

## **IPP.3925. Data Access Policy**

### **IPPMTL 0280**

July 29, 2014 - Version 2.1-*Revised*

October 8, 2010 - Original

**CLICK [HERE](#) to acknowledge that you have read, understand, and will comply with this policy.**

#### **I. PURPOSE/REASON:**

- A. To establish departmental requirements for what are considered business appropriate uses of ODJFS Confidential Personal Information (CPI) stored in ODJFS maintained computer systems. These expectations are based on federal and state statutory requirements for the multiple core Lines of Business within the Department and their supporting Offices.
- B. On April 6, 2009, Governor Ted Strickland issued the revised Management Directive - "Accessing Confidential Personal Information". This Management Directive sets forth the process that all executive agencies shall follow to implement section 1347.15 of the Ohio Revised Code. Within the Management Directive is a requirement that each state agency develop access policies - the criteria, references, procedures and requirements identified in section 1347.15(B) of the Revised Code - for the state agency's confidential personal information systems.

#### **II. REFERENCES/AUTHORITY:**

##### **A. REFERENCES**

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

1. Governors April 6, 2009 Management Directive "Accessing Confidential Personal Information"
2. Ohio Revised Code (ORC) 1347.15
3. Ohio Administrative Code Rule [5101:9-22-16](#) ODJFS Employee Access to Confidential Personal Information
4. [IPP 3001](#) ODJFS Information Security Policy
5. Research Policy

##### **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:**

IPP.3925.Data Access Policy Version 1 October 8, 2010

#### **IV. SCOPE:**

This policy applies to all state employees in the employment of ODJFS.

#### **V. DEFINITIONS:**

- A. "Access" as a noun means an opportunity to copy, view or otherwise perceive. As a verb, "access" means to copy, view or otherwise perceive.
- B. "Acquisition of a new computer system" means the purchase of a computer system, as defined in this chapter, which is not a computer system currently in place nor one for which the

# Exhibit 1

Page 2 of 7

acquisition process has been started as of the effective date of the agency rule addressing ORC 1347.15 requirements.

- C. "Computer system" means a "system," as defined by section 1347.01 of the Revised Code, that stores, maintains or retrieves personal information using electronic data processing equipment.
- D. "Confidential Personal Information (CPI)" means "confidential personal information" as defined in section 1347.15(A)(1) of the Revised Code.
- E. "Employee of the state agency" means each employee of a state agency regardless of whether he or she holds an elected or appointed office or position within the state agency. "Employee of the state agency" is limited to the specific state agency that has the appointing authority for the employee.
- F. "Incidental contact" means contact with the information that is secondary or tangential to the primary purpose of the activity that resulted in the contact.
- G. "Individual", in the context used in ORC 1347.15(C)(1)(b) means the subject of the CPI or the subject of the CPI's authorized representative, legal counsel, legal custodian or legal guardian, and anyone as otherwise permitted under state or federal law acting on behalf of, or in furtherance of, the interests of the subject of the CPI. Individual does NOT include an opposing party in litigation, or the opposing party's legal counsel, or an investigator, auditor or any other party who is not acting on behalf of, or in furtherance of the interests of, the subject of the CPI, even if such individual has obtained a signed release from the subject of the CPI.
- H. "Information owner" is the one individual appointed in accordance with section 1347.05(A) of the Revised Code to be directly responsible for a system.
- I. "Person" means natural person.
- J. "Personal information" means "personal information" as that term is defined in section 1347.01(E) of the Revised Code.
- K. "Personal information system" means a "system" that "maintains" "personal information" as those terms are defined in section 1347.01 of the Revised Code. "System" includes manual and computer systems.
- L. "Research" means to explore, analyze, or examine data.
- M. "Routine" means common place, regular, habitual, or ordinary.
- N. "System" means "system" as defined in section 1347.01(F).
- O. "Upgrade" means a substantial redesign of an existing system for the purpose of providing a substantial amount of new application functionality, or application modifications which would involve substantial administrative or fiscal resources to implement. "Upgrade" does not include maintenance, minor updates and patches, or modifications that entail a limited addition of functionality due to changes in business or legal requirements. For the purposes of this policy ODJFS defines "substantial redesign" to mean any change that modifies greater than 50% of the code or functionality in an existing application.
- P. "Health Insurance Portability and Accountability Act (HIPAA)" refers to a federal law passed in 1996 that limits restrictions that a group health plan can place on benefits for preexisting conditions, while establishing national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The Administration Simplification provisions of the act also added new standards for the security and privacy of health related personal data.
- Q. "Protected Medicaid information" refers to data which is protected under the Federal Code of Regulations specific to the Medicaid Program.
- R. "Federal Tax Information (FTI)" is any information received from the Internal Revenue Service (IRS) that is considered protected under the statutes of the Federal Internal Revenue Code (IRC).

S. "Nation Directory of New Hires (NDNH)" is a National Database that tracks wages and employment information containing:

1. New Hire (W-4)
2. Quarterly Wage (QW)
3. Unemployment Insurance (UI)

Data Matching Services of NDNH data is used by several ODJFS program areas for program administration.

T. "Public Record" means data that is subject to disclosure through Ohio public records law section 149.43 of the Revised Code.

## VI. **POLICY:**

The ODJFS mission is to help Ohioans improve the quality of their lives as the nation's leading family support and workforce development agency through: accountability, compassion, integrity, respect and teamwork.

These values that form the core guiding principles that drive this agency in the performance of our mission cannot be achieved without access to the Confidential Personal Information with which our clients and business partners have entrusted us. It is in the interest of maintaining and ensuring this trust that this policy seeks to establish the valid reasons for accessing these key information assets. ODJFS is made up of multiple lines of business that provide unique yet integrated services to Ohio citizens and employers. The computer systems used in the delivery of these services are large and complex in nature, as are the back-end data repositories that drive these systems. This makes for an extremely large array of confidential information that we are responsible for maintaining and protecting within these systems. Without this data, we could not function as an organization. Thus, anything that represents a threat to the security of this data, represents a threat to ODJFS ability to provide services. For this reason each employee must understand their vested interest in maintaining the security and privacy of the confidential information with which we have been entrusted. The purpose of the following is to provide clear guidance as to what is deemed valid access to ODJFS CPI and the legal basis for this guidance.

### A. Criteria for accessing confidential personal information

The statutory definition of "CPI" is any personal information that is not considered public record under ORC 149.43. For ODJFS, CPI includes any non-public information about ODJFS employees, contractors and service providers (such as social security numbers and non-work-related addresses), as well as any information identifying applicants for, recipients of, and participants in, ODJFS-administered programs that fall under the category of public assistance (e.g. cash and food assistance and child care subsidies) child support, child welfare (including adoption, foster care and child care), unemployment compensation, and workforce development.

ODJFS personal information systems are managed on a need to know basis, whereby each information owner determines the level of access required for an employee of the agency to fulfill his or her job duties. The determination of access to CPI must be approved by the employee's supervisor and the information owner prior to providing the employee with access to CPI within a personal information system. ODJFS has procedures for determining a revision to an employee's access to confidential personal information upon a change to that employee's job duties, including but not limited to a transfer or termination. Whenever an employee's job duties no longer requires access to confidential personal information in a personal information system, then that employee's access to CPI shall be removed.

