

<b>DEPARTMENT OF CORRECTION</b> 	<b>POLICY MANUAL</b>	<b>POLICY NUMBER:</b> 141 v2.0	<b>PAGE NUMBER:</b> 1 of 7
		<b>SUBJECT:</b> Computer, Electronic Mail, and Internet Use	Adopted: 2-02-01 Reviewed: 12-20-01 Revised: 2-26-09

## **01.00.00. POLICY OF THE DEPARTMENT**

It is the policy of the Board of Correction that the Department of Correction shall establish guidelines for the efficient and appropriate use of computers, electronic mail (e-mail), and the Internet by department employees.

## **02.00.00. TABLE OF CONTENTS**

<b>01.00.00.</b>	<b>POLICY OF THE DEPARTMENT</b>
<b>02.00.00.</b>	<b>TABLE OF CONTENTS</b>
<b>03.00.00.</b>	<b>REFERENCES</b>
<b>04.00.00.</b>	<b>DEFINITIONS</b>
<b>05.00.00.</b>	<b>PROCEDURE</b>
05.01.00.	Introduction
05.02.00.	Purpose of Guidelines
05.03.00.	Applicability
05.04.00.	Use of Computers
05.05.00.	Inappropriate Use of Computers
05.05.01.	Unacceptable Uses
05.05.02.	Games
05.05.03.	Wallpaper and Screensavers
05.05.04.	Inappropriate Information and Images
05.06.00.	Hardware and Software
05.07.00.	Internet
05.08.00.	Electronic Mail
05.08.01.	Confidentiality
05.09.00.	Access for Inquiry or Investigation
05.10.00.	Violation of Policy

## **03.00.00. REFERENCES**

Department Policy 108, Public Access to Records.

Executive Order No. 2005-22, Establishing Statewide Policies on Computer, Internet, and Electronic Mail Usage by State Employees.

<b>POLICY NUMBER:</b> 141 v2.0	<b>SUBJECT:</b> Computer, Electronic Mail, and Internet Use	<b>PAGE NUMBER:</b> 2 of 7
-----------------------------------	---	-------------------------------

State of Idaho, Information Technology Resource Management Council (ITRMC) Policy P1040, Employee Electronic Mail and Messaging Use

State of Idaho, Information Technology Resource Management Council (ITRMC) Policy P1050, Employee Internet Use

#### **04.00.00. DEFINITIONS**

Electronic Mail (e-mail). A means or system for transmitting messages electronically (as between terminals linked by telephone lines or microwave relays), or a message sent electronically.

Information Technology (IT). The department bureau that supports the hardware and software needs of the department's statewide computer network.

Internet. An electronic communications network that connects computer networks and organizational computer facilities around the world.

Local Area Network (LAN). A network of personal computers in a small area (as an office) that are linked by cable, can communicate directly with other devices in the network, and can share resources.

Management Authority. The appointed facility or unit manager having the authority and responsibility for the day to day management, control, and responsibility for a designated administrative unit within the Department. This includes the director, division chief, deputy chief, warden, deputy warden, probation and parole district manager, or community work center manager in the employee's chain of command. It also includes a designated acting manager, someone delegated to act on behalf of the manager, or someone temporarily appointed as manager while the manager is on leave or is unavailable.

Wide Area Network (WAN). A network of personal computers in a large area (such as statewide) that are linked by cable, can communicate directly with other devices in the network, and can share resources.

#### **05.00.00. PROCEDURE**

##### **05.01.00. Introduction**

Technology and its applications, including the Internet, continue to expand and to become more accessible. This expansion increases the opportunity for state employees to improve their productivity, effectiveness and efficiency. However, as the

<b>POLICY NUMBER:</b> 141 v2.0	<b>SUBJECT:</b> Computer, Electronic Mail, and Internet Use	<b>PAGE NUMBER:</b> 3 of 7
-----------------------------------	---	-------------------------------

use and accessibility of technology increases, so does the risk that the technology might be used inappropriately or inefficiently.

#### **05.02.00. Purpose of Guidelines**

The Management Team has adopted these guidelines to govern information technology to protect and prevent the abuse of state property, to ensure the continued and effective operation of the Department, including the Local Area Network (LAN) and Wide Area Network (WAN); to promote increased employee productivity; to control software viruses; and to maximize the efficient use of IT staff time.

#### **05.03.00. Applicability**

These policies apply to the usage of all computers, peripherals and software that are connected to or can be connected to the Department LAN and/or WAN.

#### **05.04.00. Use of Computers**

Department of Correction staff are encouraged to use the Internet and electronic mail (e-mail) to further the mission of the Department, to provide service to customers, and to promote professional development.

Computers are for business use only, and staff should not expect their e-mail communications, documents, or other information to be private and should not use the e-mail system for matters that are not intended for public disclosure. Only the occasional personal use of e-mail in lieu of telecommunication is acceptable.

Every employee is responsible for monitoring and prohibiting the misuse of Department property. It is each employee's responsibility to inform senders of inappropriate e-mails of the Department's e-mail policy. Inappropriate use must be reported to management.

#### **05.05.00. Inappropriate Use of Computers**

##### **05.05.01. Unacceptable Uses**

It is unacceptable for department employees to use the facilities and capabilities of the computer system to:

- Conduct any non-approved business;

- Solicit the performance of any activity that is prohibited by law;

<b>POLICY NUMBER:</b> 141 v2.0	<b>SUBJECT:</b> Computer, Electronic Mail, and Internet Use	<b>PAGE NUMBER:</b> 4 of 7
-----------------------------------	---	-------------------------------

Transmit materials, information, images, or software in violation of any local, state, or federal law;

Conduct any political activity;

Conduct any non-department supported fund raising or public relations activities;

Engage in any activity for personal gain or personal business transactions;

Make any unauthorized purchases;

Use any games on state government provided computer equipment;

Place advertisements for commercial enterprises including but not limited to goods, services, or property; and

Abuse electronic mail privileges.

