AGENCY POLICY

Office of Superintendent of Public Instruction

POLICY TITLE	**Data and Information Handling and Disposal**		
NUMBER	TE-010	**EFFECTIVE**	June 16, 2020
APPLIES TO	All OSPI Employees and Contractors	**CONTACT**	Chief Information Officer

[Original Effective Date: 10/27/14]

PURPOSE

The Office of Superintendent of Public Instruction (OSPI) collects, creates, and maintains large amounts of data and information in order to provide educational services and to comply with state and federal requirements. Data must be appropriately managed across the entire data life-cycle, from the time it is captured to the time it is destroyed. Data and information can be in electronic or paper form.

This policy prescribes the methods for handling and disposing of data and information.

DEFINITIONS

Category 3 and 4 – Confidential Data/Information

Data that carry the risk for adverse effects from an unauthorized or inadvertent disclosure. This includes any negative or unwanted effects experienced by an individual whose personally identifiable information (PII) from education records was the subject of a loss of confidentiality that may be socially, physically, or financially damaging, as well as any adverse effects experienced by the organization that maintains the PII. See *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, 2010, NIST Special Publication 800-122, for more information.

Education Records

Records that are directly related to a student and are maintained by an educational agency or institution or by a party acting for the agency or institution. For more information, see the Family Educational Rights and Privacy Act regulations, 34 CFR § 99.3.

Encryption

The process of transforming information using a cryptographic algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as an encryption/decryption key. “One way” encryption is a data destruction technique which makes use of encryption techniques to render data unusable by first encrypting the data and then destroying the key used to encrypt the data initially.

Personally Identifiable Information (PII)

PII from education records includes information, such as a student’s name or identification number that can be used to distinguish or trace an individual’s identity either directly or indirectly through linkages with other information. See Family Educational Rights and Privacy Act regulations, 34 CFR § 99.3, for a complete definition of PII specific to education records and for examples of other data elements that are defined to constitute PII.

Sanitization of the Media

A process which is applied to data or storage media to make data retrieval unlikely for a given level of effort. *Clear*, *Purge*, and *Destroy* are actions that can be taken to sanitize data and media.

POLICY

The Washington State Office of the Chief Information Officer (OCIO) directs agencies to classify information based on the sensitivity of data and information into categories (OCIO Policy/Standard 141/141.10). The four categories from the OCIO are:

- Category 1—Public Information
- Category 2—Sensitive Information
- Category 3—Confidential Information
- Category 4—Confidential Information Requiring Special Handling

The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the confidentiality of student information. FERPA protects personally identifiable information (PII) from students’ education records from disclosure without written consent from the parent or “eligible student” (a student who is 18 years of age, or who is attending a post-secondary institution), unless an exception to that consent requirement applies. PII within a student record, as described by FERPA, is Category 4 data.

While Category 1 data like finance, directory, and aggregated data are often provided on the OSPI website, Category 3 and 4 data must be properly secured. Category 2-Sensitive Information like educator data should not be released unless specifically requested through the public disclosure process. Certain educator data such as social security numbers, home addresses, home phone numbers, and home email addresses are protected by law.

OSPI must comply with applicable state and federal laws, rules, regulations, and policies related to maintaining and handling Category 4 data, including but not limited to:

- Personal information as defined in RCW 42.56.590 and RCW 19.255.10.
- Information about public employees as defined in RCW 42.56.250.
- Lists of individuals for commercial purposes as defined in RCW 42.56.070.
- Information about the infrastructure and security of computer and telecommunication networks as defined in RCW 42.56.420.
- Proper and secure maintenance of education records. FERPA: 34 C.F.R. §99; RCW 42.56; RCW 28A.605.030; WAC 392-500.
- Social Security Number Protection Act Pub.L. 111-318.
- Proper and secure maintenance of testing material, RCW 28A.635.040; WAC 181-87-060.

Below are each information class and the guidelines that help create understanding with regard to information behaviors concerning the safekeeping and disclosure of some information that is regulated by state and federal laws.

Information classifications

Category	Name	Characteristics
1	**Public Information**	Information that can be or currently is released to the public. It does not need protection from unauthorized disclosure but does need integrity and availability protection controls.
2	**Sensitive Information**	May not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.
3	**Confidential Information**	Information that is specifically protected from either release or disclosure by law.
4	**Confidential Information Requiring Special Handling**	Information that is specifically protected from disclosure by law and for which: a. Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements. b. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

Category 1—Public Information

Public information is information that OSPI can release to the public. It is information that is published by the agency for general distribution.

Public information must be authorized for publication and protected from unauthorized changes. The protection of public records is cited in RCW 42.56.100. Some examples of public information include:

- Data on the OSPI Report Card.
- Business forms.
- Business brochures.
- Aggregate program information; for example:
  - Vendor agreements.
  - Non-security IT information.
  - Request for Quotation/Proposal (RFQ/RFP) documents.

Prohibited Activities:

- Changing public information without agency consent.

Required Safeguards:

- Information is labeled and handled according to agency policy.
- Information has passed all data quality checks.

Category 2—Sensitive Information

Sensitive information is business critical information OSPI uses to carry out its mission. Sensitive information can be released to the public, subject to the public disclosure process. It is information for which there is no exemption by state or federal law allowing nondisclosure to the public. Internal use of sensitive information should be restricted to an "as needed" basis and should be protected from unauthorized changes. Some examples of sensitive information include:

- Employment information.
- Internal telephone books and directories.

