Oklahoma State University Policy and Procedures

APPROPRIATE USE POLICY	**3-0601** **ADMINISTRATION & FINANCE** **Information Technology** **February 2021**

PURPOSE

1.01 As an institution of higher learning, Oklahoma State University encourages, supports, and protects freedom of expression, the free exchange of ideas, and an open environment that facilitates the pursuit of scholarly inquiry. The purpose of this policy is to outline, in general terms, the University's philosophy about acceptable use of information technology resources, with the overall objective of remaining consistent with other OSU A&M (e)rt - (c)i (t)-2 (e)2 (s)-,2 ( )-12 (a)-nd7 (r)3 (e
a s

SCOPE

2.01 This policy applies to all University owned or controlled information technology resources whether individually controlled or shared, stand alone or networked.

2.02 This policy applies to the users of University information technology resources, whether such persons are students, staff, faculty, or authorized third-party users.

2.03 This policy applies to all information technology resource facilities owned, leased, operated, or contracted by the University

2.04 This 2 (is)1t(he)Pd( )Tj10vo d( )T-h-2 (i)-2 (e)vr the

POLICY

4.01 User Responsibility and Expectations

Within the following sections, examples of acts or omissions, though not covering every situation, are included to specify some of the responsibilities that accompany computer use at Oklahoma State University, and to outline acts or omissions that are considered unethical and unacceptable, and which may result in immediate revocation of privileges to use the University's computing

report suspected unlawful or improper activities to the proper University authorities. Users have an affirmative duty to cooperate with system administrators in investigations of system abuse.

B. It is a violation of this policy to use the University's information technology resources for transmitting political campaigning, commercial or personal advertisements, solicitations, promotions, or programs, to libel, harass, threaten, or without authorization, invade the privacy or impersonate the identity of other individuals. Offices utilizing applications that send communications on behalf of an employee have the responsibility to ensure the employee is aware of this activity. It is also a violation to use University information technology resources for the purpose of introducing a malicious program into the network, any server or any computer connected to the network. The use of any unauthorized or destructive program may result in legal civil action for damages or other punitive action by any injured party, including the University, as well as criminal action. This policy prohibits both the circumvention of mechanisms which protect private or restricted information, systems, or networks, as well as use of University resources for unauthorized access to private or restricted systems or networks and/or damage to software or hardware components of those systems or networks.

C. Modifying or removing computer equipment, software, or peripherals without proper authorization is a violation of this policy. U3 ((lic)-s)-11 (y)20 (-10 (i)-2 (nf)BTd[U3 ((c)3 (a)4z11
werriwms. (o)-10 (r[illegible]

2. dictionary words

3. personal names

4. computer system names

5. adjacent keyboard combinations such as ‘qwerty’, ‘asdzxc’ or ‘12345’

B. Users may use only their own computer accounts and are personally responsible for all use of their computer account(s). Users who have been authorized to use computing resources (by provision of a user account) may be subject to both criminal and civil liability, as well as University discipline, if the user discloses a password or otherwise makes those resources available to others without the permission of the system administrator.

C. Gaining, or attempting to gain access to the account of another user either by using programs or devices to intercept or decode passwords or similar access control information or by using any other means is prohibited. The negligence or naiveté of another user in revealing an account name or password is not considered authorized use. Convenience of file or printer sharing is not sufficient reason for sharing a computer account. Intentionally allowing or assisting others to gain unauthorized access to information technology resources is prohibited, regardless of whether the computer, software, data, information, or network in question is owned by the University. Abuse of the networks to which the University belongs or the systems at other sites connected to those networks will be treated as an abuse of Oklahoma State University information technology resources privileges.

4.06 System Logging, Reviews, Privacy

A. Users of the University’s information technology resources are placed on notice that all computer systems maintain audit logs and/or file logs within the computer and that user information is backed up periodically. Information collected and stored may include, but is not limited to, user identification, date and time of the session, software used/accessed, files used/accessed, internet use and access, when requested and deemed necessary. The University reserves the right to view or scan any file or software stored on the computer or passing through the network, and will do so periodically to verify that software and hardware are working correctly, to look for particular kinds of data or software (such as computer viruses), or to audit the use of University resources. For example, analysis of audit files may indicate why a particular data file is being erased, when it was erased, and what user identification has erased it.

B. Users should be aware that information transmitted via the Internet may be intercepted by others. Accordingly, the privacy of electronic mail, voicemail and similar data should not be presumed. With regard to all information system data, users should also be aware that the University, as an agency of the State of Oklahoma, and as its officers

and employees, are subject to the provisions of the Oklahoma Open Records Act, 51

and users are warned that they may willingly or unwillingly come across, or be recipients of, material they find offensive. To report material received via email, send a complaint to abuse@okstate.edu or Ethics Point.

C. University Access to User Email

1. Users should be aware that the University, as an agency of the State of Oklahoma, as well as its officers and employees, are subject to the provisions of the Oklahoma Open Records Act. There is no privacy associated with use of University email resources. The University owns, and has right of access to, for any purpose, the contents of all computing information transmitted through or stored on its systems. The University may access and disclose any, or all, of the following:
   a. Data transmitted through or stored on its electronic mail and Internet access systems, regardless of the content of the data,

   b. Information related to the use of electronic communication.

2. If an occasion arises when a University officer or supervisor believes that access to an individual's email account is required for the conduct of University business, the University individual is not available (i.e., death, disability, illness or separation from the University)-1 (-1 ( )](c)4 (c-2 a)4 (t 44 (s)-y)20 (d)-2 (r)3 (a)n(a)4 (t)-2 ((a) frtenrd34 Tvo ((a)4 (t)-e)-6 (s)-S-4 (f)-6 (si (h or) .5 0 V3 (ol)-2 (y)20 (a)-6)P6 35

b.

a.

communication channels often times referred to as Social Media platforms. The term digital media refers to any communications facilitated by technology. This can include online channels, phone/app-based communications and more.

to all or part of the network. Devices not approved for use on the network will be disabled to ensure the stability and availability of the network.

2. For more information on network use, reference the OSU Network Policy at it.okstate.edu/policies.

4.11 Software Licenses and Copyrights

A. Software Licenses