IPP.10002. Computer and Information Systems Usage

IPPMTL 0282

Revised: August 8, 2014

Original: June 28, 2002

CLICK HERE to acknowledge that you have read, understand, and will comply with this policy.

I. PURPOSE/REASON:

To inform all ODJFS employees, temporary service personnel, and contractors of the proper use of ODJFS electronic equipment and information systems including but not limited to computers, peripherals, software, Internet, GroupWise, e-mail, Short Message Service (SMS) Text Messaging, Portable Computing Devices and Instant Messenger (IM).

II. REFERENCE/AUTHORITY:

A. REFERENCES

*Note: ORC references can be accessed at LAWriter's Ohio Revised Code (**http://codes.ohio.gov/**) website.*

1. ODJFS-**IPP 3922**
2. ODJFS-**IPP 0003**
3. ODJFS-**IPP 9002**
4. ODJFS-**IPP 10003**
5. ODJFS-**IPP 8501**
6. ODJFS-**IPP 3100**
7. House Bill 99 (Ohio distracted driving legislation)
8. Ohio Revised Code **4511.204** [Effective 8/31/2012] (Driving while texting)

B. AUTHORITY

1. This policy is established by order of the Director, ODJFS, hereinafter referred to as Director.
2. Per **ORC 5101.02**, all duties conferred on the various work units of the department by law or by order of the Director shall be performed under such rules as the Director prescribes and shall be under the Director's control.

III. SUPERSEDES:

ODJFS-IPP 10002 revision dated October 15, 2012.

IV. SCOPE:

A. This policy applies to all Ohio Department of Job and Family Services employees, temporary service personnel, or contractors (hereinafter referred to as ODJFS personnel) use of computer and information systems, including but not limited to:

1. electronic equipment-computers, computer peripherals, computer software, and laptops;
2. information systems-documents, recordings, e-mail, Instant Messenger (IM), and the Internet; and
3. other data contained in or recoverable from such electronic equipment and information systems.

B. This applies to any equipment either provided by ODJFS or used on ODJFS property for ODJFS business purposes.

V. DEFINITIONS:

A. BYOD (Bring Your Own Device) - BYOD refers to employees bringing their own personal device to work, whether laptop, smart phone or tablet, in order to interface to the agencies internal production networks and/or confidential information.

B. Portable computing device - The term portable computing device as used in this document but not limited to: laptops, flash drives, notebooks, personal digital assistants (PDAs), Smart Phones (e.g.: Blackberry, iPhone, Android based phones etc.), tablet PCs (e.g.: iPad, Kindle, Nook, etc.) and any emerging technology containing a processor and/or memory that could be used to store agency data in a portable format. The security safeguards may vary by device type, but in all cases must comply with the requirements set forth in this policy.

VI. POLICY:

A. GENERAL

1. ODJFS computers and information systems are the property of ODJFS. They may be used only for explicitly authorized purposes. ODJFS reserves the right to examine all data stored in or transmitted by its computers and systems. Without notice, the Chief Inspector's Office, ODJFS supervisors, deputies, and authorized management information systems staff may enter, search, monitor, track, copy, and retrieve any type of electronic file of any employee or contractor. These actions may be taken for business-purpose inquiries including, but not limited to, theft investigation, unauthorized access and/or disclosure of confidential business or proprietary information, excessive personal use of the system, or monitoring work flow and employee productivity.

2. **Personnel have no rights to privacy in their use of the Internet and e-mail.** Authorized designees (as referenced above) may access any files stored on or deleted from computers and information systems. When necessary, Internet, e-mail, and Instant Messenger (IM) usage patterns may be examined for work-related purposes, including situations where there is a need to investigate possible misconduct and to assure that these resources are devoted to maintaining the highest levels of productivity. The Chief Inspector's Office has the authority and ability to monitor Internet sites contacted, e-mail, and Instant Messenger (IM) usage at its own discretion or at the request of management.

3. All software installed on any ODJFS computer must be licensed to ODJFS. Personnel must receive advance approval from their deputy director and the Office of Information Services (OIS) deputy director (or their respective designees) before adding software programs to any ODJFS computer. Questions regarding currently authorized software programs and/or software licensed to ODJFS are to be directed to the OIS deputy director or designee.