Prohibited Activities:

- Unauthorized access.
- Unauthorized deletion or changes.
- Unauthorized disclosure.
- Posting on public websites.

Required Safeguards:

- Stored on secured servers only.
- Internal use on an "as-needed" basis.
- Protection to prevent loss of information, theft, or unauthorized access.
- Controlled through the public records process to ensure proper release of information.

Category 3—Confidential Information

Confidential information is information OSPI cannot release to the public. It is information that is specifically protected by either state or federal law, exempting it from disclosure. Confidential information must be protected from unauthorized disclosure or change.

Confidential information generally includes:

- Testing materials and scores.
- Aggregate student information that is not suppressed according to suppression rules.
- IT security information that, if released, could jeopardize the integrity of data or result in fraud or unauthorized disclosure or modification of information.
- Other common exempt records as found here.

Prohibited Activities:

- Disclosure of confidential information.

- Posting on any public website.

Required Safeguards:

- Must be stored on secured servers only.

Category 4—Confidential Information Requiring Special Handling

Confidential information requiring special handling is information that OSPI cannot release to the public and for which additional protections need to be in place. This information includes:

- Information for which either state or federal laws or regulations require protection or dictate particular handling requirements.
- Information that is covered by a contract or agreement in which specific and strict handling requirements are set forth.
- Information for which serious consequences can arise from unauthorized disclosure ranging from life threatening action to legal sanctions.
- Personally Identifiable Information (PII) of students. (See Also: OSPI's Student Data Confidentiality policy)

Prohibited Activities:

- Transmitting over unsecure channels or viewing with unsecure applications, including regular email that is not encrypted.
- Posting on public websites.
- Unauthorized release of information to the public.

Required Safeguards:

- Storage on secured servers only.
- If emailed, use encryption software.
- Student records that are de-identified, containing PII, and/or records with Research IDs are provided only to external organizations with an approved OSPI data sharing agreement.
- Training for appropriate handling of this information is required.
- Information must be expunged from hard disks before servers or hard disks are surplused.

OSPI Data Share Agreements

When sharing Category 3 and 4 data outside the agency, an agreement must be in place unless otherwise prescribed by law. In OSPI, we typically call these Data Share Agreements and these agreements require specific components according to the OCIO:

- The specific data that will be shared.
- The specific authority for sharing the data.
- The category of the data shared.
- Access methods for the shared data.
- Authorized users and operations permitted.
- Protection of the data in transport and at rest.
- Storage and disposal of data no longer required.
- Backup requirements for the data if applicable.
- Other applicable data handling requirements (e.g. FERPA requirements).

Data share agreements with third parties must include provisions that specify all PII and Category 3 and 4 information provided to the third party must be destroyed when no longer needed for the specific purpose for which it was provided, including any copies of the PII and Category 3 and 4 data that may reside in system backups, temporary files, or other storage media. Depending on the sensitivity of the data being shared, be specific in the written agreement as to the type of destruction to be carried out.

Ensure accountability for destruction of PII and Category 3 and 4 information by using certification forms which are signed by the third party individual responsible for performing the destruction and contain detailed information about the destruction. The contract manager overseeing the data share agreement must conduct periodic audits.

Data Disposal Procedures

All media containing sensitive or confidential data must be secured per the OSPI Data and Information Handling and Disposal policy, Technology Acceptable Use policy, Release of Public Records policy, Records Management policy and procedure, and the Confidentiality of Student Data policy.

Contact the OSPI Helpdesk when unsure about data destruction.

For workstations and printer data scheduled for surplus follow these steps:

1. OSPI Helpdesk receives computers no longer in use by OSPI and reviews them for components that can be recycled and used further in other machines.
2. OSPI Helpdesk runs wiping software to erase data from the drives on the machines and then sends them to OSPI Agency Support.
3. Computers that do not respond to wiping software or take an unreasonable amount of time will have the hard drive removed and destroyed prior to leaving the building.
4. OSPI Agency Support sends all erased machines and drives to surplus.

PII and Category 3 and 4 information may also be present in non-electronic media. OSPI must manage non-electronic records in a similar fashion to electronic data. When data are no longer required, destroy non-electronic media using secure means to render it safe for disposal or recycling by using cross-cut shredders and/or secured recycling bins.

When destroying electronic data, use appropriate data deletion methods to ensure the data cannot be recovered. The simple deletion of the data or file is not effective. Often, when a data file is deleted, only the reference to that file is removed from the media. The actual data remain on the disk and are available for recovery until overwritten.

Do not use file deletion, disk formatting, and "one way" encryption to dispose of sensitive data—these methods are not effective because they leave the majority of the data intact and vulnerable to being retrieved by a determined person with the right tools.

Destroy CDs, DVDs, and any magneto-optical disks by pulverizing, cross-cut shredding, or burning.

Address in a timely manner, sanitization of storage media which might have failed and need to be replaced under warranty or service contract. A data breach may result from storage media containing sensitive information being returned to the manufacturer for service or replacement.

APPROVED	
Chris P.S. Reykdal	6/16/20
Superintendent's Signature	Date Signed