### B. Valid Reasons for Accessing CPI

ODJFS is organized such that there are multiple core lines of business and several supporting offices that perform the management, administrative and technical functions that are common across these multiple core lines of business.

# Exhibit 1

In general, any access to and use of CPI that is collected and maintained by ODJFS is strictly limited to those purposes authorized by ODJFS, and as directly related to the system user's official job duties and work assignments for, and on behalf of, ODJFS and/or a federal oversight agency. Some examples of when accessing CPI is prohibited include, but are not limited to, access that results in personal or political gain, and commercial use unrelated to official departmental business. Below is a list of valid reasons for accessing CPI (regardless of whether the CPI is maintained electronically or on paper) that are common across all lines of business.

1. In the course of administering or performing job duties related to the following processes, authorized employees of the agency would have valid reasons for accessing CPI:
  - a. Responding to (a) public records requests, when public records are comingled with CPI, or (b) records requests made by the individual for his/her own CPI;
  - b. Program administration, including (a) compliance with federal/state laws and regulations, (b) processing or payment of claims, (c) eligibility determinations (d) audits, investigations and oversight, (e) licensing and certification, and (f) administrative hearings;
  - c. Litigation (including discovery and responding to court orders and subpoenas);
  - d. Human resource matters (hiring, promotion, demotion, discharge, salary/compensation issues, leave requests/issues, time card approvals/issues);
  - e. Complying with an Executive Order or policy;
  - f. Complying with an agency policy or a state administrative policy issued by the Department of Administrative Services, the Office of Budget and Management or other similar state agency;
  - g. Research in the furtherance of agency specific programs in so far as allowed by statute; or
  - h. Complying with a collective bargaining agreement provision.
2. In addition to the general processes described in paragraph (A) above, ODJFS must comply with numerous federal and state laws and regulations that limit its use and disclosure of CPI, including but not limited to:
  - a. 45 CFR Parts 160 and 164 (HIPAA-45 CFR 164.501);
  - b. 5 USC 552a (Social Security Data);
  - c. 7 CFR 272.1(c) (Food Assistance);
  - d. Ohio Revised Code (ORC) sections:
    - (1) 5101.27 through 5101.31 (Public Assistance, Child Care, Foster Care, Medicaid),
    - (2) 5101.99 (penalties for disclosure),
    - (3) 3107.17 (adoption),
    - (4) 3107.42 (adoption),
    - (5) 3107.99 (penalties for disclosure),
    - (6) 3121.894 (child support),
    - (7) 3121.899 (child support),
    - (8) 3121.99 (penalties for disclosure),
    - (9) 3125.08 (child support),
    - (10) 3125.50 (child support),
    - (11) 3125.99 (child support),

- (12) 4141.21 (unemployment compensation),
- (13) 4141.22 (unemployment compensation) and
- (14) 4141.99 (penalties for disclosure);
- e. 29 USC 2935(a)(4) (workforce development), and
- f. OAC rules 4141-43-01 through 4141-43-03 (unemployment and workforce development).

Note that the citations listed above are not all-inclusive. For a more complete list of public records and confidentiality laws applicable to ODJFS-administered programs, please visit the Public Records and Confidentiality Laws e-manual available on-line.

- 3. Intentional violations of this policy shall result in disciplinary action up to and including removal in accordance with current disciplinary guidelines.

C. Other Data Privacy Concerns

- 1. Federal Tax Information (FTI)

The expectation for any state and/or local entity for protecting Federal Tax Information is identified in the latest IRS Publication 1075 "Tax Information Security Guidelines for Federal, State and Local Agencies and Entities - Safeguards for Protecting Federal Tax Returns and Return Information" which is accessible via the ODJFS InnerWeb or IRS.GOV.

- 2. National Directory of New Hires (NDNH) data

It is prohibited of any ODJFS employee to transmit Nation Directory of New Hires (NDNH) Data using any commercial or public devices.

**VII. PROCEDURES:**

- A. Any upgrades to existing ODJFS computer systems, or the acquisition of any new computer systems, that stores, manages, or contains Confidential Personal Information (CPI), shall include a mechanism for recording specific access by users of the system to CPI contained within that system. System upgrades is defined as any update requiring over half of the lines of code to be modified.;
- B. Until an upgrade or new acquisition of the type described above occurs, each Office within ODJFS is responsible for documenting a manual logging procedure for their staff. This procedure must be documented and forwarded for review to the ODJFS Chief Privacy Officer. Upon receipt of the documentation the ODJFS Chief Privacy Officer will call upon the ODJFS Chief Inspector and Chief Legal Counsel or designees to perform a joint review of the manual logging process to validate that it will meet the requirements as set forth in the legislation. This document must show that the process captures the fields identified as required within the attached Minimum Application Logging Standards;
  - 1. There exist two exceptions for the need to log access to CPI:
    - a. The access occurs as a result of research performed for official agency purposes, routine office procedures, or incidental contact with the information, unless the conduct resulting in the access is specifically directed toward a specifically named individual or a group of specifically named individuals. E.g., a helpdesk staff person is requested to assist in the resolution of a program or technical issue and in the course of resolving the issue they must access CPI.
    - b. The access is to confidential personal information about an individual, and the access occurs as a result of a request by that individual or their legal representative for confidential personal information about that same individual. E.g., a child support obligee calls with an inquiry about his/her own payment history.

# Exhibit 1

Page 6 of 7

## C. Information Requests

Upon the signed written request of any individual whose confidential personal information may be kept by the agency, the agency shall do all of the following:

1. Verify the identity of the individual by a method that provides safeguards commensurate with the risk associated with the confidential personal information.
2. Provide to the individual the confidential personal information that does not relate to an investigation about the individual or is otherwise not excluded from the scope of chapter 1347 of the Revised Code.
3. During the pendency of an ongoing investigation about the individual, determine what, if any, records can be shared with that individual.

## D. Notification of Invalid Access

1. Upon discovery or notification that CPI of a person has been accessed by an agency employee for an invalid reason, the agency shall take steps to notify the person whose information was invalidly accessed as soon as practical and to the extent known at the time. The agency shall delay notification for a period of time necessary to ensure that the notification will not delay or impede an investigation or jeopardize homeland or national security. The agency may delay the notification consistent with any measures necessary to determine the scope of the invalid access, including which individuals' confidential personal information invalidly was accessed and to restore the reasonable integrity of the system. "Investigation" as used in this paragraph includes the investigation of the circumstances and involvement of employees surrounding the invalid access of the confidential personal information. Once the agency determines that notification will not delay or impede an investigation, the agency must disclose the access to confidential personal information made for an invalid reason to the subject of the CPI.
2. The notification given by the agency shall inform the person of the type of confidential personal information invalidly accessed and the date(s) of the invalid access (or as closely approximated as possible).
3. Notification may be made by any method reasonably designed to accurately inform the person of the invalid access, including written, electronic, or telephone notice.

