Policy Title: Acceptable Use of Information Technology Resources
Summary: This policy establishes requirements and expectations for the use of information technology resources at Drake University.
Policy Category: Information & Technology
Policy Owner: Information Technology Services
Policy Status: Effective 8/1/19
Effective Date: August 2019

Purpose

The purpose of this policy is to make Users of University Information Technology (IT) Resources aware of their privileges and responsibilities. These resources are provided with a primary purpose of supporting the education, instruction, research, and administration activities of the University. Users of these resources may have access to valuable resources and sensitive information. Therefore, it is imperative that Users act in a responsible, ethical, and legal manner.

Scope

This policy applies to and governs:

- All individuals and devices using, or attempting to use, University IT Resources or University Information, regardless of their affiliation with the University and whether on campus or connecting from a remote location.
- Resources including, but not limited to, all computers, systems, software, network and internet connections, databases, and computer facilities owned, leased, managed, or maintained on behalf of the University.
- All University Information including files, documents, data, images, software, logos and other marks, and any other University-owned or managed electronic materials and content.
- Personal devices, when used to interact with or connect to or through University resources.

Policy

The IT Resources in use at Drake University are designed to support the University's mission and operations, and the use of these resources is a privilege extended to faculty, staff, students, guests, vendors, and other members of the University community. Users are expected to demonstrate sound judgment and professionalism when using or interacting with University IT Resources and to recognize and act in accordance with the understanding that University IT Resources are provided in order to support Drake's mission and conduct its business. Users are also expected to treat the protection and confidentiality of University information and data as essential responsibilities when using University IT Resources.

Users of these resources may have access to, and interact with, extensive services and sensitive information. This information, including email messages, electronic communications, and electronic files and documents, which are created, accessed, transmitted, or stored using University IT Resources are considered to be University Information, and are subject to review by authorized University representatives, disclosure to law enforcement or other third parties through subpoena or other proceedings.

Information stored on or transmitted through University IT Resources may be preserved for an extended period, including after a User's affiliation with the University ends. The University has the legal right to log, access, and review all information stored on, or transmitted through IT Resources.

While the University employs measures to protect IT Resources, Users should be aware that the University cannot guarantee absolute security. Users must take steps to safeguard accounts and information in accordance with University policy and best practices.

The University may suspend, disable, or terminate access privileges for any User or device found or suspected to be violating this or other University policies, threatening or harassing others, threatening or harming IT resources or University information, degrading performance of IT resources, or violating contractual obligations or applicable law.

All Users of University IT Resources must abide by the following responsibilities.

1. Maintain the security and privacy of the account(s) assigned by the University. Users must not share passwords or authentication credentials with others. These credentials are assigned to individuals and the responsibility for actions performed is exclusively the User's.

2. Only use the University's name as authorized. The exchange of ideas is encouraged, however Users shall take appropriate steps to avoid possible inference that communication of a message via the University email system or other electronic communication implies official University endorsement or authorization.

3. Refrain from excessive personal use. Personal use may be excessive if it affects productivity, overburdens a system or network, subjects the University to increased operating costs, or is otherwise detrimental to the University. University Resources may not be used by employees for personal commercial gain under any circumstances unless approved in advance by a member of the University President's Council or formal designee, or the Dean of a university school or college. See also: Academics Political Activity Policy.

4. Respect the rights of others by not interfering with others' authorized and appropriate use of IT Resources. This includes unauthorized access of another User's or the University's information, impersonation of others, threatening or harassing others, and/or conducting attacks against systems and networks.

5. Appropriately secure all systems and devices used to fulfill job responsibilities and/or transmit or store University information, including personal devices. Users have sole responsibility for securing any personal device(s) used in this capacity.

6. Access information only as authorized. Where access has been given to Confidential or Restricted information, Users must limit use to that which is needed to perform job duties. Secondary use of University information may be restricted by federal or state law, or industry regulations, including the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach Bliley Act (GLBA) and the Payment Card Industry Data Security Standard (PCI-DSS).

