COMMUNITY AND TECHNICAL COLLEGES
Washington State Board

DATA CLASSIFICATION GUIDELINES

DATA GOVERNANCE COMMITTEE
WASHINGTON COMMUNITY AND TECHNICAL COLLEGES
NOVEMBER 2025

TABLE OF CONTENTS

Overview

These data handling guidelines serve as operational support of ctcLink data classifications. These guidelines provide the necessary steps to securely manage, store, and transmit data, as well as a decision tree to help guide the classification of new data collected in ctcLink.

When combining data elements from different classifications, the dataset assumes the highest classification level. For example, if the dataset includes the student's name (Category 2) and SSN (Category 4), the dataset is considered Category 4.

These guidelines are intended for data which is, or could be, stored in ctcLink, but may be useful for classifying other externally held data.

Disclaimer

This document is intended to provide general guidance and best practices for handling data within the Washington Community and Technical College system. It does not replace or supersede any official policies or regulations. Each college remains fully responsible for ensuring compliance with all applicable state and federal data classification and encryption policies. Users should consult the relevant authoritative sources (see Appendix A) and institutional policies to ensure proper data handling and security practices are followed.

Category 1 – Public Information

WaTech SEC-08-01-S Definition

Public information is 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.

Regulatory Reference: WaTech Data Classification Standard

ctcLink Definition

Any public information that does not identify an individual student, employee (excluding class instructors), customer or vendor such as a college's program offerings, class catalog, retirement benefits offered or summary level financial statements.

- All Category 1 data share the same security needs and requirements.

Managing

- Category 1 data does not include information about students or employees, with the exception of instructors.
- Category 1 data may be provided publicly, included in emails or posted on public websites.
- Category 1 data does not need protection from unauthorized disclosure but does need integrity and availability protection controls. Integrity and availability protection controls include a review of the data by appropriate staff before it is shared.

Storing
Category 1 data does not require encryption at rest.

- Regulatory Reference: WaTech Encryption Standard

Transmitting
Category 1 data does not require encryption in transit.

- Regulatory Reference: WaTech Encryption Standard

Category 2 – Sensitive Information

WaTech SEC-08-01-S Definition
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.

Regulatory Reference: WaTech Data Classification Standard

ctcLink Definition
Information that is considered for official use only and may be shared publicly when requested without the consent of the student, employee, customer or vendor.

Refer to the ctcLink Data Classification Workbook for specific data classified as Category 2

All Category 2 data share the same security needs and requirements **with the exception of**:

- The combination of EMPLID and Name
  - When EMPLID and Name are combined, the combination becomes Category 3 and must follow the guidelines for Category 3 data
- Student directory information when a FERPA block has been requested
  - If the student has requested a FERPA block, the information becomes Category 3 and must follow the guidelines for Category 3 data
  - FERPA directory information is described in the ctcLink Data Classification Workbook
- Employee public information when data protection has been requested
  - If the employee has requested data protection, the information becomes Category 3 and must follow the guidelines for Category 3 data

Managing
Category 2 data do not need protection from unauthorized disclosure but does need integrity and availability protection controls. Integrity and availability protection controls include a review of the data by appropriate staff before it is shared.

Storing
- Category 2 data is not required to be encrypted at rest.
  - Regulatory Reference: WaTech Encryption Standard
- Best practice is to encrypt all Category 2 data at rest because it can include student or employee level information. All data stored within ctcLink is encrypted at rest.

Transmitting

- Data is only released to the public upon request and does not require consent from the student or employee.
- Data should not be provided/transmitted if the student has requested a FERPA block.
  - Regulatory Reference: SBCTC Policy Manual Chapter 3.30.10
- Data should not be provided/transmitted if the employee asked for data protection.
  - Regulatory Reference: RCW 42.56.250

Category 3 – Confidential Information

Data not classified as Category 1, 2 or 4 is considered Category 3.

All Category 3 data share the same security needs and requirements.

WaTech SEC-08-01-S Definition

Confidential information is information specifically protected from disclosure by law. It may include, but is not limited to:

a) Personal information about individuals, regardless of how that information is obtained.

b) Information concerning employee personnel records.

c) Information regarding IT infrastructure and security of computer and telecommunications systems.

Regulatory Reference: WaTech Data Classification Standard

ctcLink Definition

Information specifically protected from release or disclosure by law or contains information concerning the infrastructure and security of computer and telecommunication networks.

This includes, but is not limited to:

- Combination of EMPLID and Name RCW 42.56.590
- Non-public personal information as defined in RCW 42.56.590
- FERPA directory information if a FERPA block has been requested SBCTC Policy Manual Chapter 3.30.10
- Public employee information if data protection has been requested RCW 42.56.250
- Non-public personal Information about public employees as defined in RCW 42.56.250
- Information about the infrastructure and security of computer and telecommunication networks as defined in RCW 42.56.420
- All Category 3 data share the same security needs and requirements

Managing

Restrict access to only designated individuals at the educational institutions who will use the data and information only while performing their official duties.

