

---

---

## ACCESSING CONFIDENTIAL PERSONAL INFORMATION

---

---

**Subject:** Internal Management  
**Approval:** Commission Resolution 13-02

**Originally Issued:** 4/2013  
**Revised:**

---

### APPLIES TO

---

OFCC Employees and Contractors

---

### POLICY

---

This policy provides the requirements for protecting the privacy of people who have personally identifiable information in databases, electronic and paper files and other records maintained by the Ohio Facilities Construction Commission (OFCC). This policy applies to all OFCC employees and agents who gain access to OFCC physical facilities or data or computer systems. This policy lays out basic handling expectations first for all types of personally identifiable information, and second, it provides important additional handling requirements for sensitive personally identifiable information.

The Executive Director will determine the appropriate manner of ensuring that the following requirements on handling all personally identifiable information and handling sensitive personally identifiable information is provided to all OFCC employees and agents.

#### **I. Definitions**

For the purposes of this policy, “personally identifiable information” is information that can be used directly or in combination with other information to identify a particular individual. It includes:

- a name, identifying number, symbol, or other identifier assigned to a person
- any information that describes anything about a person
- any information that indicates actions done by or to a person
- any information that indicates that a person possesses certain personal characteristics

It includes “personal information” as defined by Ohio Revised Code (ORC) 1347.01. Some examples of personally identifiable information are:

- names
- Social Security numbers
- resumes
- correspondence
- addresses
- phone numbers
- driver’s license numbers
- state identification numbers
- professional license numbers
- financial account information
- medical and health information
- physical characteristics and other biometric information
- tax information
- education information
- individuals’ job classifications and salary information
- performance evaluations
- employment application forms
- timesheets

---

“Sensitive personally identifiable information” includes personally identifiable information that OFCC has discretion not to release under public records law, and it also includes “confidential personal information,” which OFCC is restricted or prohibited from releasing under Ohio’s public records law. Examples of “sensitive personally identifiable information” include:

- Social Security numbers
- a person’s financial account numbers and information
  - beneficiary information
- tax information
- employee voluntary withholdings
- passwords
- employee home addresses and phone numbers
- security challenge questions and answers
- employees’ non-state-issued email addresses
- medical and health information
- driver’s license numbers
- state ID card numbers (as issued by the Ohio Bureau of Motor Vehicles)
- confidential personal information, as defined below

“Confidential personal information” is personal information that falls within the scope of section 1347.15 of the Revised Code and that OFCC is prohibited from releasing under Ohio’s public records law. For OFCC, this specifically applies to Social Security numbers that may be in the following information systems maintained by the Commission:

Certified Payroll Reports – (paper-based and OAKS CI)

## **II. Access to Confidential Personal Information (CPI)**

OFCC employees and agents should access sensitive personally identifiable information only for a valid reason directly related to the exercise of an OFCC power or duty. Valid reasons include:

- Responding to a public records request;
- Responding to a request from an individual for the list of personally identifiable information the agency maintains on that individual;
- Administering a constitutional provision or duty;
- Administering a statutory provision or duty;
- Administering an administrative rule provision or duty;
- Complying with any state or federal program requirements;
- Auditing purposes;
- Carrying out or assisting with an authorized investigation or law enforcement purposes;
- Conducting or preparing for administrative hearings;
- Responding to or preparing for litigation, or complying with a court order or subpoena;
- Administering human resources, including but not limited to hiring, promotion, demotion, discharge, salary and compensation issues, leave requests and related issues, time card approvals and related issues;
- Administering an information system;
- Complying with an executive order or policy;
- 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; or
- Complying with a collective bargaining agreement provision.

---

OFCC employees and agents shall not access sensitive personally identifiable information for any reason other than those listed above. Examples of invalid reasons to access sensitive personally identifiable information include:

- for gain or personal profit,
- out of simple curiosity or personal interest,
- to commit a crime,
- for retribution, use in a personal conflict, or promotion of a personal point of view, or
- to harass or embarrass.

