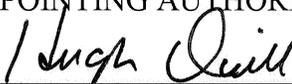


INFORMATION TECHNOLOGY RESOURCE USAGE

POLICY NUMBER: 700-01	EFFECTIVE DATE: 7/7/2008	APPOINTING AUTHORITY APPROVAL: 
REPLACES DAS POLICY DATED: 8/21/06 REPLACES OIT POLICY DATED: 6/29/07	AUTHORITY: Ohio IT Policy ITP-E.8, "Use of Internet, E-mail and Other IT Resources" (3/19/2008)	

1.0 PURPOSE

The purpose of this policy is to minimize the risks and maximize the benefits of using information technology (IT) resources and to maintain the integrity and stability of computer and network hardware, software, data, and related services within the Department of Administrative Services (DAS). This policy addresses permitted and prohibited use of IT resources in the DAS workplace and/or for DAS business.

2.0 SCOPE

This policy applies to IT resources, whether state-owned or privately-owned but authorized for state business use, used by employees, contractors, temporary personnel, and other agents of the state for DAS business or used within the DAS work environment. This policy does not apply to external DAS customers.

3.0 BACKGROUND

Ohio IT Policy ITP-E.8, "Use of Internet, E-mail and Other IT Resources," Section 3.0, states the following:

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.

DAS' policy on Information Technology Resource Usage has been created to comply with **Ohio IT Policy ITP-E.8, "Use of Internet, E-mail and Other IT Resources"** and to reduce the risks associated with the use and misuse of IT resources.

4.0 REFERENCES

4.1 DAS Policy 100-02, "Work Rules"

4.2 Ohio IT Policy ITP-E.8, "Use of Internet, E-mail and Other IT Resources"

4.3 Exchange/Outlook Mail Services Customer Guide - Available at

<http://www.oit.ohio.gov/SDD/TechServ/Exchange/Docs/MicrosoftExchangeServicesGeneral%20PoliciesFinal%201.4.pdf>

4.4 Public Records Transfer Certification form –Available in the DAS Agency-wide Safety/Security Action Plan (ASAP)

5.0 POLICY

DAS provides IT resources to employees, contractors, temporary personnel and other agents of the state to support the work and conduct the affairs of Ohio government. Users of DAS IT resources hold positions of trust both in preserving the security and confidentiality of state information and in safeguarding IT resources. Security, confidentiality, and the safeguarding of IT resources are the responsibility of all DAS IT resource users. Known violations of this policy must be reported to management immediately.

5.1 Use of IT Resources

5.1.1 Ownership and Privacy

All data, text, images, or other information created, stored, transmitted, received, or archived using DAS' IT resources belong to DAS, except for those items whose ownership is protected by law, contract, license agreement, copyright, or other agreement. All data stored or transmitted on a DAS IT resource may be subject to public disclosure and is considered a public record.

When using DAS' IT resources, the user shall have no expectation of privacy. 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.

DAS reserves the right to monitor, access, and disclose all information generated and actions performed using DAS' IT resources. Files, messages (including attachments), and logs may be retained and used as evidence in litigation, audits, and investigations. The user is responsible for all activity originating from his or her username/account and equipment, unless it can be shown that the activity was the result of theft or fraudulent use by another person.

Damage, failure, or loss of any IT resources shall be reported immediately to management. For IT resources supported or managed by DAS IT Services, damage, failure, or loss shall also be reported immediately to the DAS IT Administrator.

DAS employees and contractors shall return DAS supplied IT resources upon separation from DAS employment or termination of the contract.

5.1.2 Personal Use of IT Resources

DAS IT resources are provided for business use. However, incidental personal use of IT resources is allowed if the usage does not have an adverse impact on job performance, IT resources, or DAS business. Management may further restrict personal use of IT resources where appropriate.

The user is responsible for understanding how his/her personal use may impact IT resources and DAS business activities and for complying with all applicable laws, policies, rules, and license agreements. DAS is under no obligation to provide support for the personal use of DAS' IT resources.

5.1.3 System, Network, and Data Security

Users of DAS IT resources shall comply with all applicable policies, procedures, and standards related to the security of those resources.