4. When making use of personally owned devices such as laptops, cellular devices and wireless tablets within ODJFS facilities or on ODJFS provided networks, users of such devices MUST adhere to all ODJFS policies related to computer usage and work performance. These devices are not allowed to be physically connected to the ODJFS production network or ODJFS owned devices. For example, employees should not be linking their personal cellular phones to their assigned computers or laptops even for purposes of charging the phone. ODJFS does allow for WiFi access to the public internet in limited facilities. When making use of these ODJFS provided WiFi internet services, users are responsible for ensuring their usage of such devices does not have a negative impact on their ability to meet their work related responsibilities or inhibit the ability of those around them to perform their work. For those making use of the ODJFS WiFi public internet service, there is no expectation of privacy for any information sent across this network, and their activity is subject to monitoring.

B. ALLOWABLE USES OF COMPUTERS AND INFORMATION SYSTEMS FOR ODJFS BUSINESS PURPOSES

1. facilitating job function performance;
2. facilitating and communicating business information within ODJFS and the county network;
3. coordinating meeting locations and resources for ODJFS;
4. communicating with outside organizations as required in the performance of employee job functions.

C. PROHIBITED USES OF COMPUTERS AND INFORMATION SYSTEMS INCLUDING, BUT NOT LIMITED TO, APPLICATIONS, E-MAIL, INSTANT MESSENGER (IM), SHORT MESSAGE SERVICE (SMS) TEXT MESSAGING, Portable computing device AND THE INTERNET. The following is a non-exhaustive list of prohibited uses:

1. violating local, state, and/or federal law (See ODJFS-IPP 0003);
2. harassing or disparaging others based on age, race, color, national origin, sex, sexual orientation, disability, religion, or political beliefs (See ODJFS-IPP 9002 and ODJFS-IPP 10003). Harassment and disparagement include but are not limited to slurs, obscene messages, or sexually explicit images, cartoons, or messages;
3. threatening others;
4. soliciting or recruiting others for commercial ventures, religious or political causes, outside organizations, or other matters which are not job related;
5. using computers or information systems in association with the operation of any for-profit business activities or for personal gain;
6. sabotage, e.g. intentionally disrupting network traffic or crashing the network and connecting systems or intentionally introducing a computer virus;
7. accessing an employee's files without authorization and with no substantial business purpose;
8. vandalizing the data of another user;
9. forging electronic mail and Instant Messenger (IM) messages;
10. sending chain letters;
11. sending rude or obscene messages (e-mail or Instant Messenger (IM) should not be used to send anything that would embarrass or discredit ODJFS or the State of Ohio);
12. disseminating unauthorized confidential or proprietary ODJFS or client documents or information or data restricted by government laws or regulations (See ODJFS-IPP 8501 and ODJFS-IPP 3922);
13. disseminating (including printing) copyrighted materials, articles, or software in violation of copyright laws (See ODJFS-IPP 0003);
14. accessing the Internet in any manner that may be disruptive, offensive to others, or harmful to morale;
15. transmitting materials (visual, textual, or auditory) containing ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on age, race, color, national origin, gender, sexual orientation, disability, religious or political beliefs;
16. sending or soliciting sexually-oriented messages or images;
17. using the Internet or Instant Messenger (IM) for political activity;
18. using the Internet to sell goods or services not job related or specifically authorized in writing by an approving authority;

19. downloading and viewing non-work-related streaming audio or video (e.g. listening to radio stations, etc.) due to the limited bandwidth of the system;
20. intentionally using Internet facilities to disable, impair, or overload performance of any computer system or network or to circumvent any system intended to protect the privacy or security of another user;
21. speaking to the media or to the public within any news group or chat room on behalf of ODJFS if not expressly authorized to represent ODJFS;
22. uploading or downloading games, viruses, copyrighted material, inappropriate graphics or picture files, illegal software, and unauthorized access attempts into any system;
23. using electronic devices while operating a state vehicle;
24. storing non-work, personal documents on any drive of a state-owned computer or network.

NOTE: Whether during work hours or not, these prohibitions apply at all times. **Personnel cannot expect that the information they convey, create, file, or store in ODJFS computers and information systems will be confidential or private regardless of the employee's intent.**

D. USE OF THE E-MAIL SYSTEM AND INSTANT MESSENGER (IM)

1. Official Use

   a. When using e-mail or Instant Messenger (IM), as with all written official communications, personnel are expected to display a formal, businesslike demeanor in order to reflect professionalism and credibility on ODJFS and themselves.

   b. Everyone is responsible and liable for the content of his or her electronic mail or message. As stated earlier, all electronic data may be accessed at anytime by the Chief Inspector's Office or management for legal or business purposes.