E. The ODJFS director shall designate an employee of the agency to serve as the Data Privacy Point of Contact under the working title of ODJFS Chief Privacy Officer. The Data Privacy Point of Contact shall work closely with the State of Ohio Chief Privacy Officer and State Chief Security Officer to assist the agency with both the implementation of privacy protections for the Confidential Personal Information that the agency maintains and compliance with Section 1347.15 of the Revised Code and the rules adopted thereunder.

F. The ODJFS Chief Privacy Officer will ensure the timely completion of the Privacy Impact Assessment form developed by the Office of Information Technology.

G. The ODJFS Chief Privacy Officer will ensure that all ODJFS computer systems containing CPI employs password or an equivalent form of authentication, and employ the usage of encryption, as deemed appropriate through a Privacy Impact Assessment so as to ensure access to CPI is kept secured.

H. All ODJFS employees must take part in a departmental training program that will at a minimum include awareness of all applicable statutes, rules, and policies governing access to confidential personal information with which they may come into contact as part of their assigned job duties. It is the responsibility of the Business Office and Managing Supervisor to document and administer this required training to all direct report employees.

I. ODJFS will create a poster describing agency policies related to the protection of confidential personal information and post it in a conspicuous place in the main office of the agency and in all locations where the state agency has branch offices.

J. Receipt of this policy must be acknowledged by all agency employees.

**CLICK [HERE](#) to acknowledge that you have read, understand, and will comply with this policy.**

**VIII. APPENDIXES:**

A. SUBJECT MATTER EXPERT(S)

<b>Owning Entity</b>	<b>Address</b>	<b>Name (SME)</b>	<b>Phone/ E-mail</b>
OIS	4200 E. 5th Ave. Columbus, OH 43219	Corey Sines ODJFS Security Architect	614-387-8284 Corey.Sines@jfs.ohio.gov
OIS	4200 E. 5th Ave. Columbus, OH 43219	Rick Copley ODJFS Chief Security/ Privacy Officer	614-387-8126 Rick.Copley@jfs.ohio.gov

B. [ODJFS IPP 3001](#) Information Security

## **IPP.0003. Standards of Employee Conduct**

### **IPPMTL 0245**

May 11, 2011 - *Revised*

May 23, 2003 - *Original*

**CLICK [HERE](#) to acknowledge that you have read, understand, and will comply with this policy.**

#### **I. PURPOSE/REASON:**

- A. To provide all ODJFS employees with a clear understanding of the behaviors expected of them, behaviors that are prohibited, and the penalties that may be imposed for engaging in prohibited behaviors.
- B. An additional purpose is to standardize the rules of employee conduct so that they are applied fairly and understood by all employees.

#### **II. REFERENCES/AUTHORITY:**

##### **A. REFERENCES**

1. Ohio Revised Code (ORC) [124.34](#)
2. ORC [5101.02](#)
3. Ohio Ethics Law, [Chapter 102](#)
4. ORC [2921](#) *et al*
5. OCSEA Labor Agreement *et al*
6. SEIU 1199 Labor Agreement *et al*
7. All ODJFS Internal Policies and Procedures (IPPs)
8. OAC [123:1](#) *et al*
9. DAS policy [HR-D-02](#)

##### **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 0003 Standards of Employee Conduct dated September 4, 2009.

#### **IV. SCOPE:**

- A. This policy applies uniformly to all employees who are under the jurisdiction of the Ohio Department of Job and Family Services (ODJFS), with the following exceptions:
- B. Unclassified employees, as defined by the Ohio Revised Code, shall be required to comply with the Standards of Employee Conduct set forth in this document, however no provision of this document is to be construed as an employment contract. All unclassified employees are employed at will and serve at the pleasure of the appointing authority.
- C. Fair Labor Standards Act (FLSA) overtime-exempt employees are subject to the Standards of Employee Conduct; however, the schedule of discipline shall be adjusted to accommodate the overtime exemption.

# Exhibit 2

Page 2 of 10

- D. Initial probationary employees may be removed from their positions at any time during the probationary period for services that are unsatisfactory in accordance with OAC 123:1 and OCSEA and SEIU/1199 labor agreements.

## V. DEFINITIONS:

- A. **COUNSELING:** Corrective counseling is a tool used to communicate, define expectations, and provide an opportunity to achieve success. A corrective counseling meeting is not discipline. Counseling should be documented with a written memo noting the inappropriate behavior, steps to avoid the inappropriate behavior and a warning that future incidents may result in discipline. Such memos are not put in the employee's personnel file.
- B. **VERBAL (ORAL) REPRIMAND:** Memorandum to the employee with a copy to the personnel file (not placed in the personnel file for SEIU/1199) recording and documenting the nature of the verbal admonishment. The memorandum shall be on the standard Labor Relations form and include the date, rule violation and the nature of the violation as well as the proper course of behavior and future consequences, if the behavior is not corrected.
- C. **WRITTEN REPRIMAND:** Memorandum to the employee with a copy to the personnel file recording and documenting the nature of the written admonishment. The memorandum shall be on the standard Labor Relations form and include the date, rule violation and the nature of the violation as well as the proper course of behavior and future consequences, if the behavior is not corrected.
- D. **SUSPENSIONS:**
  - 1. **NON-WORKING:** The loss of a scheduled workday without pay.
  - 2. **WORKING SUSPENSION:** Equal in weight and retention to a non-working suspension, but differs in that the employee continues to work and receive pay. **NOTE:** May not be imposed on SEIU/1199 without the employee's consent.
  - 3. **Lengths:**
    - a) Minor - One day in length
    - b) Medium - Two to four days in length
    - c) Major - Five days in length
  - 4. Exempt employee suspensions, reductions, or fines are governed by OAC 123:1-31-01.
- E. **FINE:** Employee fines are governed by the applicable collective bargaining agreement and Ohio Administrative Code.
- F. **DEMOTION:** A reduction of exempt employees in pay or positions. Exempt employees may be reduced in pay and position for violations of the Ohio Revised Code 124.34.
- G. **REMOVAL:** The involuntary termination of employment with the Ohio Department of Job and Family Services.
- H. **LAST CHANCE AGREEMENT (LCA):** An agreement that is normally crafted when an employee is facing a major suspension or removal. The LCA requires that the employee not violate any specified standard of conduct for the term of the agreement or face removal without recourse.
- I. **OVERTIME EXEMPT EMPLOYEES:** Employees who are exempted from the overtime pay provisions of the Fair Labor Standard Act (FLSA) due to their job duties and responsibilities and/or professional status.
- J. **REDUCTION OF LEAVE:** Leave Reductions are governed by the applicable collective bargaining agreements. **NOTE:** May not be imposed without employee consent.

