Information Security Office (ISO)
25 S. Front Street
Columbus, Ohio 43025

Information Security Policy Data Protection and Privacy		
	Document No:	ISP-007
	Effective:	3/23/2011
	Published By:	Information Security Office
	Published Date:	3/23/2011
	Approved By:	Senior Leadership
	Replaces:	None

Purpose

In the course if its business, it is necessary for ODE to collect, store, process, transmit, and otherwise handle personal information about individuals. ODE is committed to protecting the privacy of the subjects with whose data we are entrusted. This policy states the intent of management to ensure that ODE practices are to be consistent with both generally accepted privacy standards and standard business practices.

Scope

The scope of this information security policy includes all employees, contractors, temporary personnel, and other agents of the Ohio Department of Education (ODE) who collect, process, store or otherwise uses ODE information assets.

This policy also applies to organizations that perform information-processing services on behalf of ODE.

Background

The Ohio Department of Education (ODE) supports the right to privacy, including the rights of individuals to control the dissemination and use of personal information that describes them, their personal choices, or life experiences.

Consistent with the Ohio Revised Code, Ohio Administrative Code and directives from the Governor's Office, ODE has developed policies and procedures designed to ensure that personal privacy is respected in all agency activities.

References

Governor's Management Directive Issued November 20, 2008

ORC Chapter 1347

ORC §149.43

Payment Card Industry Data Security Standard 1.2, October 2008

OAC 3301-2-5

OAC 3301-2-6

OAC 3301-2-7

OAC 3301-2-8

OAC 3301-2-9

OAC 3301-2-11

Glossary: A glossary of terms found in this policy is located in Section 8.0 - Definitions. The first occurrence of a defined term is in bold italics.

Policy

Collect only what is necessary: ODE will only collect the minimum amount of personal information necessary to achieve the stated purpose for the data collection effort.

Completeness, accuracy and timeliness of information: Personal information must be accurate and complete, and where necessary, kept up to date. Every reasonable step must be taken to ensure that personal information that is inaccurate or incomplete is definitively erased or corrected.

Data minimization: Personal information must not be kept in a form that permits identification of individuals for any longer than is necessary for the purposes for which the information was collected or for which it is further processed.

ODE Access to confidential personal information (CPI): Confidential personal information collected, stored or processed by the agency may only be accessed if all of the following apply:

a. Access is necessary to further a legitimate reason approved by the State Superintendent as being directly related to the agency's exercise of it powers or duties.

b. The person accessing the information has been authorized to access the specific information by an individual with authority to grant the access.

c. The access does not violate Ohio Administrative Code rules, State or Federal Law or any other policy issued by the agency.

Individual's Right of Access to Data: Individuals must be given an opportunity to examine, and issue complaints about inaccuracies in records containing their personal information. Investigations of complaints must be performed promptly, and must be answered with a letter informing the involved individuals about the courses of action that ODE will take. Any resulting modifications must be performed at no cost to the individual and within a reasonable period. Reasonable steps to prevent reoccurrence of the same inaccuracies must also be taken, for instance by adding an explanatory paragraph in the subject's file.

d. Every individual has the right to obtain the following from ODE unless that information relates to investigation records based upon specific statutory authority of the agency:

   i. Upon written request, a listing of the personal information about the individual that the agency keeps about the individual

   ii. Details as to the source of information about the individual, if such information is recorded

   iii. When appropriate, an indication that his or her personal data has been corrected, erased, or blocked because it was incomplete or inaccurate

   iv. If applicable, notification if the personal information of that individual was accessed inappropriately

Information to Be Given to the Individual: When collecting information about an individual, the agency must provide the individual with the following unless that information relates to investigatory records based upon specific statutory authority of the agency:

e. The purposes of the processing for which the data is intended

f. The policies related to handling personal data, including material changes to these policies that have gone into effect since the personal data was collected.

g. Whether replies to the questions are obligatory or voluntary and the possible consequences of the failure to reply. If replies are obligatory and they relate to the use of a SSN, the individual must be notified of the statutory provision requiring the submission.

h. The existence of the right of access to and the right to correct the data concerning the individual

i. Upon request, the Owner or his or her representative must provide all individuals with a brief written summary of the subject's rights to learn about, get copies of and correct personal information.

