OTTA Policy on Protecting Privacy

Purpose

The Ohio Tuition Trust Authority (OTTA) is dedicated to developing and implementing information access policies and controls that enhance and ensure the privacy and security of its customers who have information stored in OTTA's personal information systems. The purpose of this policy is to set for guidelines that OTTA staff and contractors must follow as they access personal information in OTTA systems.

Scope

This policy applies to all OTTA employees as well as to contractors who gain access to OTTA 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 3334-1-15 through 3334-1-19, the following general policies always apply:

- OTTA employees and contractors must only access confidential personal information (CPI) for a valid reason (see below) directly related to OTTA's exercise of its powers or duties. Employees must not access CPI for any other reason.
  - *Example*: You might appropriately access CPI because an Account Owner has called, emailed or mailed a letter to ask questions about his or her account or to give you instructions regarding his or her account. Additionally, you might appropriately access CPI when entering account application information into a database.
  - *Example*: You access CPI because someone was highlighted in media coverage or they are a political figure or just to satisfy your curiosity about someone without a valid reason. This or any other reason for accessing CPI without a direct, pending business case with OTTA 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 is prohibited.
- The OTTA system is programmed to permit access to limited information necessary for a specific employee or group of employees to perform his or her job duties and responsibilities. It is against policy to subvert OTTA's secure system to gain access to CPI you have no authority to view or to access a personal information system to which you have not been granted access.
  - *Example*: You are authorized to access CPI and your supervisor or someone else, who is not authorized to access to CPI, tells you to access the CPI of a customer without giving you a valid reason. Do not access the CPI, refuse the request and report the incident to Human Resources or General Counsel.
- 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.
  - *Example*: You stop by a co-worker's cubicle to talk and you see confidential personal information on their monitor.
- 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.
  - *Example:* All employees and contractors should lock their computers while gone from their desk and must use secure passwords.
- Employees and contractors must not create a personal information system without proper OTTA authorization.

- *Example:* No employee or contractor may create a duplicate system to circumvent these policies. Any duplicate system that is authorized by the agency and made subject to this Policy would be acceptable.

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 OTTA shall promptly remove access rights of an employee to a system upon an employee's termination or reassignment of duties.

Policy Specific to R.C. 1437.15:

Access requiring Logging:

Each OTTA employee or contractor who accesses or directs another OTTA employee or contractor 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 or contractor shall manually record such access in the appropriate CPI Log maintained for each of the OTTA'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, in whatever form or format, shall contain all of the information/elements included in the sample.

Exempt from Logging Requirement: Consistent with section 1347.15 of the Revised Code and Administrative Rules 3334-1-15 through 3334-1-19, 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 CPI because the customer requests CPI about himself/herself.
    a. This includes when the customer makes a request that OTTA take some action on their behalf and accessing the CPI is required to consider or process that request.
2. An employee or contractor accesses CPI for official OTTA 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 or contractor 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 requested a distribution in the last month; research that requires searching on everyone who makes a certain contribution level; or research to determine if statements are correct by spot-checking every so many statements.

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

- A schedule for reviewing the logs for OTTA;
- A method to secure the logs;
- Disposal of the logs according to OTTA's 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:

- Any employee or contractor shall report a suspected improper access to any of the following:

    - The employee's supervisor, OTTA's designated data privacy point of contact, or OTTA's In-House Counsel. The Executive Director, upon the advice of legal counsel and human resources, shall make the final determination of whether or not there has been a violation of this policy.
- Any employee or contractor to whom a report is made of a suspected improper access shall promptly inform all of the following:
    - The relevant business unit/owner of the system, the OTTA In-House Counsel, and the OTTA data privacy point of contact, unless one or more of those listed are suspected of improperly accessing CPI. The Director of Human Resources is an acceptable alternative.

The Executive Director, upon the advice of both OTTA's In-House Counsel and OTTA's data privacy point of contact shall make the final determination on whether or not there has been an invalid access.

