



<p>State of New Jersey IT Circular</p> <p>Title: Acceptable Internet Usage</p>	NO: 09-07-NJOIT	SUPERSEDES: Policy - 02
	DATE PUBLISHED: 01/30/09	
	VERSION: 01/30/09	EFFECTIVE DATE: IMMEDIATELY
	FOR INFORMATION CONTACT: Elizabeth Caldwell, Office of Policy and Planning (609) 633-0429	

ATTN: Directors of Administration and Agency IT Directors

I. PURPOSE

To establish the overall policy for the use of the State Networks and Internet by State Agency employees and other authorized users. Agencies may supplement this policy as needed or desire, as long as such supplement is consistent with this policy.

II. AUTHORITY

This policy is established under the authority of State of New Jersey P.L.2007.c.56.

The New Jersey Office of Information Technology (NJOIT) reserves the right to change or amend this circular to comply with changes in NJOIT Federal or other agency policies.

III. SCOPE

This policy applies to all Executive branch agency employees and system users whether authorized or unauthorized who access and use the Internet and encompasses all decisions and activities affecting or affected by access or use of the Internet by agency employees and system users whether authorized or unauthorized. The policies set forth in this document are limited and qualified by the Federal Wire Tap Act, 18 U.S.C. §2710 et seq, and the New Jersey Wiretap Act, N.J.S.A 2A:156A-1 et seq.

By accessing the State's network or Internet system a user agrees to adhere to the State's policies, including agency specific policies, regarding their use.

IV. DEFINITIONS

As used in this policy, unless the context clearly requires a different meaning, the following words shall have the meaning indicated:

"Access" means the ability to receive, use, and manipulate data and operate controls included in information technology.

"Agency" means any agency, authority, board, department, division, commission, institution, institution of higher education, bureau, or like governmental entity of the executive branch of the state government.

A **"cache"** (pronounced CASH) is a block of memory dedicated for the temporary storage and high-speed retrieval of frequently used or requested data.

A **"cookie"** is a special text file that a web site puts on the user's hard disk so that it can remember something about the user at a later time. Typically, a cookie records the user's preferences when using a particular site.

"Information infrastructure" means telecommunications, cable, and computer networks and the Internet, including the World Wide Web, E-mail, File Transfer Protocol, Usenet, bulletin board systems, on-line systems, and telephone networks.

"Instant messaging" is a type of communications service that enables a user to create a private chat room with another individual. Typically, the instant messaging system alerts a user whenever somebody on the user's private list is online. A user can then initiate a chat session with that particular individual.

"Information technology" means all electronic information processing hardware and software, including telecommunications.

The **"Internet"** is a worldwide system of interconnected computer networks in which users at any one computer can obtain and exchange information with any other computer connected to the network.

"Malicious software" is software designed to infiltrate or damage a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

"Network" in information technology, a system that transmits any combination of voice, video and/or data between users. The network includes the network operating system in the client and server machines, the cables connecting them and all supporting hardware in between such as bridges, routers and switches. In wireless systems, antennas and towers are also part of the network.

"Path Records" are the combination of history, cache, cookie, e-mail header files that record the Internet pages visited.

"Personal Information" is information about a natural person that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history, readily identifiable to a specific individual.

"Sexually explicit content" means content having as a dominant theme (i) any lascivious description of or (ii) any lascivious picture, photograph, drawing, motion picture film, digital

image or similar visual representation depicting a lewd exhibition of nudity, sexual excitement, or sexual conduct.

"State-provided" means access to the Internet via computer system networks owned, leased or operated by the State of New Jersey. Use of these services may be subject to monitoring for security or network management reasons.

"Streaming media" is streaming video with sound. With media streaming, a web user does not have to wait to download a large file before seeing the video or hearing the sound. Instead the media is sent in a continuous stream and is played as it arrives. Streaming media requires larger amounts of network resources (bandwidth).

"Streaming video" is a sequence of "moving images" that are sent in compressed form over the Internet and displayed by the viewer as they arrive. An example of a streaming video is a stock market ticker. With streaming video, a web user does not have to wait to download a large file before seeing the video. Instead the video is sent in a continuous stream and is played as it arrives. Streaming video requires larger amounts of network resources (bandwidth).

"Telecommunications" means the transmission of information, images, pictures, voice or data by radio, video, or other electronic or impulse means.

V. POLICY

The Internet can provide the State with critical business advantages as a source of research and technical information, improved communication, public access and visibility, business and recruiting contacts and electronic commerce. It is, therefore, in the State of New Jersey's best interest to encourage prudent use of the Internet for State business purposes. The Internet presents employees with opportunities for easy, rapid and efficient global communications and research but also creates certain risks, including security risks and legal liability. In order for the State to maximize the benefits and minimize the risks associated with use of the Internet, this statement sets policy for Internet access and use by all users whether authorized or unauthorized.