In the event of an invalid access, the OFCC Data Privacy Point of Contact must be made immediately aware of the specifics of the invalid access including all information compromised, dates and method of access, and responsible person(s) accessing the information. The Executive Director will authorize notifications to all affected parties of the compromise of CPI as soon as possible

### **III. Notice of Invalid Access**

Upon discovery or notification that confidential personal information of a person has been accessed by an employee for an invalid reason, the Executive Director will authorize notification to the person whose information was invalidly accessed as soon as practical and to the extent known at the time. However, the Executive Director will delay notification for a period of time necessary to ensure that the notification would not delay or impede an investigation or jeopardize homeland or national security. Additionally, the board 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 means the investigation of the circumstances and involvement of an employee surrounding the invalid access of the confidential personal information.

Once the Executive Director or the Executive Director's designee determines that notification would not delay or impede an investigation, OFCC will promptly disclose the access to confidential personal information made for an invalid reason to the person. The notification must inform the person of the type of confidential personal information accessed and the date(s) of the invalid access. Notification may be made by any method reasonably designed to accurately inform the person of the invalid access, including written, electronic, or telephone notice.

### **IV. Individual's Request for Confidential Personal Information**

Upon the signed written request of any individual for a list of confidential personal information about the individual that OFCC maintains, the Executive Director may designate an employee to do all of the following:

- Verify the identity of the individual by a method that provides safeguards commensurate with the risk associated with the confidential personal information;
- Provide to the individual the list of 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; and
- If all information relates to an investigation about that individual, inform the individual that the agency has no confidential personal information about the individual that is responsive to the individual's request.

---

## V. Restricting and Logging Access to Confidential Personal Information in Computerized Personal Information Systems

The following conditions apply to personal information systems that are computer systems and contain confidential personal information:

- **Access restrictions:** Access to confidential personal information that is kept electronically shall require a password or other authentication measure.
- **Acquisition of a new computer system:** When OFCC acquires a new computer system that stores, manages or contains confidential personal information, the system must include a mechanism for recording specific access by employees or agents to confidential personal information in the system.
- **Upgrading existing computer systems:** When OFCC modifies an existing computer system that stores, manages or contains confidential personal information, OFCC will determine whether the modification constitutes an upgrade. Any upgrades to a computer system must include a mechanism for recording specific access to confidential personal information in the system.

Logging requirements regarding confidential personal information in existing computer systems:

- a. OFCC shall require all employees and agents who access confidential personal information within computer systems to maintain a log that records that access.
- b. Access to confidential information is not required to be entered into the log under the following circumstances:
  - i. The employee or agent is accessing confidential personal information for official purposes, and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.
  - ii. The employee is accessing confidential personal information for routine office procedures and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.
  - iii. The employee comes into incidental contact with confidential personal information and the access of the information is not specifically directed toward a specifically named individual or a group of specifically named individuals.
  - iv. The employee accesses confidential personal information about an individual based upon a request made under either of the following circumstances:
    1. As part of processing a documented Public Records Request.
    2. As part of a request made by OFCC legal counsel.
- c. OFCC may choose the form or forms of logging, whether in electronic or paper formats.
- d. Log management. The Data Point of Contact shall develop procedures that includes the following:
  - i. Who shall maintain the log;
  - ii. What information shall be captured in the log;
  - iii. How the log is to be stored; and
  - iv. How long information kept in the log is to be retained.

## VI. Violations

Any OFCC employee who violates this policy is subject to disciplinary action up to and including termination.

Any OFCC employee who violates a confidentiality statute or administrative rule is subject to criminal charges, civil liability arising out of the employee's actions, employment termination and a lifelong prohibition against working for the State of Ohio.

---

Any violation of this policy by an agent of OFCC may be considered a material breach of the contract and may subject the contract to termination. Any agent who violates a confidentiality statute may also be subject to criminal charges and civil liability arising out of the agent's actions. The agent may also be subject to vendor or contractor debarment or both.