OhioDAS Service · Support · Solutions | Office of Information Technology

State of Ohio IT Policy Use of Internet, E-mail and Other IT Resources	**No:** **ITP-E.8** **Effective:** **03/19/2008** **Issued By:** R. Steve Edmonson Director, Office of Information Technology State Chief Information Officer **Published By:** Statewide IT Policy Investment and Governance Division **Original Publication Date:** 01/01/1996

1.0 Purpose

This state policy establishes controls on the use of state-provided information technology (IT) resources to ensure that they are appropriately used for the purposes for which they were acquired.

2.0 Scope

Pursuant to Ohio IT Policy ITP-A.1, "Authority of the State Chief Information Officer to Establish Policy Regarding the Acquisition and Use of Computer and Telecommunications Products and Services," this state policy applies to every organized body, office, or agency established by the laws of the state for the exercise of any function of state government except for those specifically exempted.

The scope of this information technology policy includes state computer and telecommunications systems and the employees, contractors, temporary personnel and other agents of the state who use and administer such systems.

3.0 Background

The State of Ohio furnishes a variety of ***IT resources*** to employees, contractors, temporary personnel and other agents of the state to conduct the business of the state. These resources include equipment such as desktop and notebook computers, tablet PCs, printers, digital copiers, facsimile machines, personal digital assistants, digital audio and video recorders; applications and services such as software, subscription services, e-mail, ***instant messaging***, and ***Internet*** access; and supplies such as paper, toner, and ink. With such a proliferation of devices, services and software, greater care is required to prevent misappropriation of publicly owned IT resources.

Just as important, the people of Ohio expect their ***public servants*** to devote their time to conduct the state's business and compensate them for that time. In the use of their time and IT resources, public servants must be mindful of the public trust that they

Office of the State CIO | 30 E. Broad Street, 39th Floor | Columbus, Ohio 43215
614.644.6446 | 614.644.9382 | State.CIO@oit.ohio.gov
Robert Blair, Director
Stuart R. Davis, Assistant Director/
State Chief Information Officer

discharge, of the necessity for conducting themselves according to the highest ethical principles, and of avoiding any action that may be viewed as a violation of the public trust. As custodians of resources entrusted to them by the public, public servants must be mindful of how these resources are used.

4.0 References

4.1 Ohio IT Policy ITP-A.1, "Authority of the State Chief Information Officer to Establish Policy Regarding the Acquisition and Use of Computer and Telecommunications Products and Services," defines the authority of the state chief information officer to establish State of Ohio IT policies as they relate to state agencies' acquisition and use of information technology, including, but not limited to, hardware, software, technology services and security.

4.2 Chapter 2909 of the Ohio Revised Code includes companion provisions to this policy with regard to criminal offenses. Section 2909.04 of the Ohio Revised Code specifically addresses knowingly using a computer system, network or the Internet to disrupt or impair a government operation. Section 2909.05 of the Ohio Revised Code specifically addresses causing serious physical harm to property that is owned, leased, or controlled by a government entity.

4.3 Chapter 2913 of the Ohio Revised Code includes companion provisions to this policy with regard to theft and fraud. Section 2913.04 of the Ohio Revised Code specifically addresses accessing without authorization any computer, computer system, or computer network without consent of the owner.

4.4 Chapter 2921 of the Ohio Revised Code includes companion provisions to this policy with regard to offenses against justice and public administration. Section 2921.41 of the Ohio Revised Code specifically addresses using a public office to commit theft which includes fraud and unauthorized use of government computer systems.

4.5 Ohio IT Policy ITP-H.2, "Use of State Telephones," provides requirements regarding the use of both wired and wireless state ***telephone service***.

4.6 A glossary of terms found in this policy is located in section 9.0 - Definitions. The first occurrence of a defined term is in ***bold italics***.

5.0 Policy

Agencies shall establish an Internet, e-mail and IT resources use policy in compliance with this state policy and ensure that public servants adhere to that policy. Agencies shall define and implement such a policy based on the business requirements of the agency. Agency policy shall describe the extent to which personal use is allowed. Agencies may adopt or endorse this state policy as agency policy or may further restrict the duration, frequency and nature of personal use.

5.1 Use of State-Provided IT Resources. The State of Ohio provides computers, services, software, supplies and other IT resources to employees, contractors,

temporary personnel and other agents of the state for supporting the work and conducting the affairs of Ohio government. Personal use, if permitted by an agency, shall be strictly limited and can be restricted or revoked at an agency's discretion at any time.

