Acceptable Use of Information and Technology Resources

PURPOSE OF POLICY

The University upholds the tenets of academic freedom and complies with federal and state laws, while recognizing that protecting the Information and Technology Resources of the University requires ethical, legal, and secure use by all members of the University of Oklahoma Community.

In support of the University's mission of teaching, research and creative/scholarly activity, professional and University service, and public outreach, the University provides Information and Technology Resources and services to Students, faculty, staff, and other entities in an atmosphere that encourages sharing of Information and open and free discussion, for academic and other purposes to support the University's mission.

Accordingly, each user of University Information and Technology Resources must assume responsibility and accountability for the appropriate and responsible use of these resources and associated privileges. The information set forth below further defines authorities, rights, privileges, roles, and responsibilities, as well as consequences of possible misuse, and examples of misuse.

POLICY STATEMENT

The University of Oklahoma requires people who use its Information and Technology Resources to do so in a responsible manner, abiding by all applicable laws, policies, and regulations. Use of the University's Information and Technology Resources constitutes express consent to this policy. Users understand they have no expectation of privacy in the use of state resources and are limited to the uses as described herein.

WEB ADDRESS FOR THIS POLICY

http://www.ou.edu/content/ouit/security/compliance.html

SCOPE

ENTITIES/INDIVIDUALS AFFECTED BY THIS POLICY
All Norman Campus University Workforce Members, Students, and Visitors that access or use Information or Technology Resources of the University.

RESOURCES AFFECTED BY THIS POLICY
This policy applies to all Information and/or Technology Resources that are owned, leased by, or in the custody or control of the University as well as to any Information and/or Technology Resources that access such University resources or those that are used for any University-related business.

**POLICY**

**AUTHORITIES, RIGHTS, PRIVILEGES, ROLES**

**Access, Audit, and Monitoring of University Information and Technology Resources**

- The University retains its right and responsibility to manage and protect its Information and Technology Resources. The right and responsibility to manage and protect Information and Technology Resources includes, but is not limited to, monitoring and auditing equipment, systems, and network traffic; accessing data, e-mail messages, voicemail messages, Internet communications, system, network usage records, and other Information and Technology Resources at any time, with or without users' specific consent or knowledge; disconnecting, blocking, limiting, or otherwise actively responding to user sessions, user account activity, or devices that interfere with other systems, devices, or users on the University network or that are believed to be compromised or otherwise present a security threat to University Information and Technology Resources.

- Whenever any individual’s activity potentially threatens, erodes, or damages the capability, integrity, security, or sustainability of the University’s Information and Technology Resources by use of any electronic device, the University may take any action necessary to ensure the safety, security, and integrity of University assets, including, but not limited to, blocking, accessing, or disabling the electronic device.

**Privacy: Disclosure of Information and University’s Right to Access**

- University Information and Technology Resources may be subject to the Oklahoma Open Records Act and the information they contain may be statutorily open to, and must be made available for, public access pursuant to this law, unless expressly excluded by law. Users should be mindful that all information including e-mail and other communications may be reviewed by the public and, therefore, should consider the appropriateness of contents, language, tone, etc. All users of University Information Systems and Technology Resources have no expectation of privacy as to any information or communications thereon or the uses made of the Internet or email or other social media through the University’s systems or equipment.

- The University may adopt protocols for the review and access of computers, systems, and networks in order to safeguard information and technology resources. Such protocols may be adopted at the University’s discretion and shall not limit the University’s ability to access information under law or policy.

**Incidental and General Personal Use by University Workforce Members**

- Use of University Information and Technology Resources by University Workforce Members for personal use unrelated to University business should be minimal; must not detrimentally affect employee productivity; disrupt the systems and/or harm the University’s reputation or mission; and not violate any University policy or federal, state, or local law or regulation. Nothing herein shall restrict an employee’s right to discuss matters protected by applicable federal, state, or constitutional law.

