

# **Policy on Protecting Privacy**

Effective Date 07/2012  
Revised 02/2015 and 03/2017

## **PURPOSE**

To provide guidelines that Ohio Department of Higher Education (“ODHE”) staff and contractors must follow as they access personal information in ODHE systems.

## **APPLICABILITY**

This policy applies to all ODHE employees as well as to contractors who gain access to ODHE physical facilities and/or computer systems.

## **GENERAL POLICY**

While this policy addresses implementation of section 1347.15 of the Ohio Revised Code and Administrative Rules 3333-1-32 through 3333-1-32.4, the following general policies always apply:

- ODHE employees and contractors must only access confidential personal information (“CPI”) for a valid reason directly related to ODHE’s exercise of its powers or duties. Employees must not access CPI for any other reason. Example: Accessing information about people highlighted in media coverage, political figures, or other people of interest without a direct, pending business case with ODHE is prohibited.
- Employees and contractors are not to access CPI for personal profit or personal interest, to commit a crime or to harass or embarrass. Example: accessing information about family, friends, associates, or other people without a direct case-related need to know.
- Employees and contractors must not access personal information systems which they have not been authorized to access.
- As employees and contractors perform their work, they may inadvertently or unintentionally come in contact with information that they know or have reason to believe is CPI. In those circumstances, those employees and contractors have a duty not to disclose that CPI to anyone except properly authorized persons.
- Employees and contractors accessing a CPI system shall follow the privacy procedure specific to the office and to that system, if applicable, as well as the procedures contained in this Policy.
- Employees and contractors must not create a personal information system without proper ODHE authorization.

Statewide IT policies issued by the Department of Administrative Services shall continue to be followed, including but not limited to, the policy which states that ODHE shall promptly remove access rights of an employee to a system upon an employee’s termination or reassignment of duties.

## **SPECIFIC POLICY TO R.C. 1347.15:**

### Access requiring Logging:

Each ODHE employee or contractor who accesses or directs another ODHE employee to access CPI from a personal information system shall record that specific access whenever it is directed toward a specifically-named individual or a group of specifically-named individuals, unless such information or such access is otherwise exempted. Each employee shall manually record such access in the appropriate CPI Log maintained for each of the ODHE's personal information systems governed by this Policy (see below for a list of the personal information systems governed by this Policy), unless the system records the access automatically. A sample log is attached. All logs, whatever the form or format, shall contain all of the information/elements included in the sample.

Exempt from Logging: Consistent with section 1347.15 of the Revised Code and Administrative Rules 3333-1-32 through 3333-1-32.4, an employee or contractor is not required to log access to CPI that occurs as a result of the following:

1. An employee or contractor accesses an individual's CPI because the individual requests CPI about himself/herself.
  - a. Includes when the individual makes a request that ODHE take some action on that individual's behalf and accessing the CPI is required to consider or process that request.
2. An employee or contractor accesses CPI for official ODHE purposes, including research, and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.
3. An employee or contractor accesses CPI for routine office procedures and the access is not specifically directed toward a specifically named individual or group of specifically named individuals.
4. An employee comes into incidental contact with CPI and the access of the information is not specifically directed toward a specifically named individual or a group of specifically named individuals.

*Note re 2-4: If search parameters do not target a specifically named individual or group of named individuals, no logging is required. Examples: research that requires searching on everyone who is over 25 years of age, who earned credit in a certain course, or makes a certain salary range; or random audits of information received.*

Review of Logs: The ODHE data privacy point of contact shall coordinate all of following:

- A schedule for reviewing the logs for ODHE;
- A method to secure the logs;
- Disposal of the logs according to the approved record retention schedule.

Reporting improper access to CPI: Whenever an employee or contractor suspects that CPI has been improperly accessed, that employee or contractor shall report the incident according to the following procedures:

- An employee or contractor shall report a suspected improper access to any of the following:
  - The employee's supervisor, the designated ODHE data privacy point of contact, or ODHE legal counsel.
- Any employee to whom a report of a suspected improper access shall promptly inform all of the following:

- The relevant business unit/owner of the system, ODHE legal counsel, and ODHE data privacy point of contact, unless one or more of those listed are suspected of improperly accessing of CPI. The Director of Human Resources is an acceptable alternate.

The Chancellor, upon the advice of both ODHE legal counsel and the ODHE data privacy point of contact shall make the final determination on whether or not there has been an invalid access.

#### Notice to individual of improper access to CPI

- If the Chancellor determines CPI has been improperly accessed, the affected individual whose CPI has been accessed shall be notified promptly. Legal counsel shall approve the language in the notice that will be sent to the affected individual, and the data privacy point of contact shall send the notice.