5.1.1 Use of State-Provided Telephones and Services. Restrictions on the use of IT resources outlined in this policy apply to wired and wireless telephone devices and services, including facsimile machines connected to the state's telephone service. Additional restrictions on the use of state telephones and services are covered by Ohio IT Policy ITP-H.2, "Use of State Telephones."

5.1.2 Use for Collective Bargaining Purposes. In addition to this state policy, collective bargaining contract provisions control the use of state-provided IT resources for contract enforcement, interpretation and grievance processing.

5.2 Unacceptable Personal Use. Any personal use of IT resources that disrupts or interferes with government business, incurs an undue cost to the state, could potentially embarrass or harm the state, or has the appearance of impropriety is strictly prohibited. Personal use that is strictly prohibited includes, but is not limited to, the following:

5.2.1 Violation of Law. Violating or supporting and encouraging the violation of local, state or federal law is strictly prohibited.

5.2.2 Illegal Copying. Downloading, duplicating, disseminating, printing or otherwise using copyrighted materials, such as software, texts, music and graphics, in violation of copyright laws is strictly prohibited.

5.2.3 Operating a Business. Operating a business, directly or indirectly, for personal gain is strictly prohibited.

5.2.4 Accessing Personals Services. Accessing or participating in any type of personals ads or services, such as or similar to dating services, matchmaking services, companion finding services, pen pal services, escort services, or personals ads is strictly prohibited.

5.2.5 Accessing Sexually Explicit Material. Downloading, displaying, transmitting, duplicating, storing or printing sexually explicit material is strictly prohibited.

5.2.6 Harassment. Downloading, displaying, transmitting, duplicating, storing or printing material that is offensive, obscene, threatening or harassing is strictly prohibited.

5.2.7 Gambling or Wagering. Organizing, wagering on, participating in or observing any type of gambling event or activity is strictly prohibited.

5.2.8 Mass E-mailing. Sending unsolicited e-mails or facsimiles in bulk or forwarding electronic chain letters in bulk to recipients inside or outside of the state environment is strictly prohibited.

5.2.9 Solicitation. Except for agency-approved efforts, soliciting for money or support on behalf of charities, religious entities or political causes is strictly prohibited.

5.3 Participation in Online Communities. Any use of state-provided IT resources to operate, participate in, or contribute to an online community including, but not limited to, ***online forums***, ***chat rooms***, ***instant messaging***, ***listservs***, ***blogs***, ***wikis***, ***peer-to-peer file sharing***, and ***social networks***, is strictly prohibited unless organized or approved by the agency. If an individual is approved to participate in any of these forms of communication as part of state business, that person shall fulfill agency-defined security education and awareness requirements for proper use before participating. The content of the education and awareness requirements shall include methods to avoid inadvertent disclosure of sensitive information and practices to avoid that could harm the security of state computer systems and networks.

5.4 Unauthorized Installation or Use of Software. Installing or using software including, but not limited to, instant messaging clients and peer-to-peer file sharing software, or personally owned software, without proper agency approval is strictly prohibited. Installation and use of unlicensed software is strictly prohibited.

5.5 Unauthorized Installation or Use of Hardware. Installing, attaching, or physically or wirelessly connecting any kind of hardware device to any state-provided IT resource, including computers and network services, without prior authorization is strictly prohibited. Connecting or attempting to connect a ***wireless*** device to the state's wireless service without proper agency approval is strictly prohibited.

5.6 No Expectation of Privacy. This policy serves as notice to public servants that they shall have no reasonable expectation of privacy in conjunction with their use of state-provided IT resources. Contents of state computers may be subject to review, investigation and public disclosure. Access and use of the Internet, including communication by e-mail and instant messaging and the content thereof, are not confidential, except in certain limited cases recognized by state or federal law. The state reserves the right to view any files and electronic communications on state computers, monitor and log all electronic activities, and report findings to appropriate supervisors and authorities.

5.6.1 Impeding Access. Impeding the state's ability to access, inspect and monitor IT resources is strictly prohibited. A public servant shall not encrypt or conceal the contents of any file or electronic communication on state computers without proper authorization. A public servant shall not set or manipulate a password on any state computer, program, file or electronic communication without proper authorization.

5.7 Misrepresentation. Concealing or misrepresenting one's name or affiliation to mask unauthorized, fraudulent, irresponsible or offensive behavior in electronic communications is strictly prohibited.