Whenever users of desktop or laptop computers leave their work areas, they shall use one or more of the following methods to prevent unauthorized access to their computers, software, and/or data:

- Log off all accounts, including their computer and/or network user account.
- Lock their computers by using an approved password protected screensaver.
- Lock their computers by using operating system level workstation locking.
- Shut their computers down.
- Use an alternative method of preventing unauthorized access approved by management. For IT resources supported or managed by DAS IT Services, the alternative method must also be approved by the DAS IT Administrator.

All files shall be stored on network file servers to facilitate back-up. Files maintained on the drives of desktop or laptop computers or on other mobile devices will not be centrally backed-up.

Data may not be removed from state premises without management authorization and provided that the data has been encrypted or is not classified as sensitive.

Devices shall not be connected to DAS networks without appropriate authorization and compliance with all applicable policies, procedures, and standards.

Except for devices that are inherently mobile, such as laptops and personal digital assistants (PDAs), IT equipment may be physically relocated only with appropriate authorization and in accordance with DAS procedures. For IT resources supported or managed by DAS IT Services, requests to move IT resources will be made via the IT Service Request System, and the IT resources will be moved by DAS IT Services staff.

Disposal of IT resources shall be accomplished in accordance with Ohio policies and DAS policies and procedures.

5.2 Unacceptable Use of IT Resources

Any use of IT resources, whether state-owned or privately-owned but authorized for state business use, that disrupts or interferes with DAS business, incurs an undue cost to the State, could potentially embarrass or harm the State, or has the appearance of impropriety is strictly prohibited.

5.2.1 Prohibited Use

Use that is strictly prohibited includes, but is not limited to, the following:

1. Violation of Law. Violating or supporting and encouraging the violation of local, state, or federal law is strictly prohibited.
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.
3. Operating a Business. Operating a business, directly or indirectly, for personal gain is strictly prohibited.
4. Accessing Personal Services. Accessing or participating in any type of personal advertisements or services, such as or similar to dating services, matchmaking services, companion finding services, pen pal services, escort services, or personal advertisements is strictly prohibited.
5. Accessing Sexually Explicit Material. Downloading, displaying, transmitting, duplicating, storing or printing sexually explicit material is strictly prohibited.
6. Harassment. Downloading, displaying, transmitting, duplicating, storing or printing material that is offensive, obscene, threatening or harassing is strictly prohibited.
7. Gambling or Wagering. Organizing, wagering on, participating in or observing any type of gambling event or activity is strictly prohibited.
8. Unlicensed Software. Installation and use of unlicensed software are strictly prohibited.
9. Impeding Access. Impeding the state's ability to access, inspect and monitor IT resources (e.g., inappropriately encrypting or concealing the contents of files or electronic communications, inappropriately setting or manipulating passwords, physically concealing devices) is strictly prohibited.
10. Misrepresentation. Concealing or misrepresenting one's name or affiliation to mask unauthorized, illegal, fraudulent, irresponsible or offensive behavior using IT resources is strictly prohibited. Individuals or entities shall not attempt to intentionally impersonate a third party or mislead another individual or entity into believing that an electronic communication was sent by another party. DAS employees are encouraged to verify the authenticity of the other party with whom they are communicating in order to avoid impersonation and misrepresentation by, or of, the other party.
11. Accessing or Disseminating Confidential or Sensitive Information. DAS employees shall not use IT resources to disclose or provide unauthorized access to sensitive data, confidential records and information. DAS employees shall comply with applicable rules and procedures before disclosing or providing access to public information.
12. Passwords. DAS employees, contractors, vendors, and agents with user access privileges to state IT resources shall not inappropriately disclose their passwords.

13. Distributing Malicious Code. Knowingly distributing malicious code, viruses, worms, corrupting data or software or circumventing malicious code security is strictly prohibited.
14. Peer to Peer File Transfers. The personal use of peer to peer file transfer from non-state computer systems is prohibited.
15. 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.