The only persons who may access the Internet through the State information infrastructure or information technology are State employees and such other persons as the State may specifically authorize. The authorization should be supported by documentation, which could include, but is not limited to, a signed agreement, a memo or a note to file.

Employees are given State-provided access to the Internet to assist them in the performance of their jobs. The State may monitor Internet activity and therefore users should have no expectation of privacy. All records created by Internet use, including path records, are property of the State and are subject to monitoring. Users are expected to conduct their electronic communications in a professional, responsible and courteous manner. Misuse of the State's information infrastructure, information technology and electronic communications media, including, but not limited to, the unauthorized transmission of confidential or proprietary information; the use of profane, harassing or other offensive language; or other inappropriate uses, including, but, not limited to, those listed below, may subject the user to discipline, including termination of employment, initiation of civil action, or criminal prosecution.

The ability to access the Internet using State-provided software, hardware, information infrastructure, information technology and other facilities is governed by this policy and several existing State policies summarized below. In addition, the following Internet-specific policies must be followed to maintain a secure and hostile free work environment.

All users must follow this policy and any additional policy that may be adopted by the State or agency where the user is working.

This policy supersedes Statewide IT policy number 02 - Internet Usage.

VI. No Privacy Expectations

The State reserves the right to access and disclose, for any purpose, the contents of any Internet messages sent to and from or stored on, the State's computer equipment, information infrastructure or information technology including e-mail, attachments to e-mail, and World Wide Web browsing without prior notice. All users, including State employees, using the Internet waive any right to privacy in such messages, and consent to their being accessed and disclosed by State personnel.

Users of the computers and computer network of the State specifically authorize the State to monitor, intercept, read, copy, or capture in any manner any information transmitted or stored using the State's network and Internet access. The State may disclose or use any information monitored, intercepted, read, copied or captured to authorized personnel or law enforcement to be used for disciplinary or civil action or criminal prosecution.

Nothing in this policy shall be taken to waive, relinquish or abrogate any privilege or confidentiality recognized by law or to authorize disclosure of any privileged, confidential or proprietary information except as provided by law.

VII. State System Security

All employees shall ensure that their use of the Internet does not compromise the security and integrity of State's information infrastructure or information technology, networks and computer equipment, whether by allowing intruders into the networks or by introducing viruses or other threats.

Employees shall not use another employee's computer to gain access to the Internet without that employee's consent or supervisory approval. An employee shall not permit another person to access the Internet using the employee's computer, except as provided by the agency's policy. An agency may establish a specific policy regarding access to the Internet when necessary to carry out the duties and responsibilities of the agency.

VIII. Acceptable Use: Permitted Purposes

Employees are given access to the Internet through the State information infrastructure and information technology to carry out State business. All State policies, including but not limited to the State's policy prohibiting discrimination, harassment or hostile environments in the workplace work-place violence and sexual harassment, the Conflict of Interest Law and the Uniform Code of Ethics (as may be supplemented by an agency code approved by the State Ethic Commission, apply to an employee's access or use of State information

infrastructure and technology. Users must comply with all state and federal laws and regulations applicable to the Internet. Employees must adhere to any conditions or restrictions on Internet access and use set by an agency.

Software for browsing the Internet is provided to users for State related business use only. As with the telephone, limited incidental personal use that does not interfere with work duties, that does not consume significant State resources, that does not constitute a use prohibited by this policy and that does not interfere with the activities of others may be permitted by an agency. Personal use of State equipment shall not amount to more than de minimis, occasional use. More than limited incidental personal use may subject an employee to discipline or removal of Internet access. Incidental personal use of the Internet is subject to monitoring or interception like any other Internet use. Except as otherwise provided by an agency's policy, personal use is permitted only during authorized break times, lunch periods or before or after work hours. No agency is under an obligation to make Internet access available to any employee for personal use.

Note: Users employing the State's Network or Internet for personal use must present their communications in such a way as to be clear that the communication is personal and does not represent the Agency or the State. Employees shall not engage in any communications that may harm the image, reputation and/or goodwill of the State and/or any of its employees.

