Information Technology Policy **Data Protection and Privacy**	**Document No:**	ITP-007
	Effective:	12/7/2023
	Published By:	Information Technology Office

1.0 PURPOSE

In the course if its business, it is necessary for the Department of Education and Workforce to collect, store, process, transmit, and otherwise handle personal information. The Department supports the right to privacy, including a person's right 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, the Department has developed policies and procedures to ensure that personal privacy is respected in all Department activities.

A glossary of terms found in this policy is located in section 6 - Definitions. The first occurrence of a defined term is in ***bold italics***.

2.0 SCOPE

The scope of this policy includes Department computer and telecommunications systems and the employees, contractors, temporary personnel, and other agents of the Department who use and administer such systems. This policy also applies to organizations that perform information-processing services on behalf of the Department.

3.0 POLICY

3.1 Collecting personal information: The Department will collect the minimum amount of personal information necessary to achieve the stated purpose of a ***data*** collection. The following information must be provided during a data collection unless it relates to an investigation under a specific statutory authority of the Department:

a) The intended use of the data.
b) The policies the Department follows for handling personal data, including material changes to policies that become effective after the personal data is collected.
c) 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.
d) The existence of the right of access to and the right to correct personal data.
e) Upon request, a brief written summary of the person's rights to learn about,

get copies of, and correct personal information.

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

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

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

a) Access is necessary to further a legitimate purpose directly related to the Department's exercise of it powers or duties.
b) The person accessing the information has been authorized to access the specific information by a person 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 Department.

3.5 Personal right of access to data: Any person must be given an opportunity to examine, and issue complaints about inaccuracies in records containing their personal information.

3.5.1 Requesting data: Every person has the right to obtain the following from the Department unless that information relates to an investigation under a specific statutory authority of the Department:

a) A list of the personal information that the Department keeps about the person.
b) Details about the sources of information about the person if such information is recorded.
c) When appropriate, an indication that personal data has been corrected, erased, or blocked because it was incomplete or inaccurate.
d) If applicable, notification if personal information was accessed inappropriately.

3.5.2 Resolving complaints: Investigations of complaints must be performed promptly, must be answered in writing, and must inform the involved person about any course of action that the Department will take. Any resulting modifications must be performed at no cost to the requester 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.

3.6 Disclosure of Confidential Personal Information to Third Parties: Prior to its release to a ***third party***, the Chief Legal Counsel must approve the disclosure of confidential personal information if the release is not for a reason listed below.

3.6.1 Releasing student records to parents and guardians: Confidential personal information of a minor student may be released to the parent or legal guardian unless it relates to an investigation under a specific statutory authority of the Department:

3.6.2 Employment with the Department: 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.

3.7 Use of student level data: ***Student level data*** is used throughout the Department to develop reports, evaluate programs, and as the backbone of the accountability system. There are many occasions where the Department is asked to provide student-level information to outside parties. To protect the privacy of students, the following guidelines must be followed when using or providing student level data.

3.7.1 Confidentiality label: Student level data that would allow an individual student to be identified is to be considered Confidentiality High data under *ITP-004 Data Classification Policy* and should be labeled accordingly.

3.7.2 SSIDs: Statewide Student IDs (SSIDs) are protected under both state and federal statute and, except in some very specific circumstances, must not be released.

3.7.3 Data masking: When releasing or publishing reports containing student level data, the Department will ensure that data have been deidentified to a point that would not permit a person without personal knowledge of the relevant circumstances to identify a student with reasonable certainty. The following masking rules have been adopted by the agency for deidentifying student level data.

- Calculations based on less than 10 observations should display “<10” as the result. Where appropriate, additional labels such as “NC” for Not Calculated or “NR” for “Not Rated” can be used.
- Calculations resulting in a percentage under 5% should display as “<5%“

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

3.8 Use of personal information: The following provisions apply whenever confidential personal information is used by or on behalf of the Department.

3.8.1 Protecting CPI: The ***data owner***, in collaboration with the ***data custodians***, must identify appropriate technical and organizational measures to protect CPI data against accidental or unlawful destruction, unauthorized alteration, and unauthorized disclosure. These measures must be consistent with the standards and procedures issued by the state Office of Information Security and Privacy (OISP).

3.8.1.1 Non-computerized records: When not in use, non-computerized records with confidential personal information must be secured in locked file cabinets or similarly secured containers. Non-computerized refers to paper forms, printouts, microfiche, and similar "hard copy" media.

3.8.1.2 Data at rest: Electronic records stored on a disk (PC, laptop, server, or network drive) or in cloud storage must be encrypted in accordance with the Department's encryption policy.

3.8.1.3 Data in transit: Electronic records transmitted over a computer network, including the internet, must be encrypted during transmission in accordance with the Department's encryption policy. Note that this disallows using standard email to transmit CPI, but documents where the CPI has been properly redacted is allowed.