5.8 Restrictions on the Use of State E-mail Addresses. Public servants shall avoid the appearance of impropriety and avoid the appearance of leveraging the stature of the state in the use of their assigned state e-mail address. State e-mail addresses, such as "firstname.lastname@ohio.gov" or "firstname.lastname@agency.state.oh.us," shall not be used for personal communication in public forums such as, or similar to, listservs, discussion boards, discussion threads, comment forums, or blogs.

5.9 Violations of Systems Security Measures. Any use of state-provided IT resources that interferes with or compromises the security or operations of any computer system, or compromises public trust, is strictly prohibited.

5.9.1 ***Confidentiality*** Procedures. Using IT resources to violate or attempt to circumvent confidentiality procedures is strictly prohibited.

5.9.2 Accessing or Disseminating Confidential Information. Accessing or disseminating confidential information or information about another person without authorization is strictly prohibited.

5.9.3 Accessing Systems without Authorization. Accessing networks, files or systems or an account of another person without proper authorization is strictly prohibited. Public servants are individually responsible for safeguarding their passwords.

5.9.4 Distributing ***Malicious Code***. Distributing malicious code or circumventing malicious code security is strictly prohibited.

5.10 Penalties. Violation of this policy may result in disciplinary action or contractual penalties, and may be cause for termination. In addition, public servants may be subject to a civil action or criminal prosecution as a result of inappropriate use or misuse of IT resources. The Ohio Revised Code (ORC) makes certain misuses of IT resources criminal offenses:

- ORC Section 2909.04 – knowingly using a computer system, network or the Internet to disrupt or impair a government operation.
- ORC Section 2909.05 – causing serious physical harm to property that is owned, leased, or controlled by a government entity.
- ORC Section 2913.04 – accessing without authorization any computer, computer system, or computer network without consent of the owner.
- ORC Section 2921.41 – using a public office to commit theft which includes fraud and unauthorized use of government computer systems.

5.11 Compliance. Agencies shall undertake measures to ensure that public servants adhere to agency policy.

5.11.1 Education and Awareness. Agencies shall ensure that restrictions and controls on personal use of IT resources are addressed by education and awareness programs. Public servants shall be made aware of their respective agency's use policy, this state policy, applicable local, state and federal laws, and any applicable collective bargaining agreement provisions. Agencies shall provide employees, contractors, temporary

personnel and other agents of the state under their employ a copy of the agency's Internet, e-mail and IT resources use policy.

5.12 State Registry. The Ohio Office of Information Technology Investment and Governance Division Statewide IT Policy Program Area ("Statewide IT Policy") shall maintain a registry of the Internet, e-mail and IT resources use policies of state agencies.

5.12.1 Statewide IT Policy shall establish a procedure for the submission of agency Internet, e-mail and IT resources use policies and shall instruct agencies as to the requirements of the procedure. Agencies shall be notified of any relevant changes in the procedure.

5.12.2 Upon request, Statewide IT Policy shall make the registry available for inspection in a timely manner to any interested party.

6.0 Procedures

6.1 Agencies shall submit a copy of their Internet, e-mail and IT resources use policy to the Office of Information Technology, Statewide IT Policy.

6.1.1 If at any time an agency should make a change of substance in their Internet, e-mail and IT resource use policy, a copy of the revised policy shall be submitted to Statewide IT Policy.

6.1.2 Copies of policies shall be submitted using one of the following forms and methods.

- For hardcopy documents or for documents in .pdf or .doc formats on optical media, submit via interagency mail to OIT, Statewide IT Policy, 30 East Broad Street, 39th Floor
- For facsimile transmission, submit to OIT, Statewide IT Policy at (614) 644-9152
- For documents in .pdf or .doc formats, submit as e-mail attachments to State.ITPolicy.Manager@oit.ohio.gov
- For documents posted to an externally available Web site not requiring authentication, submit the applicable URL via e-mail to State.ITPolicy.Manager@oit.ohio.gov

7.0 Implementation

The requirements of this policy are anticipated to already be established and in practice. The policy has not been substantively revised since March of 2008.

8.0 Revision History

Date	Description of Change
01/01/1996	Ohio IT Policy OPP-008 replaces PB-002 and all previously released memoranda regarding this topic.