## VI. PROCEDURES:

- A. **RESPONSIBILITY**

1. The director or designee is responsible for ensuring that the *Standards of Employee Conduct* are provided and made known to each employee of the department.
2. It is the responsibility of all employees of ODJFS to familiarize themselves with and adhere to the policies and procedures of the Agency. Consistent with that is the responsibility of all employees of the Agency to conduct themselves in such a manner that their activities, both on and off duty, are consistent with the mission of the Agency and do not adversely affect their ability to perform their duties.
3. Managers and Supervisors are responsible for the appropriate and consistent application of the standards of employee conduct, policies, and procedures of the department. Supervisors also are responsible for counseling employees when appropriate and initiating the request for disciplinary action as soon as they are aware of a potential situation and have consulted with Labor Relations.
4. Labor Relations staff is responsible for providing requested advice, guidance, and assistance. Labor Relations staff are the Agency's designated management advocates and the Agency Designee for Union Contract Administration.
5. Labor Relations must be contacted anytime there is a question about counseling or discipline to ensure equal protection to the employee, supervisor and the Agency.

#### B. GENERAL STANDARDS OF CONDUCT

1. Attendance
  - a) Each employee is important to the operation of the organization and each job function is essential. Accordingly, it is essential that each employee take personal responsibility for good attendance practices, as attendance is a vital concern to the Agency. It is recognized that illness, personal matters, and emergencies may occasionally occur which could not have been predicted and that may cause an employee to be away from work.
  - b) Abuse or misuse of leave and failure to timely notify a supervisor of one's need for leave adversely impacts operation of the Agency. The abuse or misuse of leave results in excessive costs to the Agency (e.g., overtime to cover absent staff). Several violations are listed in the disciplinary grid to address the various elements of attendance violations.
2. Government Property
  - a) All government property, including but not limited to automobiles, supplies, equipment, telephones, computer hardware, computer software, electronic mail, ODJFS information systems, internet usage, and facilities are to be used for official purposes only, unless otherwise stated. Misuse, abuse, loss, theft, damage, or destruction of an employee's government property must be reported to his/her supervisor immediately.
  - b) ODJFS credentials or identification cards shall not be used to coerce, intimidate, or deceive others or to obtain any privilege or article not otherwise authorized in the performance of official duties.
3. Personal Conduct

Employees have a responsibility to respect the diversity of our workforce and afford their fellow workers a workplace free from harassment and intimidation. Employees shall recognize the limitations of their authority and at no time use the power of their position for personal advantage or gain. No employee shall accept or solicit bribes, gifts, money, or favors from vendors or agencies/entities with which ODJFS has a regulatory or fiduciary relationship.
4. Civil Workplace

**Civility is valued here.** ODJFS is dedicated to maintaining a workplace that is both productive and civil. Employees must treat colleagues, coworkers, internal/external customers, and the public with respect. Courteous and positive communication is expected; belittling, rude, hostile, and volatile behavior will not be tolerated. Vulgar language and gestures are not conducive to a reasonable and satisfactory work environment. Disagreements shall be settled by discussion and intervention.

5. Outside Employment

Employees shall not have a direct or indirect financial interest or other interest that conflicts or appears to conflict with one's government duties and responsibilities. For more information regarding conflicts of interest or outside employment see Chapters 102 (the Ohio Ethics Law) and 2921 of the Ohio Revised Code. Employee must report outside employment in accordance with IPP 5003.

6. Illegal Activities

Illegal activities on the part of any employee, in addition to being unlawful reflect on the integrity of the Agency and betray the trust and confidence placed in it by the public. It is expected that employees will obey, not only the letter of the law, but also the spirit of the law whether engaged in personal or official activities. An employee convicted of a felony must immediately report it to the Director or designee.

7. Confidentiality

Employees of the Agency have access to many different types of information. Each employee may only disclose or release information consistent with applicable law and agency policy.

8. Nepotism

- a) Except as provided in Section D of DAS policy HR-D-02, no public official or employee shall supervise any person closely related by blood, marriage or other significant relationship including business association.
- b) Employees will not authorize or use their authority or influence of his or her position to secure the authorization of employment or benefit (including a promotion or preferential treatment) for a person closely related by blood, marriage or other significant relationship including business association.

C. INVESTIGATIONS

Allegations of misconduct will be investigated. During the course of an investigation, employees are to cooperate fully by providing all pertinent information. Failure of an employee to answer any inquiry fully, truthfully and to the best of their knowledge will be grounds for disciplinary action. Individuals may also be required to submit to an official search of person or property. An employee may be placed on Administrative Leave during an investigation.

D. EMPLOYEE ASSISTANCE PROGRAM (EAP)

1. Employees experiencing personal problems that interfere with their duties and responsibilities are encouraged to seek the services of the Employee Assistance Program.
2. Participation by an employee in an EAP program may be considered in mitigating disciplinary action.
3. Imposition of discipline can be delayed until the employee completes an EAP program. Upon notice by the OHIO EAP of successful completion under the provisions of an Ohio EAP Participation Agreement, ODJFS will give serious consideration to modifying the contemplated discipline.
4. Separate disciplinary action may be instituted for offenses committed after commencement of an EAP Participation Agreement.

E. DISCIPLINE

1. In the Ohio Department of Job and Family Services, it is important that disciplinary actions be for just cause and be administered fairly throughout the department within the guidelines set herein. The discipline shall be commensurate with the offense taking into account the severity of the violation, mitigating circumstances, as well as previous discipline and other aggravating circumstances.
2. ODJFS is committed to the policy of constructive progressive discipline. Disciplinary actions should be imposed with the intent of giving the employee the opportunity to correct his/her behavior so long as the discipline is commensurate with the offense. If the behavior is not corrected, discipline should become increasingly more severe up to and including removal. However, certain offenses warrant severe discipline to include removal on the first offense.
3. Individual violations are not mutually exclusive. Progressive discipline need not be measured in terms of following the complete progression in each category. The violation of different work rules, the closeness in time and repetitive nature of the violations are examples of circumstances that aggravate the penalty.

F. VIOLATIONS AND PENALTIES

1. Appendix B provides the Violations and Penalties commonly referred to as the disciplinary grid. This is a guideline to inform employees of those actions that are considered unacceptable and the possible corrective action for such. **These guidelines are not all-inclusive and may vary depending upon individual mitigating or aggravating circumstances.**
2. Disciplinary corrective actions include, but are not limited to, the following forms:
  - a) Verbal Reprimand
  - b) Written Reprimand
  - c) Fine
  - d) Reduction of Leave
  - e) Working Suspension
  - f) Non-Working Suspension
  - g) Demotion
  - h) Removal

NOTE: Per appropriate bargaining unit contract or statute, not all corrective actions may be applicable.