Disclosure of Confidential Personal Information to Third Parties: The following provisions govern the disclosure of confidential personal information.

j. Confidential personal information can and in most cases, should be released to the subject of the information or in the case of a minor's student records, to the parent or legal guardian of the subject, upon request. One notable exception to this is in the case of investigatory records such as those in the Office of Professional Conduct. Investigatory records should only be released when approved by the ODE information owner or the ODE Chief Legal Counsel.

k. ODE, through the Chief Legal Counsel, may provide third parties with personal information processed on its systems for reasons such as court orders, subpoenas and other reasons required by law.

l. The Office of Human Resources may also provide personal information to third parties for the purposes of employment verification, benefits compensation and other reasons specifically authorized by law. All recipients of such information must definitively identify themselves, certify in writing the legal and customary purposes for which the information is sought and certify that the personal data will be used for no other purposes.

    i. The Chief Legal Counsel must approve any other disclosure of confidential personal information prior to its release.

Disseminating student-level information: Student-level information is used throughout the agency to develop reports, evaluate programs and as the backbone of the accountability system. There are many occasions where the agency is asked to provide student-level information to outside parties. The following guidelines must be followed when disseminating student-level information outside of the agency to protect the privacy of the students.

m. Student-level information that would allow an individual student to be identified is to be considered restricted information under ISP-004 Data Classification Policy and should be labeled accordingly.

n. Student IDs are protected under both state and federal statute and except in some very specific circumstances must not be released.

o. When releasing or publishing reports containing student-level information, the agency will ensure that data have been de-identified to a point that would not permit a person in the school or its community who does not have personal knowledge of the relevant circumstance to identify a student with reasonable certainty. The following masking rules have been adopted by the agency for de-identifying student-level information.

    i. Cells of data containing less than 10 observations will show a „<10" label and resulting calculations will display a „NC" label

    ii. Cells showing percentages over 95% will show a „>95%" label

    iii. Cells showing percentages under 5% will show a „<5%" label

Any request for information outside of these guidelines must be approved by the Chief Legal Counsel's Office.

Processing Confidentiality and Security: The following provisions apply to all situations where personal information is being processed by or on behalf of the agency.

p. The Owner in collaboration with the information custodians must identify appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, unauthorized alteration, and unauthorized disclosure. These measures must be consistent with the standards and procedures issued by the Information Security Office.

q. The Owner or his or her designated representative must prepare a privacy impact assessment to determine the privacy implications of all significantly new or different uses of personal data. Such

an assessment must be completed before these uses take place, and must include all steps in the proposed processing, including access, storage, transmission and destruction. Such an assessment must include not only consideration of the risks, but also the security measures to be employed such as access controls, encryption, logs, data retention schedules, and data destruction procedures.

r. When developing and testing applications, developers must use fictional or sanitized personal data that preserves the essential characteristics of the data, but that does not expose confidential personal information.

s. Confidential personal information such as account numbers, social security numbers, taxpayer identification numbers, driver license numbers and state identification numbers issued by the Bureau of Motor Vehicles should not be displayed in applications in their full form. No more than first five (5) or last four (4) numbers should be displayed unless a specific exception has been authorized by Senior Leadership.

t. State employees, including contractors acting on behalf of the agency, access to applications, databases or files (either electronic or paper) containing confidential personal information must be logged so that every recent access to confidential personal information can be traced to a specific user.

u. Information owners must develop a process for regularly reviewing the access to systems or files in their control for unauthorized access.

v. When not in use, confidential personal information must be stored in encrypted form if held in a computer or network, or in locked file cabinets or similarly secured containers if held in paper, microfiche or other non-computerized form. When sent over public computer networks such as the Internet, personal data must be protected using encryption methods approved by the Information Security Office.

w. Confidential personal information should not be sent via email unless the data are encrypted using acceptable encryption algorithms. This applies to both internal and external email. Sending information that is partially redacted or obfuscated is acceptable.

x. When they are no longer needed, all copies of personal information, including those on backup tapes, must be irreversibly destroyed according to standards and procedures defined by ISP-006 Information Handling. A document describing the personal information destroyed and the Reasons for such destruction must be prepared for each destruction process, and promptly submitted to the relevant Owner. Permission to destroy personal information may be granted by the Information Owner, the Chief Information Officer or the Chief Legal Counsel and only if all legal retention requirements and related business purposes have been met.

y. ODE will not use externally meaningful identifiers as its own internal individual account numbers. For example, to prevent identity theft, ODE account numbers must never be equivalent to social security numbers, driver's license numbers or any other identifier that might be used in identity theft or fraudulent activities.