Storing

- Category 3 data must be encrypted at rest. All data is encrypted while at rest within ctcLink.
  - Regulatory Reference: WaTech Encryption Standard
- Data must be stored using encryption algorithms from FIPS 140-3 Security Requirements for Cryptographic Modules.
- Encryption algorithms are used in such a way that the data becomes unusable to anyone but authorized personnel.
- Encryption keys or other means to decipher the information must be protected from unauthorized access.

Transmitting

- Category 3 data must be encrypted in transit.
  - Regulatory Reference: WaTech Encryption Standard
- Category 3 data should never be included in unencrypted emails or unencrypted communications
  - If you are unfamiliar with the encryption methods of your college, please contact your IT Department to ensure compliance.
- Category 3 data should only be included in data extracts shared with external parties or integrated with third-party applications when a data sharing agreement or contractual language specifically addressing data sharing is in place and at a minimum includes:
  - The purpose and specific authority for sharing the data
  - Description of the data including the classification
  - Time period of the agreement
  - Authorized uses
  - Authorized users
  - Protection of data in transit
  - Secure storage requirements
  - Data retention and disposal responsibilities
  - Backup requirements if applicable
  - Incident notification and response
  - FERPA exemption if applicable

Regulatory Reference: WaTech Data Sharing Policy

Category 4 – Confidential Information Requiring Special Handling

WaTech SEC-08-01-S Definition

Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:

a) Especially strict handling requirements are dictated, such as statutes, regulations, agreements, or other external compliance mandates.
b) Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

Regulatory Reference: WaTech Data Classification Standard

ctcLink Definition

Data that requires especially strict handling dictated by statutes, laws or regulations or if serious consequences arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

- All Category 4 data share the same security needs and requirements
- Refer to the ctcLink Data Classification Workbook for specific data elements classified as Category 4

Managing

- Access is provided only to authorized individuals who require access to perform their job duties
- Access must be monitored for accountability and effectiveness
- Requires unique ctcLink security and query roles
- Category 4 data will be masked on ctcLink pages. Any user requiring access to unmasked category 4 data on the page will need to be assigned the appropriate security role
- For access to queries that include Category 4 data, a specific role needs to be applied to the user, otherwise the user will not see or be able to execute the query
- Included in the dataLink metadata data classification table
- Yes/No indicators (such as a Student Group) that do not provide details are considered Category 3, not Category 4

Storing

- Category 4 data must be encrypted at rest. All data is encrypted while at rest within ctcLink.
  - Regulatory Reference: WaTech Encryption Standard
- Data must be stored using encryption algorithms from FIPS 140-3 Security Requirements for Cryptographic Modules
- Encryption algorithms are used in such a way that the data becomes unusable to anyone but authorized personnel

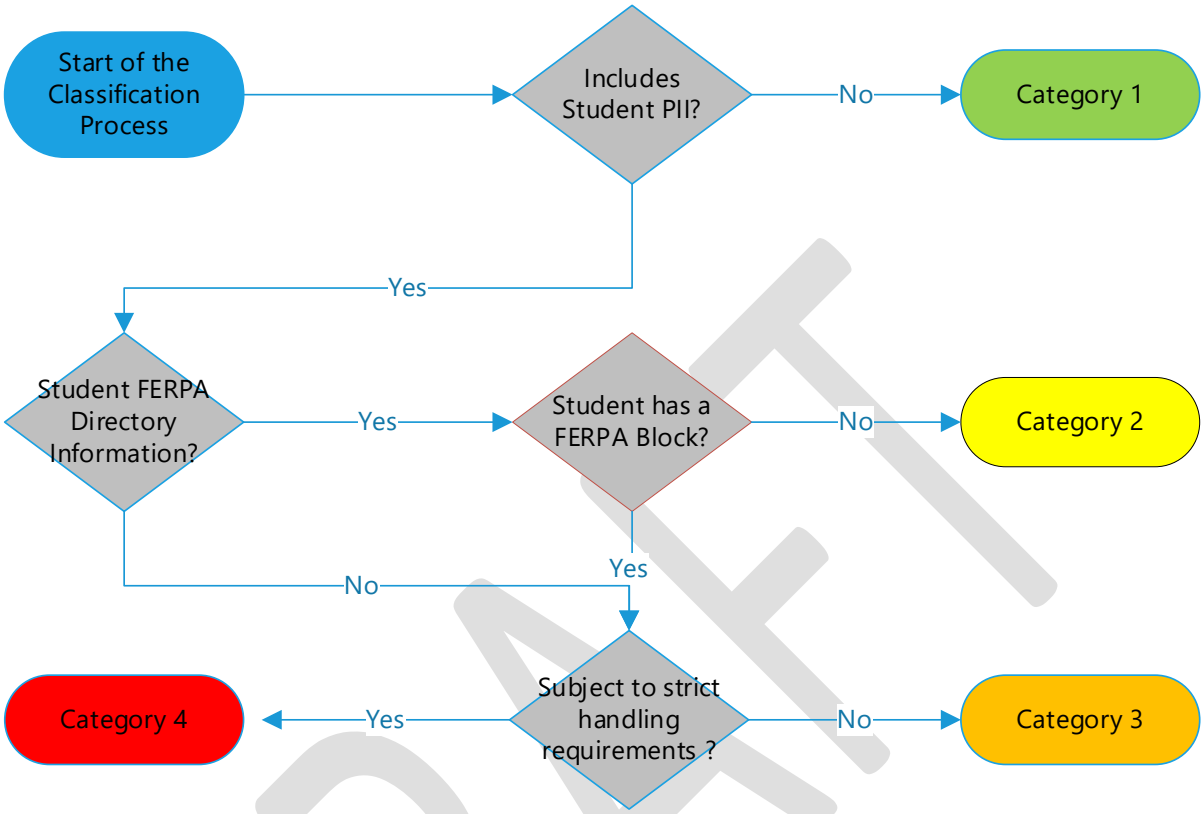
- Encryption keys or other means to decipher the information must be protected from unauthorized access