2. Nonofficial Use

   a. Personnel may access the e-mail and Instant Messenger (IM) system for nonofficial business provided that such communication does not disrupt or interfere with official ODJFS business, is kept to a minimum duration and frequency, does not violate other provision of this policy and is not political in nature. Similar to telephone usage, minimal personal e-mail and Instant Messenger (IM) may be received or sent provided that no cost is incurred by ODJFS.

   b. **<u>CAVEAT</u>: Please remember that there is no expectation of privacy for anything sent by e-mail or Instant Messenger (IM) and that others can view this information at any time.**

3. INTERNET ACCESS GUIDELINES:

   a. Applicability

      This policy provides only guidelines to ODJFS personnel for Internet access. It does not supersede state or federal laws or any office policies regarding confidentiality, information dissemination, or standards of conduct.

   b. General Information

      In our effort to enhance client service and facilitate communication among personnel, ODJFS provides all personnel with Internet access. Personnel Internet access accommodates basic e-mail functions, file transfer, and interactive terminal access to accomplish ODJFS business goals. ODJFS permits personnel to use and explore this technology so that everyone may become as proficient as

possible in order to improve work quality and efficiency. All ODJFS personnel must become familiar with and acknowledge ODJFS policies relating to the Internet use in order to make the best use of the technology, maintain a professional environment, and protect valuable ODJFS and client information.

c. Guidelines for Incidental/Occasional Personal Internet Usage:

Generally, the Internet is to be used for work-related purposes. ODJFS will permit personal use of the Internet with reasonable restrictions as to the amount of time devoted to personal usage and sites visited provided such use does not adversely affect business or productivity. Incidental/occasional use is comparable to time authorized for meals and reasonable breaks during the workday and those times only should be used to attend to personal matters. ODJFS has the right to insist that agency Internet resources are devoted to maintaining the highest degree of productivity. Personal Internet usage is a privilege, not a right. As such, the privilege may be revoked at any time and for any reason.

CAVEAT: Please remember incidental/occasional use is considered part of the meal and break time of personnel. Personnel are not permitted to utilize the Internet equal to meal and break times and also take their scheduled meal and breaks. Such actions will be considered excessive.

d. Filtering by Screening Software

ODJFS has the right and may filter and deny users Internet access to sites considered inappropriate. Although not all-inclusive, examples of inappropriate sites that may be filtered are those depicting violence/profanity, partial or full nudity, sexual activity, gross depictions, intolerance, satanic/cult images, militant/extremist images, questionable/illegal, and gambling activities.

CAVEAT: Please remember that there is no expectation for privacy for an employee's use of the Internet and that others can view this activity at any time.

E. SECURING COMPUTER EQUIPMENT AND ELECTRONIC DATA

1. ODJFS employees who are responsible for or are assigned portable computer equipment and electronic media (i.e., laptops, thumb drives, external hard drives, DVD's, CD's, etc.) shall secure those items when they are not present in the office. These items routinely contain confidential and/or HIPAA information which could be compromised if lost or stolen.

2. If over-night travel is required, the computer equipment is expected to be secured in the hotel room, residence, etc. When necessary, computer equipment can be placed in the trunk of a vehicle so long as items are not visible, but the trunk and the vehicle must be locked. Leaving computer equipment on the front or back seat of a vehicle, or in any way visible, is not permitted.

3. If an ODJFS employee is responsible for a pool of portable equipment (e.g., equipment that is shared by many employees), the equipment shall be secured while in and out of the office. Sign-in and sign-out sheets shall be utilized to track the location of the equipment at all times. The sign in and out sheet at a minimum should include the employee's name who is using the equipment and the pick-up and return date.

4. If an employee loses a piece of equipment or it is stolen, they are required to immediately notify their supervisor and the Chief Inspector's Office.

5. Failure to properly secure portable computer equipment and electronic data is subject to disciplinary action.

F. VIOLATIONS OF POLICY:

Violations of this policy will be reviewed on a case-by-case basis and may result in disciplinary action up to and including removal.

CLICK HERE to acknowledge that you have read, understand, and will comply with this policy.

VII. APPENDIXES:

A. SUBJECT MATTER EXPERT

Owning Entities	Address	Name (SME)	Phone/ Fax/ E-mail
Chief Inspector	30 East Broad Street, 32nd Floor, Columbus, Ohio 43215-3414	Steven Johnson, Investigations Supervisor	614-466-3015 614-466-0207 steven.johnson@jfs.ohio.gov