#### **05.05.02. Games**

No games or unapproved applications may be installed on Department computers.

#### **05.05.03. Wallpaper and Screensavers**

The only acceptable wallpaper and screensavers are those provided by the Windows operating system, current department approved office applications, or those approved by Information Technology.

#### **05.05.04. Inappropriate Information and Images**

It is unacceptable to knowingly or intentionally submit, publish, display, transmit, retrieve or store on the department's network or on any department computer system any information or image which:

Violates or infringes on the rights of any other person, including the right to privacy;

Contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive or other biases, discriminatory, or illegal materials;

<b>POLICY NUMBER:</b> 141 v2.0	<b>SUBJECT:</b> Computer, Electronic Mail, and Internet Use	<b>PAGE NUMBER:</b> 5 of 7
-----------------------------------	---	-------------------------------

Violates state government regulations prohibiting sexual harassment;

Restricts or inhibits other users from using the system, or the efficiency of the computer systems;

Encourages the use of controlled substances or uses the system for criminal purpose;

Uses the system for any other illegal purpose; or

Contains statements, which might incite violence or which describe or promote the use of weapons or devices associated with terrorist activities.

#### **05.06.00. Hardware and Software**

Only Information Technology staff members are authorized to approve new hardware/software, acquire, install or remove software applications; and install, remove, or change the configuration of hardware.

#### **05.07.00. Internet**

Users of the Internet are to comply with appropriate laws, regulations and accepted Internet etiquette. Users should identify themselves properly when using the Internet, and conduct themselves as professional representatives of Idaho State government. Each user is individually responsible for the content of any communication sent over or placed on the Internet.

#### **05.08.00. Electronic Mail**

Employees are reminded that electronic mail (e-mail):

Can, and probably will, be copied, saved, or seen by third parties, both internal and external to state government, so care should be given regarding content of the communication;

May be monitored; and

Is subject to disclosure under the Idaho Public Records Act and any other Department policies pertaining to records.

<b>POLICY NUMBER:</b> 141 v2.0	<b>SUBJECT:</b> Computer, Electronic Mail, and Internet Use	<b>PAGE NUMBER:</b> 6 of 7
-----------------------------------	---	-------------------------------

#### **05.08.01. Confidentiality**

Employees who send e-mail messages containing confidential and/or privileged information must include the following statement in the body of the message:

DO NOT read, copy, or disseminate this communication unless you are the intended addressee. This e-mail communication contains confidential and/or privileged information intended only for the addressee. If you have received this communication in error, please call us immediately at 208-658-2000 and ask to speak to the sender. Please e-mail the sender to notify him immediately that you have received the communication in error, and delete message received in error immediately.

Employees who receive a confidential message should delete the message from the e-mail system immediately after a printed copy can be made.

#### **05.09.00. Access for Inquiry or Investigation**

Use of state-owned computers must comply with all federal, state, or local laws and regulations, Executive Orders, or Department policies, procedures, standards, or guidelines. The Department has the right to inspect any and all files stored in secured areas of State networks, on computing devices owned or leased by the State, or on any other storage medium provided by the State for official business (i.e. flash drives, external hard-drives, floppy disks, tapes, CD's, DVD's, and other media) in order to monitor compliance with this policy. Inappropriate use may be investigated by Management Authorities or the Office of Professional Standards.

Basic computer, email and Internet data is available from IT Services to Management Authorities upon approval of their respective Division Chief for the following:

E-Trust Internet surfing history and a blocked sites list for the most recent thirty (30) day time frame. This information will not identify the user, but only the computer used and the date and time of Internet website access of or attempted access.

Daily snapshots for the past year of 'Sent' and 'Received' emails for an employee's email address.

Current Novell Mailbox inspection of contents with an altered password. This requires resetting an employee's password and then notifying the employee to reset it again after the mailbox contents have been inspected.

<b>POLICY NUMBER:</b> 141 v2.0	<b>SUBJECT:</b> Computer, Electronic Mail, and Internet Use	<b>PAGE NUMBER:</b> 7 of 7
-----------------------------------	---	-------------------------------

To request IT Services support, send an email to the Division Chief with a full description of the request. The Division Chief will approve the request by forwarding it to the IT Manager.

Upon approval of their respective Management Authority trained staff members may preview Department computers for the presence of objectionable pictures with issued or approved preview software programs. In a preview, the original hard drive or media is viewed, but not copied, using an approved computer search tool such as the FBI's Image Scan, DHS' Knoppix or Field Search.

Advanced technical computer forensics previews, computer or cellular telephone examinations and real-time information is available, in conjunction with an approved investigation, from the Office of Professional Standards for the following:

Previews for the presence of objectionable pictures or movies on a Department computer.

Detailed methodical examination of the hard drive or media upon submittal of a Department computer to a certified computer forensics laboratory. This also includes extremely comprehensive forensics examinations when looking for difficult-to-find evidence or for specific exculpatory or incriminating evidence.

Access to an employee's Novell Mailbox activity without altering the employee's password.

Access to an employee's GroupWise Messenger historical and real-time activity.

#### **05.10.00. Violation of Policy**

Employees violating this policy are subject to disciplinary action up to and including dismissal.

---

**Director, Department of Correction**

---

**Date**