systems, contractual obligations, or applicable law.

Definitions

1. **Cloud Services**: The array of Internet-based services and applications, often available to the public, for gathering, storing, processing and sharing information. Cloud services are managed and operated by the vendor offering the service and are not under the control of the university except as defined in the terms of any contract governing the service’s
use. The university may enter into approved contractual relationships with certain cloud vendors. These vendors and their approved services are considered approved IT resources.

2. **Community Members:** May include all Gonzaga University employees, staff, faculty, students, contractors, affiliates, alumni, benefactors, visitors, and guests.

3. **Information Technology (IT) Resources:** Those facilities, technologies, and information resources required to accomplish information processing, storage, access, security, and transmission of electronic information, whether individually controlled or shared, stand-alone or networked. IT resources include cloud services (See #1, above) for which the university has entered into an approved contractual relationship. Personal equipment physically or logically connected to the university network is also subject to this policy, including any technology already in place or to be deployed.

4. **University Data:** University data is information about members of the extended Gonzaga University community (for example: students, faculty, emeriti, staff, honored retirees, donors, authenticated guests and authenticated vendors) or information that is created, managed, maintained, collected, or stored in the course of conducting university business and academic activities (associated policy: Records Retention Policy).

5. **User:** Any entity accessing, logging into, or attempting to access or log into, a university hardware or software system; or connecting to, or attempting to connect to or traverse a university network, whether by hardware or software or both, from any location. The term "user" thus includes faculty, staff, students, visitors, vendors, contractors, service providers, automated software programs/agents (and their developers), and any other individuals or agents who access and use university information technology.

---

**Enforcement and Administration (Sanctions)**

Violations of this Acceptable Use Policy can range in seriousness from accidental to illegal. Where acceptable use comes into question, the university reserves the right to determine what is appropriate and acceptable and what is not. When requested, users are required to cease any activity deemed in violation of this policy. Failure to comply may result in revocation of user account credentials or other action, up to and including dismissal from employment or the university, depending on the nature and severity of the offense.

Using IT resources in the work environment in a manner that results in inappropriate conduct will be addressed as an employee performance or student conduct issue, even if such conduct does not rise to the level of a university policy violation. Violators are subject to disciplinary action as prescribed in the Student Handbook, the Gonzaga University Policies and Procedures Manual, the Faculty Handbook, and other applicable documents. Offenders also may be subject to criminal prosecution or civil suit under laws including, but not limited to, the Communications Act of 1934 (as amended), the Computer Fraud and
Abuse Act of 1986, The Computer Virus Eradication Act of 1989, Interstate Transportation of Stolen Property, the Electronic Communications Privacy Act, the U.S. Copyright Act, and state and federal child pornography laws. Violators may also be responsible for reimbursing the University for any costs resulting from violations of this policy.

This policy is administered jointly by Information Technology Services and Human Resources. Questions or reports of policy violations should be made to the Office of Information Technology Services, the Office of Human Resources, or anonymously via the Whistleblower procedure (see Whistleblower Policy).

Related Policies, Documents & Forms

Whistleblower Policy

Data Retention Policy

Data Release Authorization Policy