**CLICK [HERE](#) to acknowledge that you have read, understand, and will comply with this policy.**

VII. **APPENDIXES:**

A. SUBJECT MATTER EXPERT(S)

Owning Entity	Address	Name(SME)	Phone/ Fax/ E-mail
Bureau of Civil Rights / Labor Relations	BCR/LR Office: 30 East Broad Street, 30th Floor, Columbus Ohio 43215	Labor Relations Staff	614-466-6514 614-752-6381 IPPM_STAFF@jfs.ohio.gov

B. THE DISCIPLINARY GRID, ODJFS STANDARDS OF EMPLOYEE CONDUCT, RULE VIOLATIONS AND PENALTIES

ODJFS-IPP 0003

**Standards of Employee Conduct**

Revised: June 20, 2011

Original: May 23, 2003

**APPENDIX B  
ATTENDANCE**

<b>CODE</b>	<b>VIOLATION OFFENSE</b>	<b>FIRST OFFENSE</b>	<b>SECOND OFFENSE</b>	<b>THIRD OFFENSE</b>	<b>FOURTH OFFENSE</b>
<b>A1</b>	FAILURE TO PROVIDE PROPER CALL OFF	VERBAL - WRITTEN	MINOR - MEDIUM	MEDIUM - MAJOR	MAJOR - REMOVAL
<b>A2</b>	ABSENT WITHOUT LEAVE, (AWOL)				
	A) ONE DAY OR LESS	WRITTEN - MINOR SUSPENSION	MEDIUM SUSPENSION	MAJOR SUSPENSION	REMOVAL
	B) TWO DAYS	MEDIUM SUSPENSION	MAJOR SUSPENSION	REMOVAL	*
	C) THREE DAYS	MAJOR SUSPENSION	REMOVAL	*	*
	D) FOUR OR MORE DAYS	REMOVAL	*	*	*
<b>A3</b>	MISUSE OF ACCRUED LEAVE	WRITTEN - MINOR SUSPENSION	MEDIUM SUSPENSION	MAJOR SUSPENSION	REMOVAL
<b>A4</b>	FAILURE TO WORK SPECIFIC HOURS WHEN REQUIRED, INCLUDING MANDATORY OVERTIME	WRITTEN - MINOR SUSPENSION	MEDIUM SUSPENSION	MAJOR SUSPENSION	REMOVAL
<b>A5</b>	TARDINESS 30 MINUTES OR LESS	VERBAL - WRITTEN	MEDIUM	MAJOR	REMOVAL
<b>A6</b>	JOB ABANDONMENT 3 CONSECUTIVE WORKDAYS WITHOUT PROPER NOTICE	REMOVAL	*	*	*
<b>A7</b>	PATTERN ABUSE CONSISTENT PERIODS OF SICK LEAVE WITHIN A SIX WEEK PERIOD	VERBAL - WRITTEN	MINOR - MEDIUM SUSPENSION	MEDIUM - MAJOR SUSPENSION	MAJOR SUSPENSION - REMOVAL
<b>A8</b>	FAILURE TO PROVIDE A PHYSICIANS VERIFICATION WHEN REQUIRED	VERBAL - WRITTEN	MINOR - MEDIUM SUSPENSION	MEDIUM - MAJOR SUSPENSION	MAJOR SUSPENSION - REMOVAL
<b>A9</b>	LEAVING WORK AREA, EXTENDEING BREAKS, OR EXTENDING LUNCH WITHOUT AUTHORIZATION	VERBAL - WRITTEN	MINOR - MEDIUM SUSPENSION	MEDIUM - MAJOR SUSPENSION	MAJOR SUSPENSION - REMOVAL

ODJFS-IPP 0003

## Standards of Employee Conduct

Revised: June 20, 2011

Original: May 23, 2003

### FAILURE OF GOOD BEHAVIOR

CODE	VIOLATION	FIRST OFFENSE	SECOND OFFENSE	THIRD OFFENSE	FOURTH OFFENSE
<b>F1</b>	FAILURE TO CARRY OUT AND/OR FOLLOW DIRECTIONS, ASSIGNMENTS, WRITTEN POLICIES, PROCEDURES, AND/OR WORK RULES	VERBAL WRITTEN	MINOR - MEDIUM SUSPENSION	MEDIUM - MAJOR SUSPENSION	MAJOR SUSPENSION REMOVAL
<b>F2</b>	FAILURE TO CARRY OUT A DIRECT ORDER	WRITTEN - MINOR SUSPENSION	MINOR - MEDIUM SUSPENSION	MEDIUM - MAJOR SUSPENSION	REMOVAL
<b>F3</b>	DISCOURTEOUS AND/OR RUDE CONDUCT: TREATMENT OF ANOTHER THROUGH OFFENSIVE OR INDECENT CONDUCT	WRITTEN - MINOR SUSPENSION	MEDIUM SUSPENSION	MAJOR SUSPENSION	REMOVAL
<b>F4</b>	PROMOTION OF OR PARTICIPATION IN ILLEGAL GAMBLING ACTIVITIES DURING WORKING HOURS	VERBAL - WRITTEN	MINOR - MEDIUM SUSPENSION	MEDIUM - MAJOR SUSPENSION	MAJOR SUSPENSION - REMOVAL
<b>F5</b>	VIOLATION OF ODJFS DRESS CODE POLICY	VERBAL - WRITTEN	MINOR - MEDIUM SUSPENSION	MEDIUM - MAJOR SUSPENSION	MAJOR SUSPENSION - REMOVAL
<b>F6</b>	UNAUTHORIZED DISPLAY, SOLICITATION, AND/OR DISTRIBUTION OF LITERATURE	VERBAL - WRITTEN	MINOR - MEDIUM SUSPENSION	MEDIUM - MAJOR SUSPENSION	MAJOR SUSPENSION - REMOVAL
<b>F7</b>	POSTING OR DISPLAYING INAPPROPRIATE MATERIAL	VERBAL - WRITTEN	MINOR - MEDIUM SUSPENSION	MEDIUM - MAJOR SUSPENSION	MAJOR SUSPENSION - REMOVAL
<b>F8</b>	ACTS OF SEXUAL HARRASSMENT, DISCRIMINATION, INSULT, INTIMIDATION, OR HARASSMENT ON THE BASIS OF A PROTECTED CLASS	MEDIUM SUSPENSION - REMOVAL	MAJOR SUSPENSION - REMOVAL	REMOVAL	*
<b>F9</b>	NEPOTISM	MEDIUM SUSPENSION - REMOVAL	MAJOR SUSPENSION - REMOVAL	REMOVAL	*
<b>F10</b>	FELONY CONVICTION OR FAILURE TO DISCLOSE A FELONY CONVICTION	REMOVAL	*	*	*
<b>F11</b>	PURPOSEFUL, CARELESSNESS, OR UNAUTHORIZED USE OR ABUSE OF STATE EQUIPMENT, PROPERTY, STATE PAID TIME, OR	WRITTEN - REMOVAL	MINOR SUSPENSION - REMOVAL	MEDIUM SUSPENSION - REMOVAL	MAJOR SUSPENSION - REMOVAL

