



CONFIDENTIAL PERSONAL INFORMATION POLICY

Purpose

The Ohio Department of Agriculture (ODA) is dedicated to ensuring the privacy and security of Ohio citizens who have personal information stored in systems maintained by ODA and controlling access to such information by its employees. To further these goals, ODA has adopted this Confidential Personal Information Policy.

Authority

O.R.C. Chapter 1347
O.A.C. Chapter 901-10

Scope

This Policy is applicable to all full-time and part-time permanent ODA employees and any contractors or temporary workers who perform services for ODA.

Definition

“Confidential personal information” (CPI) means personal information that is not a public record under the Ohio Public Records Law, specifically O.R.C. § 149.43.

Examples of CPI include:

- Social Security Numbers;
- Employee’s Home Addresses and Phone Numbers when in combination with and linked with an individual’s first name or first initial and last name;
- Driver’s license number or state identification number when in combination with and linked with an individual’s first name or first initial and last name; and
- Medical Information.

Please note that these examples are not intended to be a full list of what information is considered CPI. If you need additional information or clarification on what is CPI, please contact the Office of General Counsel at 614-728-6430.

Access to CPI

ODA provides employee access to CPI on a need-to-know basis. An employee’s access to CPI will be determined on a case-by-case basis depending upon the access required to perform his or her job duties. An employee’s access may be reassessed periodically and access may be modified as appropriate.

ODA’s Data Privacy Point of Contact shall work with the Chief Privacy Officer within the Office of Information Technology to maintain compliance with privacy protections for CPI.



Requesting CPI

An individual may request CPI about themselves upon a signed, written request and with verification of the individual's identity. The individual may receive relevant information that does not relate to an investigation about the individual or is otherwise not excluded from the scope of Ohio Revised Code Chapter 1347.

Valid Reasons for Authorized Employees to Access CPI

The following functions constitute valid reasons for authorized employees to access CPI:

- a. Responding to a public records request;
- b. Responding to a request from an individual for the list of CPI that ODA maintains on that individual;
- c. Administering a constitutional provision or duty;
- d. Administering a statutory provision or duty;
- e. Administering an administrative rule provision or duty;
- f. Complying with any state or federal program requirements;
- g. Processing or payment of claims or otherwise administering a program with individual participants or beneficiaries;
- h. Auditing purposes;
- i. Licensure, permitting, or registration processes;
- j. Investigation or law enforcement purposes;
- k. Administrative hearings;
- l. Litigation, complying with an order of the court, or subpoena;
- m. Human resource matters;
- n. Complying with an executive order or policy;
- o. Complying with an ODA 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
- p. Complying with a collective bargaining agreement provision.

Duty of Nondisclosure

Employees, through their normal work, may inadvertently or unintentionally come in contact with information that an employee knows or has reason to believe is CPI. In those circumstances, the employee has a duty not to disclose that information to anyone except properly authorized persons and should, if possible, take reasonable steps to protect that information from the risk of further inadvertent disclosure. For any questions regarding who is properly authorized to handle information, employees should contact the Data Privacy Point of Contact.

Logging Access to CPI

CPI that is kept electronically shall have security measures attached to its access. If the system has automatic logging capabilities, it will record who has accessed the CPI. Where the system does not have automatic logging capabilities, authorized employees who access the system must log or record their access. Access does not need to be logged under the following circumstances:

- 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.



- b. The access is to confidential personal information about an individual, and the access occurs as a result of a request by that individual for confidential personal information about that individual.

Logging access for systems that do not log access automatically shall be done in paper or electronic format, as appropriate for the system.

The logs for such systems shall contain:

- a. The name of the person accessing the CPI,
- b. The records reviewed, and
- c. The date of access.

The logs shall be periodically provided to the Data Privacy Point of Contact who shall maintain the logs and store them until audited by the Auditor of State and an audit report is released and all discrepancies are resolved.

Duty to Report Improper Access

If an employee suspects that CPI has been improperly accessed or disclosed, the employee has a duty to report the incident. The employee shall report the incident to either the Data Privacy Point of Contact or the Chief Privacy Officer within the Office of Information Technology. ODA shall then conduct an investigation.

Notice of Invalid Access

Upon a finding that CPI has been accessed by an employee for an invalid reason in violation of O.R.C. Chapter 1347 and this Policy, ODA will notify the individual whose information was invalidly accessed as soon as practical and to the extent known at the time. Where a notification could delay or impede an investigation or jeopardize homeland or national security, ODA may delay notification. ODA may also delay notification consistent with any measures necessary to determine the scope of the invalid access and to restore the reasonable integrity of the system. The notification may be made by any method reasonably designed to accurately inform the individual of the invalid access. Notification shall inform the individual of the type of CPI accessed and the date(s) of invalid access if known.

Personal Information

ODA also seeks to ensure that any personal information it collects, even if that information does not meet the threshold of CPI, is maintained appropriately.

“Personal information” means any information that describes anything about a person or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics.

Only personal information that is reasonably necessary and relevant to the functions of ODA shall be collected and maintained by ODA.

Handling Personal Information

The following apply to personal information collected and maintained by ODA. Employees should:

- a. Use personal information only for official, lawful purposes;



- b. Enter personal information accurately; and
- c. Take reasonable precautions to protect personal information from unauthorized modifications, destruction, use or disclosure.

No Retaliation

An employee who, in good faith, reports a possible improper access to CPI shall not be subject to retaliation.

Public Records

Nothing in this Policy shall restrict the release of public records, defined in O.R.C. § 149.43

Violation

Any violation of this Policy may result in disciplinary action in accordance with the ODA disciplinary grid and/or criminal prosecution under O.R.C. § 1347.99.

Contact

The Human Resources Director is available for questions or consultation regarding this Policy.

Revision History

Date	Description of Change
1/2016	Initial Policy Issued