Date	Description of Change
03/20/2006	Revise policy requirements on acceptable and unacceptable personal use of IT resources by public servants.
03/19/2008	Policy requirements concerning participation in online communities were moved from ITP-B.6, "Internet Security," into section 5.3 of this policy.
04/18/2011	References to Ohio IT Policies ITP-B.3, "Password and PIN Security," and ITP-B.4, "Malicious Code Security," were removed from the policy. These policies were rescinded due to the publication of Ohio IT Standard ITS-SEC-02, "Enterprise Security Controls Framework."
03/19/2012	Scheduled policy review.

9.0 Definitions

9.1 Blog. Web-based content consisting primarily of periodic articles or essays listed with the latest entry and visitor comments at the top. Blog topics can range from personal diaries to political issues, media programs and industry analysis. Blogs are also known as "Weblogs" or "Web logs."

9.2 Chat Room. An online forum where people can broadcast messages to people connected to the same forum in real time. Sometimes, these forums support audio and video communications, allowing people to converse and to see each other.

9.3 Confidentiality. The assurance that information is disclosed only to those systems or persons who are intended to receive the information. Areas in which confidentiality may be important include nonpublic customer information, patient records, information about a pending criminal case, or infrastructure specifications. Information systems that must ensure confidentiality will likely deploy techniques such as passwords, and could include encryption.

9.4 Instant Messaging. A software tool that allows real-time electronic messaging or chatting. Instant messaging services use "presence awareness," indicating whether people on one's list of contacts are currently online and available to chat. Examples of instant messaging services are AOL Instant Messenger, Yahoo! Messenger and MSN Messenger.

9.5 Internet. A worldwide system of computer networks — a network of networks — in which computer users can get information and access services from other computers. The Internet is generally considered to be public, untrusted and outside the boundary of the state of Ohio enterprise network.

9.6 IT Resources. Any information technology resource, such as computer hardware and software, IT services, telecommunications equipment and services, digital devices such as digital copiers and facsimile machines, supplies and the Internet, made available to public servants in the course of conducting state government business in support of agency mission and goals.

9.7 Listserv. An electronic mailing list software application that was originally developed in the 1980s and is also known as "discussion lists." A listserv

subscriber uses the listserv to send messages to all the other subscribers, who may answer in similar fashion.

9.8 Malicious Code. Collective term for program code or data that is intentionally included in or inserted into an information system for unauthorized purposes without the knowledge of the user. Examples include viruses, logic bombs, Trojan horses and worms.

9.9 Online Forum. A Web application where people post messages on specific topics. Forums are also known as Web forums, message boards, discussion boards and discussion groups. They were predated by newsgroups and bulletin boards in the 1980s and 1990s.

9.10 Peer-to-Peer (P2P) File-Sharing. Directly sharing content like audio, video, data, software or anything in digital format between any two computers connected to the network without the need for a central server. Examples of P2P networks are Kazaa, OpenNap, Grokster, Gnutella, eDonkey and Freenet.

9.11 Public Servant. Any employee of the state, whether in a temporary or permanent capacity, and any other person performing a government function, including, but not limited to, a consultant, contractor, advisor or a member of a temporary commission.

9.12 Social Networks. Web sites promoting a “circle of friends” or “virtual communities” where participants are connected based on various social commonalities such as familial bonds, hobbies or dating interests. Examples include eHarmony, Facebook, Friendster, LinkedIn, Match.com, MySpace, Plaxo and Yahoo!Groups.

9.13 Telephone Service. Unless otherwise stated, telephone service includes both wired telephones and wireless telephones.

9.14 Wiki. A Web application that allows one user to add content and any other user to edit the content. The popular software used to implement this type of Web collaboration is known as “Wiki.” A well-known implementation is Wikipedia, an online encyclopedia.

9.15 Wireless. Use of various electromagnetic spectrum frequencies, such as radio and infrared, to communicate services, such as data and voice, without relying on a hardwired connection, such as twisted pair, coaxial or fiber optic cable.

10.0 Related Resources

None.

11.0 Inquiries

Direct inquiries about this policy to:

Enterprise IT Architecture & Policy
Investment and Governance Division
Ohio Office of Information Technology
30 East Broad Street, 39th Floor
Columbus, Ohio 43215

Telephone: 614-644-9352
Facsimile: 614-644-9152
E-mail: State.ITPolicy.Manager@oit.ohio.gov

Ohio IT Policy can be found on the Internet at: www.ohio.gov/itp.

12.0 Attachments

None.