ODJFS-IPP 0003

**Standards of Employee Conduct**

Revised: June 20, 2011

Original: May 23, 2003

**FAILURE OF GOOD BEHAVIOR**

CODE	VIOLATION	FIRST OFFENSE	SECOND OFFENSE	THIRD OFFENSE	FOURTH OFFENSE
	THE PROPERTY OF ANOTHER				

**FAILURE OF GOOD BEHAVIOR**

<b>F12</b>	ENGAGING IN POLITICAL ACTIVITIES AS PROHIBITED BY ORC 124.57	WRITTEN - MINOR SUSPENSION	MEDIUM SUSPENSION	MAJOR SUSPENSION	REMOVAL
<b>F13</b>	PARTICIPATION IN WORK STOPPAGE, STRIKE, SLOW DOWN, SICK OUT OR OTHER FORM OF JOB ACTION OR WORK INTERRUPTION CONCERTED OR OTHERWISE; INTERFERING WITH THE ACTIVITIES OF EMPLOYEES WHO DO NOT PARTICIPATE IN A WORK STOPPAGE	MAJOR SUSPENSION - REMOVAL	REMOVAL	*	*
<b>F14</b>	REFUSAL TO FULLY COOPERATE WITH AND/OR PROVIDING FALSE, INCOMPLETE, OR MISLEADING INFORMATION IN AN INVESTIGATION OR INQUIRY	MEDIUM SUSPENSION - REMOVAL	MAJOR SUSPENSION - REMOVAL	REMOVAL	*
<b>F15</b>	MISUSE, REMOVAL OF PROVIDING OR DISCUSSING CONFIDENTIAL MATERIAL, RECORDS, OR OFFICIAL DOCUMENTS OR CUSTOMER INFORMATION	MAJOR SUSPENSION - REMOVAL	REMOVAL	*	*
<b>F16</b>	UNAUTHORIZED USE OF RECORDING DEVICES	WRITTEN - MINOR SUSPENSION	MINOR - MEDIUM SUSPENSION	MEDIUM - MAJOR SUSPENSION	REMOVAL
<b>F17</b>	SLEEPING WHILE ON DUTY	WRITTEN - MINOR SUSPENSION	MINOR - MEDIUM SUSPENSION	MEDIUM - MAJOR SUSPENSION	REMOVAL
<b>F18</b>	INATTENTION TO DUTY, NOT ALERT ON DUTY, APPEARING TO BE IN OR TAKING ON A POSTURE OF REST WHILE ON DUTY.	VERBAL - WRITTEN	MINOR - MEDIUM SUSPENSION	MEDIUM - MAJOR SUSPENSION	MAJOR SUSPENSION - REMOVAL
<b>F19</b>	FAILURE TO REPORT IMMEDIATELY A VIOLATION OF ANY WORK RULE, LAW, OR REGULATION	WRITTEN - MINOR SUSPENSION	MEDIUM SUSPENSION	MAJOR SUSPENSION	REMOVAL

**FAILURE OF GOOD BEHAVIOR**

<b>CODE</b>	<b>VIOLATION</b>	<b>FIRST OFFENSE</b>	<b>SECOND OFFENSE</b>	<b>THIRD OFFENSE</b>	<b>FOURTH OFFENSE</b>
<b>F20</b>	VIOLATION OF OHIO ETHICS LAW	MAJOR SUSPENSION - REMOVAL	REMOVAL	*	*
<b>F21</b>	THEFT IN OFFICE	MAJOR SUSPENSION - REMOVAL	REMOVAL	*	*
<b>F22</b>	REPORTING TO WORK UNDER THE INFLUENCE OF ANY INTOXICANT; UNFIT FOR DUTY	REMOVAL	*	*	*
<b>F23</b>	POSSESSION, CONSUMPTION, SELLING OR DISTRIBUTION OF ALCOHOL, ILLEGAL DRUGS, OR MISUSE OF PRESCRIBED DRUGS WHILE ON DUTY OR ON ODJFS PROPERTY	REMOVAL	*	*	*
<b>F24</b>	REFUSAL TO SUBMIT TO / FAILURE TO PASS A PROPERLY ORDERED DRUG OR ALCOHOL TEST	REMOVAL	*	*	*
<b>F25</b>	DISRUPTING THE WORK ENVIRONMENT BY HORSEPLAY OR PRACTICAL JOKES	WRITTEN - MINOR SUSPENSION	MEDIUM - MAJOR SUSPENSION	MAJOR SUSPENSION - REMOVAL	REMOVAL
<b>F26</b>	PHYSICAL ATTACK TO ANOTHER	REMOVAL	*	*	*
<b>F27</b>	VERBAL OR WRITTEN THREATS TO ANOTHER	MAJOR SUSPENSION - REMOVAL	REMOVAL	*	*
<b>F28</b>	VIOLATION OF ANY PROHIBITED CONDUCT AS DEFINED BY WORKPLACE VIOLENCE POLICY	MAJOR SUSPENSION - REMOVAL	REMOVAL	*	*
<b>F29</b>	INAPPROPRIATE RELATIONSHIPS FROM ONE EMPLOYEE TO ANOTHER	WRITTEN - MINOR SUSPENSION	MINOR - MEDIUM SUSPENSION	MEDIUM - MAJOR SUSPENSION	REMOVAL
<b>F30</b>	ANY FAILURE OF GOOD BEHAVIOR THAT MAY DISCREDIT, EMBARRASS, UNDERMINE, OR INTERFERE WITH THE MISSION OF ODJFS	WRITTEN - MINOR SUSPENSION	MINOR - MEDIUM SUSPENSION	MEDIUM - MAJOR SUSPENSION	REMOVAL

**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.

# Exhibit 3

Page 2 of 6

## 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. **CAVEAT: 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:

# Exhibit 3

Page 6 of 6

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

<b>Owning Entities</b>	<b>Address</b>	<b>Name (SME)</b>	<b>Phone/ Fax/ E-mail</b>
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

## **IPP.3922. Code of Responsibility**

### **IPMTL 0249**

July 25, 2014 - *Reviewed*

July 19, 2011 - *Revised*

May 9, 2003 - *Original*

**CLICK [HERE](#) to acknowledge that you have read, understand, and will comply with this policy.**

#### **I. PURPOSE:**

- A. To inform all ODJFS system users (ODJFS state employees, temporary service personnel, contractor personnel, county users, business partners, and external agencies) of their responsibility for maintaining the security of all personal information (hard-copy and electronic) to which they have access in the course of performing their work.
- B. To provide the revised form JFS 07078 - OHIO DEPARTMENT OF JOB AND FAMILY SERVICES CODE OF RESPONSIBILITY (see Appendix B) which describes the specific information and confidentiality requirements to which all ODJFS system users (ODJFS employees, temporary service personnel, contractor personnel, county users, business partners, and external agencies) must subscribe in order to gain access to ODJFS and specific State of Ohio computer systems.

#### **II. REFERENCE/AUTHORITY:**

##### A. REFERENCES

*Note: References to the Ohio Revised Code (ORC) can be accessed at the following website:*

<http://codes.ohio.gov/>.

1. Information Technology Policy ITP E.8, Use of Internet, E-mail and Other IT Resources, published by The Ohio Department of Administrative Services, dated March 19, 2008.
2. Internal Revenue Code, Section 7213 (a).
3. Ohio Revised Code (ORC) [5101.02](#), [5101.27](#) through [5101.31](#), [5101.99](#), [3107.17](#), [3107.42](#), [3107.99](#), [3121.894](#), [3121.899](#), [3121.99](#), [3125.08](#), [3125.50](#), [3125.99](#), [4141.21](#), [4141.22](#) and [4141.99](#)
4. Code of Federal Regulations: 45 CFR 160 and 164 (HIPAA-45 CFR164.501); 42 CFR 431.300 through 431.307; 5 USC 552a; 7 CFR 272.1(c)
5. Ohio Administrative Code (OAC) rules [4141-43-01](#) through [4141-43-03](#)
6. [IPP 3001](#) ODJFS Information Security
7. [IPP10002](#) Computer Usage and Information System Usage
8. [IPP 3925](#) ODJFS Data Access Policy
9. [IPP 10004](#) Incident Reporting
10. [IPP 8106](#) Research and Research Data Approval

##### B. AUTHORITY

This policy is established by order of the director, ODJFS, hereinafter referred to as director.