- Use of University Information and Technology Resources for personal use is at one’s own risk. The University makes no guarantee of any users’ continued access to their personal information stored on University Resources.
Courtesy Email Accounts

- The University may provide courtesy email accounts to retirees, alumni, and other individuals no longer directly associated with the University. Courtesy email accounts are not a right and must be used for personal, non-public use. As such, these accounts are not records as defined by the Oklahoma Open Records Act, 51 O.S. § 24A.1 et seq. Courtesy email account users are required to comply with the terms and conditions of this policy and any other applicable information technology policy. The University reserves the right, in its sole discretion, to revoke use of this resource if it is used in a manner not consistent with University policies or at any time for any reason. The University is not responsible to courtesy email account users for any data loss, integrity, reliability, security, or unavailability.

RESPONSIBILITIES

Computers and networks can provide access to resources on- and off-campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege, and requires that individuals act responsibly. Users must respect the rights of other users, respect the integrity of University Information and Technology Resources, information or data thereon, and related physical resources, and observe all relevant laws, regulations and contractual obligations. All University Workforce Members, Students, and Visitors, and all University Components and their leadership, are responsible for and accountable for their use and management of University Information and Technology Resources.

Individuals

All University Workforce Members, Students, and Visitors are personally responsible and accountable for:

Integrity of Identity

- Maintaining the secrecy and security of any University account and password or other authenticator information, and for preventing their knowledge, access or use by anyone other than the individual to which the User was assigned.
- Protecting against unauthorized activities associated with the User’s University ID.
- Accurately representing the User’s identity while using University Information and Technology Resources and/or conducting University business.

Responsible Access

- Ensuring the User accesses only the Information the User is authorized to use and view.
- Ensuring that the User’s access to Information is in accordance with the intellectual property rights or confidentiality obligations pertaining to the Information.

Responsible Disclosure

- Determining and considering the sensitivity and value of University Information prior to sending it to another entity inside or outside the University, whether electronically or in hardcopy, and safeguarding the Information as appropriate.
- Ensuring that the User’s disclosure of University Information is in accordance with the intellectual property rights pertaining to the Information, and is in accordance with University policy and/or applicable law.

Care, Security, and Safeguarding

- Ensuring that University equipment, devices, systems, Information Resources, and technology remain within the control of or adequately secured by the University or its Workers at all times.
• Exercising due care in the use of University Information and Technology Resources and safeguard any such Information and Technology Resources within your control.

• Ensuring that use of University Information and Technology Resources does not interfere with, infringe upon, or otherwise negatively affect the equitable use or availability of the resources by other authorized users.

• Complying with all applicable laws, regulations, and University policy, whether or not specifically addressed in this policy.

**Responsible Reporting**

• Promptly reporting any suspected or confirmed violations of this policy or compromises of University systems or resources to appropriate management or campus contact.

**Departments and Department Leadership**

Leaders and management of University Components should

• Ensure all of their staff are informed of this policy and that each employee understands and undertakes to comply with this Acceptable Use Policy.

• Incorporate specific acceptable use and information security responsibilities into all contracts with third party individuals who have access to restricted, customer, or otherwise sensitive Information.

**RESTRICTIONS**

Activities that are expressly prohibited of all University Workforce Members, Students, and Visitors include, but are not limited to:

**Misuse of Identity**

• Allowing use of any University account or system session by others to whom it is not assigned.

• Using any University identifier, identity, account or credential that has not been assigned and authorized for your use.

**Malicious Use**

• Knowingly introducing malicious programs into a University network, server, or other resource.

• Attempting to harm or destroy data or systems of the University, another user, another agency, or network.

• Using University Information or Technology Resources in any way that is in violation of law, regulation, or other University policy.

**Violation of Intellectual Property, Software Licensing, Copyright, and Export Responsibilities**

• Using University Information or Technology Resources to copy and/or transmit any document, software or other matter in violation of any copyright, patent, or any other applicable intellectual property right, law, or regulation.