Transmitting

- Data must be encrypted in transit.
  - Regulatory Reference: WaTech Encryption Standard
- Category 4 data should never be included in unencrypted emails or unencrypted communications
  - If you are unfamiliar with the encryption methods of your college, please contact your IT Department to ensure compliance.
- Category 4 data should only be included in data extracts shared with external parties or applications when a data sharing agreement or contractual language specifically addressing data sharing is in place and at a minimum includes:
  - The purpose and specific authority for sharing the data
  - Description of the data including the classification
  - Time period of the agreement
  - Authorized uses
  - Authorized users
  - Protection of data in transit
  - Secure storage requirements
  - Data retention and disposal responsibilities
  - Backup requirements if applicable
  - Incident notification and response
  - FERPA exemption if applicable

Regulatory Reference: WaTech Data Sharing Policy

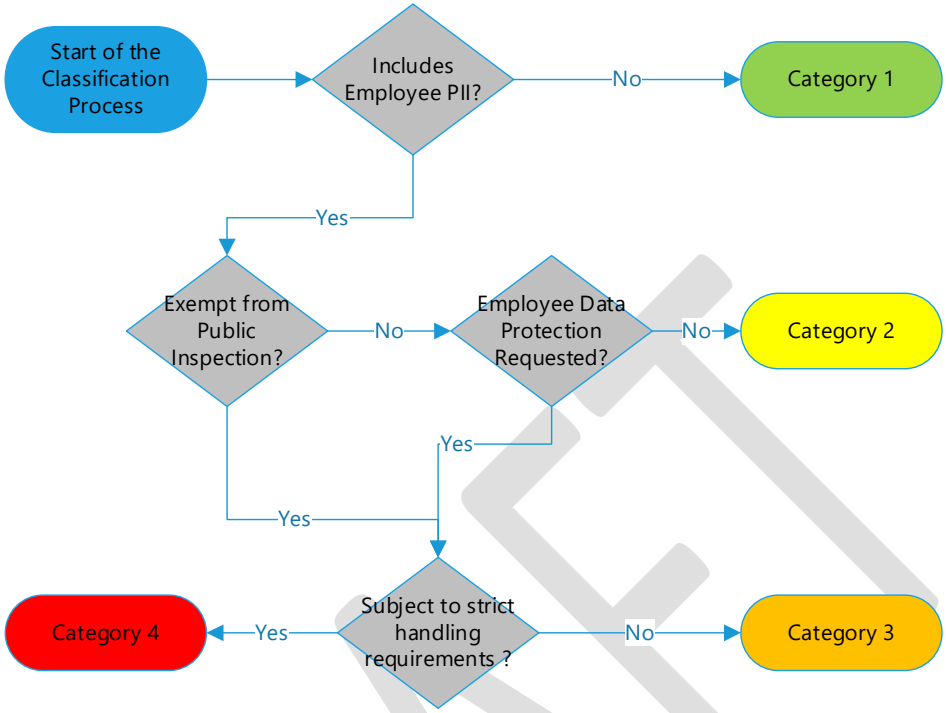
ctcLink CS Student Data Classification Decision Tree



Steps for illustration above.

