Information Technology Use

FULL POLICY CONTENTS

Effective: *February 15, 2018*

Last Updated: *March 2021*

Responsible University Office: *Information Technology Services*

Policy Contact: *Chief Information Officer*

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 of Gonzaga University's IT Resources, 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. Use of IT Resources by Users must always be ethical, demonstrate academic honesty, show restraint in the consumption of shared resources, respect intellectual property rights, maintain the privacy and security of Sensitive or Confidential Information, and promote 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 use of University IT Resources by any user, IT personnel may engage in activities authorized by this policy, subject to the Faculty Handbook and to Community Member's professional and legal obligations to protect others' confidential or privileged 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.

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; and

- Access to the University computing resources from personal equipment.

Definitions – Unless otherwise indicated, the following definitions apply only within the context of this policy.

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. A list of approved cloud vendors can be found at www.gonzaga.edu/its or by contacting the Support Center at techsupport@gonzaga.edu.

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

3. **Excessive Use of Resources:** Excessive use of university information technology resources, especially when it impedes the mission-related activities of other users, or adversely affects system availability or performance.

4. **Information Technology (IT) Resources**: Those facilities, technologies, and other 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 for which the University has entered into an approved

contractual relationship. Personally owned equipment connected to the University wired and wireless network is also subject to this policy, including any technology already in place or to be deployed.

5. **Sensitive or Confidential University Data:** This includes but is not limited to FERPA, HIPAA, PCI, or GDPR- protected information, personally identifiable information,

   personal health information, proprietary or confidential University business information, or personnel records, information relating to the authorized legal representation of a client by a Community Member or other information that reasonably could be considered sensitive or confidential. Nothing in this definition or policy shall interfere with an employee's right to participate in protected concerted activity or other protected activity.

6. **University Data**: University Data is information about members of the extended Gonzaga University community (for example: students, faculty, emeriti, staff, 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).

7. **User**: Any person or 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" 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.

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 IT 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;

2. Use University Data only for approved academic and administrative purposes;

3. Respect the finite capacity of the University's IT Resources. This means to not consume an unreasonable amount of those resources or to interfere with the activity of other Users;

4. Gonzaga email accounts and Morning Mail are the only official means of University email communication. Users are responsible for checking their email account on a regular basis;

5. Ensure that personal devices are patched with the latest operating system and security updates before using them to access University Data;

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. Physically secure devices that store or transmit University Data by using a cable lock or keeping them in a locked drawer when not in use. Lock any log-in screen when walking away from the device;

10. While users may access Sensitive or Confidential University Data using personal devices, the data should only be stored and transmitted using university systems like Office 365, Blackboard, Zagweb, etc.;

11. Use only those IT Resources you are authorized by the University to use and only in the manner and to the extent authorized;

12. Protect your account and passwords;

13. Create and change passwords when prompted;

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 Chief Information Officer (CIO);

16. Use only licensed software, in compliance with licensor's terms of use;

17. Do not engage in prohibited activities (see below); and

18. Follow all 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. Pornography
g. Copyright infringement

2. Political Campaign Activity: Gonzaga IT Resources may not be used in a purely political manner to support or oppose a candidate for public office, political party, or ballot initiative. This prohibition on the use of University IT Resources in a purely political manner is necessary to maintain the University's tax-exempt status as a 501(c)(3) organization.

3. Commercial Use: Gonzaga IT Resources 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 (User Responsibilities, subparagraph 1, above) during non-working time. Users may not use Sensitive or Confidential University Data for 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 from the University, disrupting services, damaging files, intentionally damaging or destroying hardware, software, or other data belonging to Gonzaga University or other Users, or obtaining unauthorized IT 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. Anonymous Usage: Users may not run network services (i.e. connecting a device to the university's wired or wireless network) 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.

7. 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.

8. Unauthorized Access: Password protected systems may not be accessed without appropriate authorization. Users may not gain or attempt to gain unauthorized access to these systems through any other means than their own user ID and password. Another user's User ID and password must never be used. Authorized access must not be used beyond the purpose for which access is granted. Information obtained from password protected systems is confidential.

9. 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.

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

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

12. Falsifying University Data: Users may not knowingly or negligently falsify University Data.

13. Transmitting or Storing Sensitive or Confidential University Data on Cloud Services: Users may not store or transmit Sensitive or Confidential University Data using Cloud Services other than those listed as approved on the ITS Web Site.

14. Processing Payment Cards Without Authorization: Users may not accept payment card payments, transmit, or process payment card information without prior authorization from the Controller's Office.

15. Sharing Sensitive or Confidential University 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 Authorization).

Security and Privacy

Gonzaga IT Resources are intended for Gonzaga business and academic purposes. All email, 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 subject to the Faculty Handbook and to Community Members' professional and legal obligations to protect others' Sensitive or Confidential University Data. This includes work performed from remote locations or personally owned devices.

Although University staff does not routinely monitor email, data, software, text messages, 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 and client confidences including Sensitive or Confidential University Data as required in the conducting of authorized professional services provided by 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 the Provost & Senior Vice President, Assistant VP for Human Resources, CIO, or in case of information relating to the legal representation of a client by a Community Member, the Dean or Associate Dean of the Law School, 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 and Administration (Sanctions)" below.

The University recognizes the unique nature of digital information stored or created by the law school in the representations of clients; specifically, records covered by the attorney-client privilege, or otherwise relating to the authorized representation of a client, and the attorneys' professional and legal obligations regarding those records. Prior to the University accessing, monitoring, removing, viewing, collecting, or disclosing Sensitive or Confidential University Data from the law school, its students, its faculty, or any Community Member providing services to Gonzaga Law School – Clinical Legal Program (GLS-CLP), for any purpose other than internal maintenance of IT Resources, the University, to the extent permitted by law, will notify the Dean of the Law School, the Associate Dean for Academic affairs & Program Innovation, or the Coordinating Lawyer of GLS-CLP, each of whom may require the persons involved, as prerequisite to such activity, to execute a confidentiality agreement as appropriate to preserve the right of any legal client to assert the attorney-client privilege.

Enforcement and Administration (Sanctions)

Violations of this policy can range in seriousness from accidental to illegal. The University reserves the right to determine when use is in compliance with this policy and when it 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.

The University may also 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, performance degradation or interruption of IT systems, contractual obligations, or applicable law.

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 the Chief Information Officer, the Office of Human Resources, or anonymously via the Whistleblower procedure (see Whistleblower Policy).

Related Policies, Documents & Forms

Data Release Authorization
Faculty Handbook
Policies & Procedures Manual
Records Retention Policy
Student Code of Conduct
Whistleblower Policy