• Using University Information or Technology Resources to copy and/or transmit any document, software or other matter in violation of any export control or other federal law or regulation.
Unprofessional Use and Use Inconsistent with University Mission

- Using University e-mail or IP address or University Technology Resources to engage in conduct that violates University policies, guidelines, or state or federal law.

- Misrepresenting or exceeding the User’s authority in representing the opinion of the University when posting to a public newsgroup, distribution list, listserv, web site, blog/web log, social media service, or other public site or service with a University e-mail or IP address that may represent the University to the public.

- Using University Technology Resources to store, collect, distribute, or share content, information, or any data of any type that violates any University policy or guidelines.

- Using University Information and Technology Resources for commercial exploitation; dissemination of false, fraudulent, or misleading commercial advertising; dissemination of unsolicited commercial bulk emails; or to propose, consummate, or engage in any illegal transaction.

- Nothing herein shall restrict an employee’s right to discuss matters protected by applicable federal, state, or constitutional law.

Educational Systems and Platforms

The University provides faculty, staff, and students with access to various educational systems and platforms (course management systems, learning management systems, etc.) for academic, educational, and research use. These educational systems and platforms are extensions of the classroom and learning environment. Accordingly, their use is limited to academic, educational, and research purposes. Any other use is specifically prohibited, including, but not limited to, disseminating unsolicited, commercial messages; engaging in disruptive activity or behavior; or engaging any other conduct or behavior violating a University policy. Student information (i.e., class lists, contact information, or other education records relating to students) contained on an educational system or platform may be used solely for participation in the course, lesson, or presentation; dissemination of such student information should adhere to University policy.

Enforcement

- This policy is authorized and approved by the Security Governance Executive Council. The University’s Internal Auditing department is responsible for monitoring and enforcement of this policy. This policy will be reviewed every 3 years or as needed.

- The University considers any violation of this policy to be a potentially serious offense.

- Violators may be subject to disciplinary action including, but not limited to, those outlined in the Student Code, Staff Handbook, Faculty Handbook, and applicable laws.

- When it is determined that a system or account is being used in a way that appears not to comply with University policy, the system may be temporarily removed from the network or account disabled. When appropriate, the owner or user of the system or account may be informed of the reason for the action. It is the user’s responsibility to work collaboratively with the University to resolve the problem.

- The University reserves the right to copy, monitor, and/or examine any files or Information residing on University systems, networks, or computing resources related to the alleged unacceptable use and to protect its systems and networks from events or behaviors that threaten or degrade operations, and/or where an applicable Legal Hold notice is initiated, and/or the Office of Legal Counsel otherwise directs such action.
## Revisions and Approvals

### Revisions

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Version</th>
<th>Revised By</th>
<th>Changes made</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/5/2016</td>
<td>1.0</td>
<td>Caleb Muckala</td>
<td>Creation</td>
</tr>
<tr>
<td>8/31/2016</td>
<td>1.0</td>
<td>Anna Biggers/Caleb Muckala</td>
<td>SGAC and SGEC feedback and formatting</td>
</tr>
<tr>
<td>6/29/2017</td>
<td>2.0</td>
<td>Anna Vakulick</td>
<td>ITC Comments</td>
</tr>
<tr>
<td>12/20/2017</td>
<td>2.1</td>
<td>Ron Fellhauer</td>
<td>Approval updates</td>
</tr>
</tbody>
</table>

### Approvals

<table>
<thead>
<tr>
<th>Approval Date</th>
<th>Version</th>
<th>Approved By</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/31/2016</td>
<td>1.0</td>
<td>SGEC</td>
<td>CIO, OLC, AF, Provost</td>
</tr>
<tr>
<td>12/20/2017</td>
<td>2.1</td>
<td>IT Security Executive Committee</td>
<td>CIO, OLC, AF, Provost, VPR</td>
</tr>
</tbody>
</table>