7. Respect and adhere to all laws and regulations, including those governing software and copyright. Users are responsible for recognizing and honoring the intellectual property rights of others, and must not install, copy or use software except as permitted by the software owner and the University. Users must not use images or

other digital works except as permitted by the copyright owner.

The following activities are provided as examples of prohibited behavior as outlined by this policy. Examples are illustrative and do not represent an exhaustive list of scenarios governed by this policy.

1. Circumventing or harming, whether through hardware or software, any security or access control measure on any computer or network system.

2. Examining, collecting, or modifying any information from a computer, network, or system, or breaking the confidentiality, integrity, or availability of such information or systems for which the User is not authorized.

3. Transmitting or storing University information classified as Confidential (see Information & Technology policy *Information Security*) using an unapproved cloud service.

4. Activities violating the law and/or University policy, including harassment, discrimination, fraud, viewing or distributing certain types of pornography, and copyright infringement.

5. Threatening, harassing, intimidating or otherwise engaging in interpersonal behavior and communication that is unprofessional or violates other university policy or law.

6. Failing to follow procedures or take reasonable precautions to appropriately protect and prevent unauthorized access to university information and data.

7. Connecting network devices to the University network without authorization from Information Technology Services, including network monitoring/analysis tools, routers, switches, wireless access points, or other devices that grant special access to one or more devices.

By using or attempting to use University information technology resources, Users agree to abide by this policy and all related University policies and procedures, as well as applicable local, state, and federal laws.

Enforcement

Violations of this 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. The University may also take action unilaterally and without consultation. When requested, Users must 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. Some violations may also be subject to civil or criminal action.

Definitions

User – An individual who connects, accesses, logs into, or traverses a University system or network; or attempts to connect, access, log into, or traverse a University system or network. Therefore, a User includes faculty, staff, students, visitors, vendors, and other authorized and unauthorized entities.

Information Technology (IT) Resources – Facilities, technologies, and information resources used for University information processing, transfer, storage, and communications. This includes computer labs, classroom technologies, computing and electronic communications devices and services, email, networks, mobile devices, voicemail, fax transmissions, video, multimedia, and instructional materials. This also includes services that are University-owned, leased, operated or provided by the University or otherwise connected to University resources, such as cloud and Software-as-a-Service (SaaS), or any other connected/hosted services provided.

University information – Information created, accessed, transmitted, or stored in the course of conducting University business and academic activities. This includes information produced by the extended University community when executing work on behalf of the University, including course information, student work, grades, academic outcomes, research, and information about University strategy, operations, and intellectual property. University information does not include, for the purposes of this policy, information that a member of the University community owns or has rights to, or information housed in the public domain.

Cloud Service – A product offered by a third-party company consisting of on-demand, shared internet-based platforms, infrastructure, applications, or storage services. Third-party cloud services are not approved IT resources by default. The University may enter into

contract with a third party offering a cloud service, at that point the Cloud Service would be considered an approved IT resource.

Excessive Personal Use – University IT Resources may be used for personal purposes, but should not be associated with political activity, result in the disclosure of Confidential information, impact productivity, or promote illegal or unethical behavior. Remember that University IT Resources are not private and may be subject to subpoena and their use disclosed by court order. See Human Resources Policy *Use of Communications Tools* for more information.

Unauthorized Network Devices – Devices or tools that subvert or bypass the security of the University network, or cause interference with normal network and security operations. Examples include a router or access point, which may allow unauthorized devices to connect to the University network and interfere with existing wireless infrastructure.

Appropriately-secured Personal Devices – Computers and mobile devices with security equivalent to the sensitivity of University information stored on them. For mobile devices on which Confidential information may be accessed or stored, this includes device encryption, a PIN or password, deleting information when no longer needed, and limiting features which allow insecure connections. See Information & Technology Policy *Information Security* for more information.