5.2.2 Use Prohibited without Agency Authorization

Use that is prohibited without proper authorization includes, but is not limited to, the following:

1. Solicitation. Except for agency approved efforts, soliciting for money or support, for example on behalf of charities, religious entities or political causes is strictly prohibited.
2. 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 management.
3. Unauthorized Installation or Use of Software. Installing or using software without proper agency approval is strictly prohibited. (See also Sections 5.3.3.2 and 5.3.4 of this policy.)
4. Unauthorized Installation or Use of Hardware. Installing, attaching, or connecting devices to DAS systems or networks without proper authorization is strictly prohibited.
5. Data Transport. When authorized by management, state-owned, encrypted removable media (such as a USB memory stick, CD, or DVD) may be used to transport state data from one location to another, if the data is not classified as sensitive.
6. Accessing Systems without Authorization. Accessing networks, files or systems or an account of another person without proper authorization is strictly prohibited.
7. Privately-owned IT Resource Usage. Privately-owned IT resources, including private web-based e-mail accounts (e.g., AOL, Google, Yahoo, or MSN), shall not be used to conduct DAS business unless authorized by management. DAS is under no obligation to provide support for privately-owned IT resources. (See also Section 5.3.1 of this policy.)

5.3 Electronic Communications

5.3.1 Public Records and Records Retention

Depending upon their purpose or content, electronic communications and attachments may be public records and/or subject to records retention requirements specified by policy, rule, or law. The purpose or content of an electronic communication determines if it is a public record, not the account, device, or method used to create or transmit the communication. See Sections 5.2.2 and 5.3.3.2 of this policy regarding restrictions on the use of private web-based e-mail accounts.

When using DAS IT resources for electronic communications, users are responsible for ascertaining and complying with the public records and/or records retention requirements associated with their messages and attachments. Management shall review public records and records retention requirements associated with electronic communications with each newly hired

permanent or temporary DAS employee and with vendors, contractors, and other agents of DAS prior to allowing them to access DAS IT resources.

DAS employees and contractors shall review their files and messages (including attachments) upon separation from DAS employment or termination of the contract. They shall then transfer all public records to a designated representative of management and complete the Public Records Transfer Certification form.

5.3.2 Professionalism

DAS employees shall use professional and appropriate language in all electronic communications. Sending abusive, harassing, threatening, menacing, discriminatory, pornographic, disrespectful, or otherwise offensive or embarrassing electronic communications is prohibited.

5.3.3 Electronic Mail (E-mail)

5.3.3.1 Use of DAS' E-mail System

DAS' e-mail system is currently based upon Microsoft Exchange mail using Microsoft Outlook client software. E-mail accounts are provided by the DAS/OIT/ISD Exchange/Outlook Mail Services group.

Policies, procedures, and standards applicable to the use of Exchange/Outlook Mail Services are published in the Exchange/Outlook Mail Services Customer Guide. The user of a DAS e-mail account must abide by these policies, procedures, and standards as a condition of receiving access to the DAS e-mail system. Other statewide or DAS policies may also apply. Compliance is the user's responsibility.

DAS employees 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 shall not be used for personal communications in public forums such as or similar to listservs, discussion boards, discussion threads, comment forums, or blogs.

5.3.3.2 Use of Personal, Consumer-Grade E-mail Systems

Downloading, installing, and/or using personal, consumer-grade e-mail client software (e.g., AOL, Google, Yahoo, or MSN) to conduct DAS business via the public Internet or for personal use involving DAS' IT resources is prohibited. If there is a business need for e-mail usage, the potential user may request access to DAS' e-mail system. When authorized by management, using an external e-mail account for transmission/connectivity testing purposes is an exception to this provision.

Some e-mail providers allow access to personal e-mail directly via an Internet browser interface. Using such e-mail systems for personal use in the DAS workplace may be allowed if the usage does not have an adverse impact on job performance or IT resources. The user is responsible for understanding how the personal e-mail system they are using functions and for compliance with this policy.

When using DAS' IT resources to access personal e-mail, messages may be opened, read, and forwarded to a DAS provided e-mail address. However, opening attached files or executing attached software from personal e-mail is strictly prohibited. Transfer of files or software from the personal e-mail provider's servers to a DAS device, system, or network is also strictly prohibited.

