



**Ohio Office of Information Technology**  
 Bob Taft, *Governor*  
 Mary F. Carroll, *Director / State Chief Information Officer*

Statewide IT Policy 614.644.9352 tel  
 Investment and Governance Division 614.644.9152 fax  
 30 East Broad Street, 39<sup>th</sup> Floor www.ohio.gov/itp  
 Columbus, Ohio 43215

<p><b>State of Ohio IT Policy</b>          Use of Internet, E-mail and Other IT          Resources</p>	<b>No:</b> <b>ITP-E.8</b>
	<b>Effective:</b> <b>03/20/2006</b>
	<b>Issued By:</b> Mary F. Carroll Director, Office of Information Technology State Chief Information Officer <b>Published By:</b> Statewide IT Policy Investment and Governance Division

### 1.0 Purpose

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

### 2.0 Scope

Pursuant to Section 125.18 of the Ohio Revised Code, 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, other than any state-supported institution of higher education, the office of the auditor of state, treasurer of state, secretary of state, or attorney general, the public employees retirement system, the Ohio police and fire pension fund, the state teachers retirement system, the school employees retirement system, the state highway patrol retirement system, the general assembly or any legislative agency, or the courts or any judicial agency.

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 in order 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; software, subscription services, e-mail, instant messaging, and Internet; 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 compensates them for that time. In the use of their time and IT resources, public servants must be mindful of the public trust that they 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 Section 125.18 of the Ohio Revised Code establishes the authority of the director of the office of information technology to promulgate policies and standards for the acquisition and use of information technology by state agencies.
- 4.2 This policy replaces all previously released memoranda and specifically obsoletes Ohio IT Policy ITP-E.8, "Limitations on the Use of Publicly Owned Hardware and Software," which had an effective date of January 1, 1996.
- 4.3 Ohio IT Policy ITP-H.2, "Use of State Telephones," provides requirements regarding use of both wired and wireless state telephone service.
- 4.4 Ohio IT Policy ITP-B.6, "Internet Security," requires state agencies to implement and operate security protection for Internet, extranet and intranet use.
- 4.5 Ohio IT Policy ITP-B.3, "Password and PIN Security," establishes minimum requirements regarding the proper selection, use and management of passwords and personal identification numbers (PINs).
- 4.6 Ohio IT Policy ITP-B.4, "Malicious Code Security," requires state agencies to implement and operate a malicious code security program to ensure that adequate protective measures are in place against introduction of malicious code.
- 4.7 A glossary of terms found in this policy is located in Section 8.0 - Definitions. The first occurrence of a defined term is in ***bold italic***.

#### 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 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, listservs, blogs, wikis, peer-to-peer file sharing, and social networks**, is strictly prohibited unless organized or approved by the agency.
- 5.3.1 Internet Security. A public servant participating in an online community organized or approved by the agency shall adhere to the security requirements as outlined in Ohio IT Policy ITP-B.6, "Internet Security."
- 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 communications 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 communications 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 in accordance with Ohio IT Policy ITP-B.3, "Password and PIN Security."
- 5.9.4 Distributing Malicious Code. Distributing malicious code or circumventing malicious code security is strictly prohibited. Ohio IT Policy ITP-B.4, "Malicious Code Security," outlines requirements for protecting IT resources against threats from malicious code.
- 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 their 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 to 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 establish an Internet, e-mail and IT resources use policy in compliance with this state policy.

6.2 Agencies shall provide their employees, contractors, temporary personnel and other agents of the state under their employ a copy of their agency use policy.

6.3 Agencies shall incorporate their agency use policy into new employee and new contractor orientation procedures, and any other policy education and awareness efforts they may have.

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

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

6.4.2 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 inter agency mail to OIT Statewide IT Policy, 30 East Broad Street, 39<sup>th</sup> Floor
- For facsimile transmission, submit to OIT Statewide IT Policy at (614) 644-9152
- For documents in .pdf or .doc formats, submit as email attachments to [State.ITPolicy.Manager@oit.ohio.gov](mailto:State.ITPolicy.Manager@oit.ohio.gov)
- For documents posted to an externally available website not requiring authentication, submit the applicable URL via email to [State.ITPolicy.Manager@oit.ohio.gov](mailto:State.ITPolicy.Manager@oit.ohio.gov)

## 7.0 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.
09/26/2001	Ohio IT Policy ITP-E.8, "Limitations on the Use of the Internet, E-mail and Publicly Owned Computer Hardware and Software," supersedes OPP-008.
07/11/2003	Remove references to DAS Directive 01-25, which was rescinded on July 20, 2003.
03/20/2006	Revise policy requirements on acceptable and unacceptable personal use of IT resources by public servants.
03/20/2008	Scheduled policy review.

## 8.0 Definitions

- 8.1 Blog. Web-based content consisting primarily of periodic articles or essays listed with the latest entry and visitor comments at the top. Blogs topics can range from personal diaries to political issues, media programs and industry analysis. Blogs are also known as "weblogs" or "web logs."
- 8.2 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 chat in audio and watch each other.
- 8.3 Instant Messaging (IM). 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 IM services are AOL Instant Messenger, Yahoo! Messenger and MSN Messenger.
- 8.4 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.
- 8.5 Listserv. An electronic mailing list software application that was originally developed in the 1980s and 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.
- 8.6 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.

- 8.7 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.
- 8.8 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.
- 8.9 Social Networks. Websites promoting a “circle of friends” or “virtual communities” where participants are connected based on various social familiarities such as familial bonds, hobbies or dating interests. Examples include eHarmony, Facebook, Friendster, LinkedIn, Match.com, MySpace, Plaxo and Yahoo!Groups.
- 8.10 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.

## 9.0 Related Resources

None.

## 10.0 Inquiries

Direct inquiries about this policy to:

Statewide IT Policy  
Investment and Governance Division  
Ohio Office of Information Technology  
30 East Broad Street, 39<sup>th</sup> Floor  
Columbus, Ohio 43215

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

Ohio IT Policy may be found on the Internet at: [www.ohio.gov/itp](http://www.ohio.gov/itp).

## 11.0 Attachments

None.