#### Responding to request for CPI

- Whenever an individual requests information that ODHE maintains about the individual, employees shall follow the following procedures for responding to a request for a list of CPI:
  - Each employee receiving a request for a list of CPI ODHE maintains of the requestor shall verify the identity of the person making the request:
    - Signed,
    - In Writing, and
    - Proof of identity (each system may set forth requirements depending on the information contained in the system. The requirements may be a photo identification, social security number, or other acceptable forms of identification)
      - proof of authorization for attorneys, guardians, and people with power of attorney will be accepted when appropriate
  - Employee should consult with the General Counsel before releasing this information to the individual requesting it.
  - After the requestor's identity has been verified, the employee shall notify the ODHE data privacy point of contact and the data privacy point of contact shall verify the legitimacy of the request;
  - If the request is verified as legitimate, the data privacy point of contact shall request the supervisor of the system to direct the appropriate staff person to prepare the request.
  - After the request is processed, the employee preparing the request shall return it to the data privacy point of contact for review. Prior to the data privacy point of contact sending the information to the requestor, the information shall be reviewed by ODHE legal counsel or designee to ensure the information is not to be excluded under applicable law.

The information may be sent to the requestor in the manner determined by the Chancellor, or designated employee, as most reasonable and appropriate.

#### Penalty for violating CPI laws and this Policy:

Any employee who violates a confidentiality statute or ODHE's Ohio Revised Code 1347.15 implementing rules (3333-1-32 through 3333-1-32.4) 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 employee may result in disciplinary action up to and including removal.

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

An employee or contractor who complies in good faith with this policy is not subject to discipline under this policy.

**Definitions and list of systems:**

For the purposes of this Policy, a personal information system is a system of record that contains all of the following attributes:

1. It is a group or collection of records that are kept in an organized manner in either electronic or paper formats. (See the definition of "system" in ORC 1347.01(F))
2. It contains "personal information" which is a person's name or other identifier (such as SSN or driver's license number) associated with any information that describes anything about a person or indicates that a person possesses certain personal characteristics. (See the definition of "personal information" in ORC 1347.01(E))
3. Personal information is retrieved from the system by name or other identifier. (See the definition of "system" in ORC 1347.01(F))
4. ODHE has ownership of, control over, responsibility for, or accountability for that system of record. (See the definition of "maintains" in ORC 1347.01(D))

Therefore, this Policy applies to the following ODHE personal information systems:

- Higher Education Information System (HEI)
- State Grants and Scholarships (SGS)
- Ohio College Opportunity Grant (OCOG)
- Nurse Education Assistance Loan Program (NEALP)
- Ohio War Orphans Scholarship
- Choose Ohio First
- Course Equivalency Management System (CEMS)
- College Credit Plus
- Articulation and Transfer Clearinghouse (ATC)
- ABLElink
- Ohio Technical Center

The remainder of ODHE's personal information systems are exempted from the application of this Policy as the information contained within such systems do not meet definition of CPI and/or such systems are specifically exempted from the application of ORC 1347.15 under ORC 1347.01(F).

"Confidential Personal Information" for the purposes of this Policy is personal information that the law prohibits ODHE from releasing. Examples of personal information that fall within the scope of CPI collected and maintained by ODHE include, but are not limited to, the following:

- Social Security Numbers;
- Medical and health information;
- Benefit-related information; and
- Certain information relating to children and income tax information where that information has been voluntarily submitted by constituents.
- Federal Educational Rights and Privacy Act ("FERPA") information

“Access,” for the purposes of this Policy, means the retrieval of CPI from a personal information system by name or personal identifier so that CPI is viewed, or so that CPI is copied or retained outside of the personal information system.

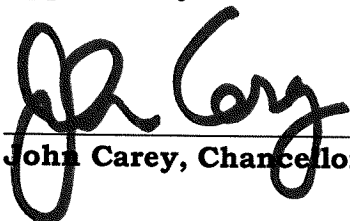
SAMPLE LOG:

<b>Information Recorded in Logs</b>	<b>Description</b>
<b>Name of the Personal Information System</b>	Name of the personal information system from which a person’s confidential personal information (CPI) is being viewed or otherwise retrieved by name or personal identifier.
<b>Date</b>	The date of the access. Note: The format should be standardized, such as DD-MM-YYYY or MM-DD-YYYY. “DD” means day; “MM” means month; and “YYYY” means year.
<b>Time</b>	The time of the access occurred (HH:MM for manual logs; HH:MM:SS for automated logs). Note: If the log is automated, it should capture U.S. Eastern Time as the default or Greenwich Mean Time with the offset. “HH” means hour; “MM” means minute; and “SS” means second.
<b>Name of the Employee Accessing CPI</b>	The name of the employee accessing or attempting to access CPI in the personal information system. Note: A system username is sufficient as long as the username is associated only with a single user who is the director, assistant director or deputy director accessing CPI directly or indirectly.
<b>Identification of the Person Whose CPI Was Accessed</b>	The name or identifier of the person whose CPI was accessed. Note: When possible, do not record identifiers that are considered confidential such as Social Security Number, but record an identifier that is not confidential.

**AUTHORITY & REFERENCE**

Ohio Revised Code Section 1347.15  
Ohio Administrative Code 3333-1-32 through 3333-1-32.4

Approved by:

  
\_\_\_\_\_  
John Carey, Chancellor

  
\_\_\_\_\_  
Date