3.8.2 Privacy Impact Assessments: The data owner designee must prepare a privacy impact assessment (PIA) to determine the privacy implications of all significantly new or different uses of personal data. This includes, but is not limited to, creating a new application or function in an existing application that stores or processes CPI. A PIA must be completed before the data is used and must include all steps in the proposed ***processing***, including plans for access, storage, transmission, and destruction. A PIA must demonstrate consideration of the risks of using the CPI and describe the security measures to be employed such as access controls, encryption, logs, data retention schedules, and data destruction procedures.

3.8.3 Developers and CPI: When developing and testing applications, workflows, or reports, the developers must use fictional or sanitized personal data that preserves the essential characteristics of the data necessary to create the product but that does not expose CPI to the developers.

3.8.4 Masking CPI: CPI such as account numbers, social security numbers or taxpayer identification numbers, or driver's license or state identification numbers issued by the Bureau of Motor Vehicles, should not be displayed in applications in their full form. No more than the first five or last four characters should be displayed unless a specific exception has been authorized by the data owner. Any exceptions should be noted in the privacy impact assessment.

3.8.5 Logging access to CPI: When a state employee or contractors acting on behalf of the Department accesses CPI in an application, databases, or files (whether electronic or paper), the access must be logged so that every recent access to confidential personal information can be traced to a specific user. Data owners are responsible for reviewing these logs to control unauthorized access of CPI.

3.8.6 External identifiers: The Department shall not use externally meaningful identifiers as its own internal individual account numbers. For example, to combat identity theft, Department account numbers must never be equivalent to social security numbers, driver's license numbers, or any other identifier considered CPI and that could be used for fraudulent activities if improperly accessed.

3.9 Destruction: When appropriate based on the records retention considerations, all copies of personal confidential information must be destroyed according to the Department's Data Handling policy. Where required, a destruction document or record describing the personal information destroyed and the reasons for the destruction must be prepared and promptly submitted to the Department's records manager. Permission to destroy confidential personal information may be granted by the data owner, the Chief Information Officer, or the Chief Legal Counsel if all legal retention requirements and related business purposes have been met.

4.0 PENALTIES

Violation of this policy shall result in disciplinary action and may be a cause for termination, civil penalties, and criminal prosecution.

5.0 ROLES AND RESPONSIBILITIES

5.1 Data owners: Responsible for data they are responsible for is handled consistent with this policy.

5.2 Data custodians: Responsible for ensuring that security and privacy requirements identified by data owners or generally accepted privacy practices are implemented.

5.3 Data users: Must take all reasonable precautions, including following all information security policies and procedures, to protect confidential personal information they have access to from unauthorized disclosure.

5.4 Chief Legal Counsel: The Office of the Chief Legal Counsel reviews and approves all MOUs or contracts involving the release of personal information to third parties.

5.5 Information Security Officer: Responsible for working with data owners to create privacy impact assessments and for maintaining the Department's library of privacy impact assessments. Also monitors compliance with the provisions of this policy by data owners and custodians.

6.0 DEFINITIONS

Confidential personal information (CPI): Personal information that is not a public record according to public records law. To be designated as CPI, the information must have a statute which makes the information confidential.

Data: Coded representation of quantities, objects and actions. The word "data" is often used interchangeably with "information".

Data owner: The person who determines the appropriate use and purposes for accessing or processing data, and who makes decisions about the security mechanisms to be used to protect such data.

Data custodian: The person responsible for the care, custody, and control of data. Typically, members of the ITO will serve as custodians for electronic data used by the Department. However, anyone who has direct control over data is a custodian.

Personal information: Any information that describes anything about a person, such as personal characteristics or actions taken by or on behalf of a person; and that can be retrieved from a system by a name, identifying number, symbol, or other identifier assigned to the person.

Processing: Any set operations performed on data, including by automated 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.

Student level data: Data which describes an individual student, actions taken by that student, or actions done to that student.

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

7.0 REFERENCES

7.1 ITP-004: Data Classification Policy
7.2 ITP-008: Encryption Policy
7.3 Ohio Revised Code chapter 1347
7.4 Ohio Administrative Code section 3301-02
7.5 Family Educational Right to Privacy Act

8.0 INQUIRIES

Direct inquiries about this policy to:

Information Technology Office
25 S. Front Street MSG05
Columbus, Ohio 43215
Email: ITOServiceDesk@education.ohio.gov

All Department information technology policies are located on the intranet at https://ohiodas.sharepoint.com/sites/EDU-Intranet/SitePages/Policies.aspx.

9.0 REVISION HISTORY

Change Date	Description of Change and Comments
03/20/2008	Original policy
03/23/2011	Policy review
12/7/2023	Updated for agency transition to the Department of Education and Workforce.