Private web-based e-mail accounts (e.g., AOL, Google, Yahoo, or MSN), shall not be used to conduct DAS business. In certain management approved circumstances use of a private web-based e-mail account for DAS business may be acceptable. An example of such type of use may be to access information regarding professional association benefits (i.e. registered architects, licensed attorneys, etc.)

5.3.4 Instant Messaging (IM)

DAS currently has no standard or supported IM system available. If such a system becomes available in the future, this policy will be revised.

Downloading, installing, and/or using personal, consumer-grade instant messaging client software (e.g., AOL, Google, Yahoo, or MSN) is strictly prohibited.

6.0 PROCEDURES

Procedures shall be developed at various levels within the DAS organization in order to effectively and efficiently implement this policy.

At a minimum:

- This policy shall be distributed to each newly hired DAS employee during orientation, in conjunction with other applicable policies and procedures, and the new employee shall sign an acknowledgement of receipt of this policy.
- Vendors, contractors, and temporary employees shall receive a copy of and sign an acknowledgement of receipt of this policy prior to gaining access to IT resources.
- Management shall include this policy when reviewing the DAS Agency-wide Safety/Security Action Plan (ASAP) with employees.

7.0 COMPLIANCE

It is the responsibility of management to implement and ensure compliance with the laws, rules, policies, procedures, standards, and license agreements applicable to the use of IT resources within their functional areas.

It is the responsibility of the user of IT resources to ascertain, understand, and comply with the laws, rules, policies, procedures, standards, and license agreements applicable to their use of those resources.

7.1 Consequences of Violation of Policy

Violation of this policy by any user of IT resources may result in loss of access to those resources.

Any DAS employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. In addition, employees may be subject to civil action or criminal prosecution as a result of inappropriate use or misuse of IT resources.

Any contractor, vendor, or other agent of the state performing work for or on behalf of DAS found to have violated this policy may be subject to consequences specified in the contract or other agreement governing their engagement by DAS, up to and including termination of the contract. In addition, contractors may be subject to civil action or criminal prosecution as a result of inappropriate use or misuse of IT resources.

8.0 DEFINITIONS

DAS – Department of Administrative Services.

DAS Contractors – For the purposes of this policy, DAS contractors are defined as contracted staff and vendor technicians.

DAS Employees – For the purposes of this policy, DAS employees are defined as all employees and representatives of DAS, whether they are permanent staff or temporary staff.

DAS-owned – Purchased with DAS funds or otherwise acquired by DAS; property of DAS.

DAS-provided or **DAS-supplied** – Made available to users by DAS.

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.

IT Resources – Any information technology resources, such as computer hardware and software, IT services, telecommunications equipment and services, networks, digital devices such as digital copiers and facsimile machines, supplies, and the Internet.

Management – Management refers to supervisory staff responsible for the completion of activities to fulfill DAS’ mission. If Position A is shown as subordinate to Position B on the Table of Organization, then Position B is supervisory in nature for the purposes of this policy.

OIT – Office of Information Technology.

Peer to Peer – Direct connection between computer systems or devices, usually for the purpose of content sharing or communication.

Personal Information – An individual’s last name along with the first name or first initial, in combination with one or more of the following data elements: social security number; driver’s

license number; state identification card number; financial account number; or credit or debit card number.

Privately-owned - Purchased with personal or corporate (vendor or contractor) funds; not provided by the state.

Sensitive Data – Means any electronic information that an agency collects and maintains but must keep confidential as required by law. It also includes “personal information”.

State-owned - Purchased with state funds or otherwise acquired by the state; property of the state of Ohio.

Users - For the purposes of this policy, users are defined as employees, contractors, temporary personnel and other agents of the state who administer or use privately-owned (if authorized) or state-owned IT Resources on behalf of the state.

9.0 INQUIRIES

Direct inquiries about this policy to:

Risk Management Services
Office of Information Technology
Ohio Department of Administrative Services
1320 Arthur E. Adams Drive
Columbus, Ohio 43221

Telephone: 614-995-7632
E-mail: RiskManagementServices@OIT.Ohio.Gov

10.0 REVISION HISTORY

Date	Description
7/7/2008	New policy to reconcile DAS policy dated 8/21/06 and OIT policy dated 6/29/07

11.0 ATTACHMENTS

None.