IX. Examples of Impermissible Uses

The following are examples of impermissible uses of the State information infrastructure or information technology systems. This list is by way of example and is not intended to be exhaustive or exclusive. A user may not:

- Violate or infringe on a recognized privilege or the right to privacy;
- Violate agency or departmental regulations or policies prohibiting discrimination, harassment or hostile environments in the workplace;
- Violate any local, state, or federal law;
- Conduct personal, for profit business activity;
- Solicit for religious, political, charitable or other causes;
- Perform any political campaign activities;
- Conduct any non-governmental related fund raising or public relations activities;
- Perform illegal, unethical, or criminal activities;
- Transmit or download, store, install, or display any kind of image or document on any agency system that violates agency and/or State policies on prohibiting discrimination, harassment or hostile environments in the workplace or workplace violence;
- Download software in violation of licensing agreements or agency policies;

- Transmit or post agency information without management approval;
- Gain or attempt to gain unauthorized access to any computer, computer records, data, databases or electronically stored information;
- Violate licensing, trademark or copyright laws;
- Knowingly cause the transmission of a program, information, code or command, and as a result of such conduct, intentionally causes damage to a computer;
- Gamble or play games on the Internet;
- Engage in instant messaging, streaming media or streaming video for non-work related purposes;
- Transmit defamatory, false, inaccurate, abusive, profane, pornographic, threatening, racially offensive, or otherwise biased, discriminatory or illegal material.
- The use of State equipment or assets by an individual to access, transmit, copy, convey information in violation of an executed agency or department non-disclosure agreement.

Except to the extent required in conjunction with a bona fide, agency approved project or assignment or other agency approved undertaking, no user shall utilize State owned or leased information infrastructure or information technology to access, download, print or store any information infrastructure files or services having sexually explicit content. Such agency approvals shall be given in writing by agency heads or their designees.

Users shall not use a password or transmit encrypted data through the State Internet system unless they make the password, key or other means of decrypting the transmittal available to their supervisor.

X. Monitoring of Site Access and System Use

The State reserves the right to monitor and filter site access by users and to review data downloaded from the Internet. The State may also monitor access to the State information infrastructure and information technology system (including successful and failed login attempts and logouts), inbound and outbound file transfers, and sent and received e-mail messages. The State may monitor, intercept, read, copy, or capture in any manner any information placed on its computers or computer systems. The State may disclose or use any information monitored, intercepted, read, copied, or captured to authorized personnel or law enforcement in any disciplinary or civil action or criminal prosecution.

XI. Software

The agency IT Director must approve all software used to access the Internet.

XII. Virus Scanning

All files downloaded must be scanned for viruses and other malicious software, using virus detection software approved by the agency in consultation with OIT.

XIII. Representing the State

Employees must exercise the same care in posting information to the Internet as they would with any external communication by the agency.

XIV. Proprietary and Confidential Information

Users shall maintain all proprietary and confidential information in confidence and shall not use the Internet or the State information infrastructure or technology to access, disclose or distribute such information in an unauthorized manner or attempt to do so.

XV. Copyright

Users should not violate any of the copyright laws when accessing printing or disseminating materials found on the Internet.

XVI. Consent

Access or use of State-furnished computers or Internet facilities constitutes consent to this policy on Acceptable Use of the Internet.

XVII. Technical

Users should schedule, wherever possible, communications-intensive operations such as large file transfers, video downloads, mass e-mailings and the like for off-peak times.

XVIII. RESPONSIBILITIES

Employee

Employees shall follow this policy and all agency Internet policies and procedures. Users should report any misuse or policy violations to their supervisor or Agency IT Director.

Agency

Agencies may develop agency guidelines, procedures, and internal controls for monitoring compliance that are in accordance with this policy.

All agencies shall immediately furnish their current employees copies of this notice, and shall furnish all new employees copies of this policy concurrent with authorizing them to use agency computers.

Agencies may discipline employees for violations of this policy or any standards or guidelines referenced.

Agencies may promote awareness of acceptable use of the Internet by training employees in the use of tools to access the Internet.

XIX. EXCEPTIONS AND NON-COMPLIANCE

Failure to comply with this policy may result in disciplinary action. A compliance exception must be requested if there is an inability to comply with this policy because of a business reason or system constraint. All requests for a compliance exception shall be made to the Statewide Information Security Officer (SISO) in writing.

XX. REFERENCES

Title 7 of the Civil Rights Act of 1964 as amended

Communications Decency Act of 1996

N.J.S.A. 10:5-1 et. seq.

N.J.S.A. 11A:1-1 et. seq.

N.J.A.C. 4A:7-1.3

Uniform Code of Ethics/New Jersey Conflicts of Interest Law

Executive Order 49 (Issued April 17, 1996 - Governor Whitman)

The Computer Fraud and Abuse Act

Signature on File

ADEL EBEID
Chief Technology Officer

1/30/2009

DATE