Penalties: Violation of this policy shall result in disciplinary action and may be a cause for termination as well as civil and or criminal actions.

Roles and Responsibilities

Information Owners: Owners must ensure that information they are responsible for is handled consistent with this policy.

Information Custodians: Must ensure that security requirements identified by owners or generally accepted privacy practices are implemented.

Information Users: Must take all reasonable precautions, including following all information security policies and procedures, to protect personally identifiable information they have access to from unauthorized disclosure.

Chief Legal Counsel: The Office of the Chief Legal Counsel must review and approve all MOUs or contracts for the release of personal information to third parties prior to said release.

Chief Information Security Officer (CISO): Annually, the information security officer must complete a privacy impact assessment form and have it posted on the agency Internet site by December 1 of each year. Further, the ISO must monitor compliance with the provisions of this policy working with Information Owners and Custodians.

Revision History

Version	Change Date	Author(s)	Section(s)	Description of Change and Comments
0	12/15/08	David Shaw	All	(original policy)
1	3/23/2011	Lori Denzer	All	Review of Original Policy & Add to Policy Site
2	12/27/2011	L. Denzer	All	Scan for ISO references

Next scheduled policy review: 7/31/2015

Definitions

Personal Information: 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 and that contains and can be retrieved from a system by a name, identifying number, symbol or other identifier assigned to a person.

Confidential personal information: Personal information that is not a public record for purposes of the Public Records Law. To be designated as CPI, the information must have a statute which makes the information confidential.

Processing of personal data or "processing": Any operation or set of operations performed on personal data, whether by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, combination, blocking, erasure or destruction.

Owner: The ODE manager or executive, who determines the purposes for processing personal data, and who makes decisions about the security mechanisms to be used to protect such personal data.

Custodian: Custodians are the person or persons responsible for the care, custody and control of information. Typically, members of the ODE ITO will serve as custodians for electronic information used by the agency. However, anyone who has direct control over information is a custodian.

Third party: Any person, partnership, corporation, public authority, government agency, or any other entity other than the individual, Owner, Custodian, and the persons who, under the direct authority of the Owner or the Custodian, are authorized to process the data.

Recipient: The person, public authority, government agency, or any other entity to whom personal data is disclosed.

Consent: Any freely-given informed indication of his or her wishes by which the individual signifies his or her agreement to have his or her personal data processed, which may include disclosure.

Super-users: Super-users are defined as either of the following:

a. Those users of a computer system who have access to system control, system monitoring or system administration functions such that they have access to all confidential personal information on all individuals maintained by the agency. Super-users include but are not limited to system administrators, information systems security officers, maintainers, system programmers who have access to these functions.

b. Any other state employee of the agency with access to all confidential personal information on all individuals maintained by the state agency whether that access is directly through a system or indirectly through a state employee of the agency.

Student-level information: Information presented which describes an individual student, actions taken by that student or actions done to that student.

Related Resources

Inquiries

Direct inquiries about this policy to:

Matt Williams
Chief Information Security Officer
25 S. Front Street, MSG05
Columbus, Ohio 43215

Telephone: 614.728.8105
Email: ODE.InfoSec@ode.state.oh.us

Attachments

None

Implementation

Management realizes that the implementation of the requirements in this policy may have significant fiscal impacts in addition to substantial code modification. For these reasons, the following implementation requirements are adopted.

12.1 Existing systems: Systems that are currently in production or so close to production that system modifications are impractical or cost prohibitive must facilitate the following:

a. Auditing or logging requirements in section 5.9 (e) must be implemented using a manual process which records the actions of each specific access unless such access is either of the following:

i. At the request of the individual who is the subject of the record(s) being accessed.

ii. Part of official routine office procedures or incidental contact with the information unless the conduct resulting in the access is specifically directed towards a named individual or group of individuals.

New systems or systems undergoing upgrades: Systems developed or upgraded after the effective date of this policy must include a mechanism for recording each specific access by employees of the state agency to confidential personal information.