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 3922 ODJFS Code of Responsibility dated May 5, 2010.

# Exhibit 4

Page 2 of 3

## IV. SCOPE:

This procedure applies to all ODJFS system users as noted in Section I (A) of this policy.

NOTE: Requirements for county users, business partners, and external agencies also specified under Administrative Rule.

NOTE: County users, business partners, and external agencies must follow any applicable Ohio Administrative Code rules regarding data access. (Ohio Revised Code (ORC) - 1347.15)

## V. DEFINITIONS:

### A. County Local Security Coordinators

The County partner representative, as defined in the OIS Service Level Agreement, is the point of contact with the ODJFS OIS Access Control for all security issues.

### B. Office Information Services (OIS)

OIS is responsible for developing, maintaining, and supporting ODJFS applications. Access Control is a unit contained within the Bureau of Production and Operations, Office of Information Systems, which is responsible for provisioning and de-provisioning functions as they relate to application and data access.

### C. State Point of Contact

The state manager representative of an external entity or specific areas of ODJFS. The state manager is held accountable for the external users access to the internal ODJFS network and internal ODJFS applications. The state manager is responsible for notifying OIS Access Control of personnel changes and contract amendments/terminations/extensions with the external entity.

### D. External Entity

An external business partner or external sister agency requiring access to the ODJFS internal network and/or internal applications.

## VI. PROCEDURES:

A. All ODJFS system users (as noted in I.A.) must complete the JFS 07078 - ODJFS Code of Responsibility Any access to information about recipients of ODJFS benefits or services, or about ODJFS employees, that is collected and maintained on ODJFS or state computer systems is strictly limited to those purposes authorized by ODJFS, and as directly related to the system user's **official** job duties and work assignments **for, and on behalf of**, ODJFS and/or a federal oversight agency.

It serves several purposes:

1. The form provides the statement of understanding concerning the confidentiality and security of data and the acknowledgment of that statement by the individual.
2. It is used to establish or change access to specific ODJFS or State of Ohio systems for ODJFS system users (as noted in I.A.).

B. Any access to information about recipients of ODJFS benefits or services, or about ODJFS employees, that is collected and maintained on ODJFS or state computer systems is strictly limited to those purposes authorized by ODJFS, and as directly related to the system user's **official** job duties and work assignments **for, and on behalf of**, ODJFS and/or a federal oversight agency.

C. This form is completed for state employees when a new hire initially reports to the ODJFS Office of Employee and Business Services for in-processing. Upon completion of the form, the Human Resources (HR) representative will sign, then fax or email the JFS 07078 along with a Confirmation Letter to the OIS Access Control Unit. The Access Control Unit will grant a Novell Network, GroupWise and Confidential Personal Information (CPI) LOG Accounts and notify both the HR Representative and the employee's supervisor of the Novell Network ID.

- D. Change requests, including modifications to existing access, must be submitted using the JFS 07078 and be completed by the unit supervisor and sent to Access Control.
- E. If this system access request is originating from a county office, business partner, external agency, or specific areas of ODJFS; then it must be first directed to their Local Security Coordinator (Security Point of Contact) or State Point of Contact for signature approval. Then the JFS 07078 form along with a cover memo from the Local Security Coordinator or State Point of Contact detailing the system access requested shall be mailed, faxed, or emailed, to the Access Control Unit, Production and Operations, Office of Information Services at the address indicated on the information security web page:  
<http://innerweb/omis/InfoSecurity/InfoSecindex.shtml>.
- F. The responsibility for forwarding completed JFS 07078 forms and associated cover memos belongs to the State employee's supervisor, the county equivalent Local Security Coordinator (LSC), or designated State Point of Contact as listed above.
- G. If a specific copy of a completed and approved JFS 07078 form is needed, it may be requested through the Access Control Unit, Production and Operations, Office of Information Services.

**CLICK [HERE](#) to acknowledge that you have read, understand, and will comply with this policy.**

**VII. APPENDIXES:**

A. SUBJECT MATTER EXPERT

Owning Entity	Address	Name (SME)	Phone/ E-mail
OIS	4200 E. Fifth Ave. Columbus, OH 43219	Rick Copley, ODJFS Chief Security/ Privacy Officer	614-387-8126 (desk) Rick.Copley@jfs.ohio.gov
OIS	4200 E. Fifth Ave. Columbus, OH 43219	Corey Sines, Security Architect	614-387-8284 (desk) Corey.Sines@jfs.ohio.gov

B. ODJFS Code of Responsibility, [JFS 07078](#)

## IPP.5003. Outside Employment

February 20, 2004 - Original

Click [HERE](#) to acknowledge that you have read, understand, and will comply with this policy.

### I. PURPOSE/REASON:

- A. To require notification to ODJFS management when an employee is employed outside of the Agency. In addition, the policy provides the Agency's position compliance with federal, state, and local statutes by those that are self-employed or employ others in the course of outside employment.
- B. Acceptance of employment with ODJFS obligates an employee to give Agency job duties and scheduled hours priority over outside employment duties and hours. Employees may not accept or maintain any outside employment that would present a conflict of interest, interfere with regularly assigned Agency duties, or require the utilization of or derive benefit from state resources. Scheduled hours of outside employment cannot conflict in any manner with scheduled work hours at ODJFS.

### II. REFERENCES/AUTHORITY:

#### A. REFERENCE

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

1. Ohio Revised Code (ORC) 5101.02
2. ORC 102 et al
3. Ohio Administrative Code (OAC) 102 et al
4. [ODJFS-IPP 0003](#)
5. [ODJFS-IPP 2101](#)
6. ODJFS-IPP 4100
7. [ODJFS-IPP 10002](#)

#### 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:

No current policy exists regarding this matter.

### IV. SCOPE:

This policy applies to all ODJFS employees.

### V. DEFINITIONS:

For the purposes of this policy, OUTSIDE EMPLOYMENT is defined as any form of non-Agency employment or business relationship involving the provision of personal services by the employee. It **does not** include participating in the activities of a nonprofit, charitable, religious, public service, or civic organization, unless such activities involve the provision of professional services or are for compensation.

**NOTE:** Employment with certain nonprofit organizations could present an ethics law violation or a conflict of interest in that many nonprofits receive contracts and grants from ODJFS and if the ODJFS

# Exhibit 5

Page 2 of 3

employee is in a fiduciary role with or otherwise benefits from the nonprofit that does business with ODJFS, there could still be a conflict and ethics violation. (See section VI - E below.)