Notice to the individual of improper access to CPI

- If the Executive Director determines that CPI has been improperly accessed, the affected individual whose CPI has been accessed shall be notified promptly. OTTA's In-House 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 a Request for CPI

If a customer or another individual wants to have a copy of all CPI OTTA keeps about that person, 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 OTTA maintains of the requestor shall verify the identity of the person making the request:
    - Signed,
    - In writing, and
    - Proof of identity (the relevant business unit/owner of 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
- After the requestor's identity has been verified, the employee shall notify the OTTA 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 OTTA's In-House 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 Executive Director, or designated employee, as the most reasonable and appropriate.

Penalties for violating CPI laws and this Policy:

Any employee who violates a confidentiality statute or OTTA's Ohio Revised Code 1347.15 implementing rules (3334-1-15 through 3334-1-19) 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 employee who violates this Policy is subject to termination 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. OTTA 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 OTTA personal information systems:

- Marketing/Prospect Database
- OTTA Web Database
- Ascensus/UNITE Database

The remainder of the OTTA's personal information systems are exempted from the application of this Policy as the information contained within such systems does not meet the 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 OTTA from releasing. ***Examples*** of personal information that fall within the scope of CPI collected and maintained by OTTA include, but are not limited to, the following:

- Names;
- Social security numbers;
- CollegeAdvantage account numbers;
- Driver's license numbers;
- Bank account numbers;
- Credit card numbers;
- Debit card numbers;
- Medical information (for proof of disability);
- Data classified as highly critical or confidential;
- Other personal information required by law to be maintained in a secure manner; or
- Account balances, earnings, distributions or any other account specific 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

A sample log of access is attached to this Policy. Other formats may be acceptable for logging access but must first be approved by the data privacy point of contact.

Authority & Reference
Ohio Revised Code Section 1347.15
Ohio Administrative Code 3334-1-15 through 3334-1-19

Approved by:

_____

Paul Paeglis, Executive Director

_____

Date

SAMPLE LOG

Ohio Tuition Trust Authority
Log of Access of Confidential Personal Information

Name of Personal Information System:	*OTTA Database or Marketing Database*
Name of Person Accessing Confidential Personal Information (CPI)	*Your Name*

Acknowledgment: I acknowledge that the information on this log is true and complete and that I have accessed CPI only for purposes relating to my job duties or my agency's governmental function. Initials *YN* Date *mm/dd/yy*

	Name (or identifier) of person whose CPI was accessed	Date	Time	Valid Reason for Access pursuant to OAC §3334-1-17*
1	*Customer Name*	*mm/dd/yy*	*hh:mm*	*3334-1-17(4)*
2				
3				
4				
5				
6				

***OAC 3334-1-17 Valid Reasons for Accessing CPI** (Logging is still necessary with a valid reason where not exempt; see policy above)

(A) Performing the following functions constitute valid reasons for authorized employees of the authority to access CPI:

(1) Responding to a public records request;
(2) Responding to a request from an individual for the list of CPI the authority maintains on that individual;
(3) Administering a constitutional provision or duty
(4) Administering a statutory provision or duty
(5) Administering an administrative rule provision or duty
(6) Complying with any state or federal program requirements
(7) Processing or payment of claims or otherwise administering a program with individual participants or beneficiaries
(8) Auditing purposes
(9) Investigation or law enforcement purposes
(10) Litigation, complying with an order of the court or subpoena
(11) Human resource matters (e.g., hiring, promotion, demotion, discharge, salary/compensation issues, leave requests/issues, …)
(12) Complying with an executive order or policy
(13) Complying with a policy of the authority or a state administrative policy issued by DAS, OBM or other similar state agency.

INSTRUCTIONS FOR COMPLETING SAMPLE LOG

Information Recorded	Description
Name of the Personal Information System	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.
Date	The date of the access. Note: The format should be standardized, such as DD-MM-YYYY or MM-DD-YYYY. "DD" means date; "MM" means month; and "YYYY" means year.
Time	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.
Name of OTTA's Employee Accessing CPI	The name of the senior official 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.
Identification of the Person Whose CPI Was Accessed	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.

Revised April 7, 2015.