## VI. Policy:

- A. The work of the Agency takes precedence over other occupational interests. No ODJFS employee shall accept or continue outside employment that in any manner conflicts with the employee's approved work schedule or duties at ODJFS. This includes conflicting work hours as well as outside employment that impairs the ODJFS employee's mental or physical capacity to perform ODJFS work duties. Any employee seeking or involved in outside employment shall notify ODJFS in writing of such outside employment. Assumption of outside employment by an employee without notification to the Agency may subject the employee to disciplinary action.
- B. An employee's work hours will not be changed to accommodate outside employment.
- C. It is the responsibility of every employee, employer, or self-employed individual to conform to Federal, State, and Local statutes. An ODJFS employee involved in outside employment is expected to conform so as not to bring discredit upon himself or herself or the Agency. Failure of an ODJFS employee to pay any fees or taxes required of an outside employment that are subject to direct control ODJFS may be in violation of [ODJFS-IPP 0003](#), Standards of Employee Conduct, and may face disciplinary action.
- D. An employee may not use state resources for purposes other than state business as defined in various ODJFS policies. These include but are not limited to: [ODJFS-IPP 2101](#) Payment Card Program; ODJFS-IPP 4100 Telephone Usage; and [ODJFS-IPP 10002](#) Computer and Information Systems Usage.
- E. No ODJFS employee will participate in any outside employment that presents a conflict of interest, raises the appearance of impropriety, or violates state ethics laws. Questions concern these areas shall be addressed to the ODJFS Office of Legal Services (LEGAL@jfs.ohio.gov) or the Ohio Ethics Commission (<http://www.ethics.ohio.gov>).

## VII. PROCEDURES:

### A. NOTIFICATION

- 1. An employee seeking or involved in outside employment shall notify ODJFS in writing of such outside employment by completing and submitting a JFS 01793 Notification of Outside Employment form (See Appendix B)
- 2. The JFS 01793 is then submitted to the employee's supervisor or manager for review and signature. It will then be submitted for final review and acknowledgement by the office's deputy director. In either case, if there are any ethical concerns or questions about the employment, the manager/ supervisor and/or the deputy director should contact the Office of Legal Services.
- 3. The supervisor/manager will maintain the original form and forward a copy of the signed form to the Bureau of Human Resources (BHR) to be maintained in the employee's personnel record.

### B. CHANGES OF EMPLOYMENT

- 1. If there is a significant change in the outside employment status, the employee shall immediately notify the appropriate supervisor/manager.
- 2. The supervisor/manager will determine if a new Notification form is required.
- 3. In the case of termination of outside employment, the employee will notify management. Management will in turn notify BHR to remove Notification form from the personnel file.

Click [HERE](#) to acknowledge that you have read, understand, and will comply with this policy.

## VIII. APPENDIXES:

### A. SUBJECT MATTER EXPERT

Owning Entity	Address	Name (SME)	Phone/ Fax/ E-mail
Labor Relations	30 East Broad Street, 30th Floor, Columbus Ohio 43215	Labor Relations Staff	614-466-6514 614-752-6381 IPPM_STAFF@jfs.ohio.gov

B. JFS 01793 NOTIFICATION OF OUTSIDE EMPLOYMENT, [JFS 01793](#)

ODJFS

Fax 6147285938

Jun 27 2007 09:51am P002/002

OHIO DEPARTMENT OF JOB AND FAMILY SERVICES  
CODE OF RESPONSIBILITY

\* PLEASE PRINT \*

NAME: First, MI, Last Robert L. Lucks

Agency ODJFS Local Operations

Work Phone (330) 364-9777

County Tuscarawas

Date of Birth [REDACTED]

Work Unit One Stop

Social Security No. [REDACTED]

Supervisor Cheryl Stiles

AGENCY TYPE:  ODJFS  Non-ODJFS State  County  Local Govt.  Private/non-profit  Federal

Contract Employee Contract Company Name & Telephone No. \_\_\_\_\_

ACCESS REQUESTED: (Local Security Coordinator/Supervisor use only)

ODJFS network / email access  CRISE  SETS  FACSIS  MMIS

OTHER access:

Time Keep, SCOTI, Group Wise

Novell Container:

Existing RACF / Novell ID's:

PLEASE READ CAREFULLY

Security and confidentiality are a matter of concern for all users of the Ohio Department of Job and Family Services (ODJFS) information systems and all other persons who have access to ODJFS confidential data. Each person that is entrusted with an authorized ID to access ODJFS systems, holds a position of trust relative to this information and must recognize the responsibilities entrusted to him/her in preserving the security and confidentiality of this information. Confidentiality requirements contained in law include, but are not limited to: 45 CFR 164.501 et al HIPAA; ORC sections 2301.35, 5101.26, 5101.27, 5101.28, 5101.29, 5101.30; and OAC rules 5101:1-1-03 and 5101:1-29-071.

An authorized user's conduct either on or off the job may threaten the security and confidentiality of this information. It is the responsibility of every user to know, understand and comply with the following:

1. I agree to abide by the ODJFS Information Security policy and ODJFS Internet Usage Policies. These policies are available via the ODJFS InnerWeb or upon request, they will be provided by either your supervisor or the ODJFS Information Security Unit. It is the responsibility of the applicant requesting access to become familiar with these policies.
2. I will not make or permit unauthorized uses of any information in hard copy or computer files maintained by ODJFS.
3. I will not seek to benefit personally or permit others to benefit personally by any confidential information to which has come to me by virtue of my work assignment.
4. I will not exhibit or divulge the contents of any record to any person except in the conduct of my work assignment or in accordance with the policies of ODJFS.
5. I will not knowingly include or cause to be included in any record or report false, inaccurate or misleading information.
6. I will not remove or cause to be removed copies of any official record or report from any file from the office where it is kept, except in the normal conduct of my work assignment and in accordance with the policies of ODJFS.
7. I will not operate or request others to operate any ODJFS or Ohio Data Network equipment on personal business.
8. I will not violate rules and/or regulations concerning access and/or improperly use Security entry cards or codes for controlled areas.
9. I will not divulge or share any security codes (e.g., sign-ons, passwords, key card PIN, etc.) used to access any secured files.
10. I will report any violation of this code by anyone to my supervisor and / or the Information Security Unit immediately.
11. I will not aid, abet or act in conspiracy with another or others to violate any part of this code.
12. I will not load any personally owned software or software not licensed to ODJFS on any ODJFS-owned equipment without proper authorization.
13. I will treat all case record material as confidential, and will handle Income and Eligibility Verification System (IEVS) material with extra care. I understand that Internal Revenue Code Sections 7213(a), 7213A and 7431 provide civil and criminal penalties for unauthorized inspection or disclosure. These penalties include a fine of up to \$5000 and/or imprisonment of up to 5 years.

Any violation of this policy may result in disciplinary action pursuant to the agency work rules.

I have read, understand and will comply with the ODJFS Code of Responsibility for Security and Confidentiality of Data:

Applicant Signature

[Signature]

Date

26 Jun 07

Supervisor Signature

[Signature]

Date

26 Jun 07

1. Form Instructions: <http://innerweb/Omts/InfoSecurity/InfoSecindex.shtml>
2. Fax or Mail with cover memo detailing system access requested.  
To: ODJFS / BISS / Information Security Unit  
4200 E. Fifth Ave. Columbus, Ohio 43219-2551  
Fax #: (614) 995-0118

JFS 07078 (Rev. 4/2005)