- Start the classification process.
- Does the data include Student PII? If not, it is **Category 1 data**.
- If the data does include Student PII, is it also Student FERPA Directory Information? If yes and the student does not have a FERPA block, it is **Category 2**.
- If yes and the student does have a FERPA block, and the information is not subject to strict handing requirements, it is **Category 3**.
- If yes and the student has a FERPA block, and the information is subject to strict handing requirements, it is **Category 4**.

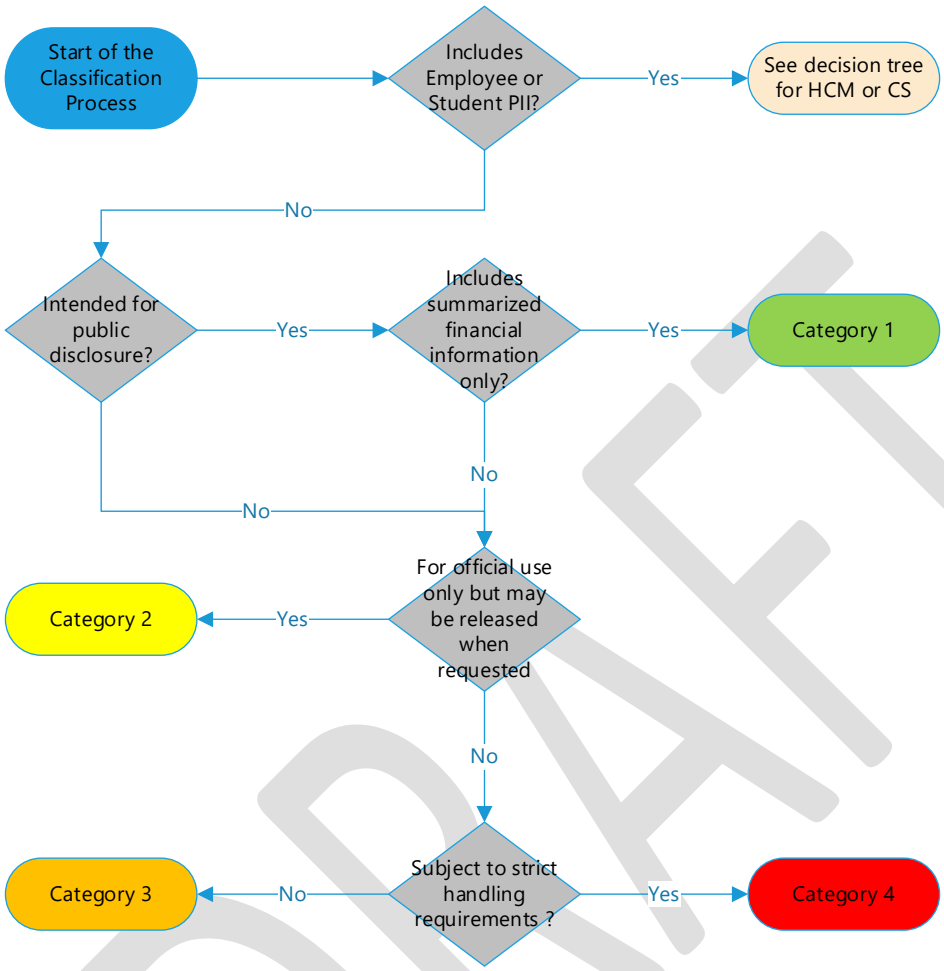
ctcLink HCM Employee Data Classification Decision Tree



Steps for illustration above:

- Start the classification process.
- Does the data include Employee PII? If not, it is **Category 1 data.**
- If the data includes Employee PII, is it also Exempt from Public Inspection? If no, and Employee Data Protection has not been requested, it is **Category 2.**
- If yes, and Employee Data Protection has been requested and not subject to strict handing requirements, it is **Category 3**.
- If yes, and Employee Data Protection has been requested and the information is subject to strict handing requirements, it is **Category 4.**

ctcLink Financial Data Classification Decision Tree



Steps for illustration above.

- Start the classification process.
- Does the data include Employee or Student PII?
- If the data includes PII, is it intended for public disclosure? If yes, refer to the decision tree for HCM or CS above.
- If the data does not include PII, it includes only summarized information, and is intended for public disclosure, it is **Category 1.**
- If the data does not include PII, and is not intended for public disclosure, it is for official use only and may be released if requested, it is **Category 2.**
- If the data may not be released if requested, and is not subject to strict handing requirements, it is **Category 3**.
- If the data may not be released if requested, and is subject to strict handing requirements, it is **Category 4**.

Personally Identifiable Information (PII)

Personally Identifiable Information (PII) data can be used to distinguish or trace an individual's identity either alone or when combined with other information such as name.

This list of ctcLink data elements is not exhaustive. Refer to the relevant RCW or regulation for more information.

Data	Employee PII RCW	Student PII Regulation	OCIO Data Classification
Residential addresses	RCW 42.56.250	34 CFR §99.3	Category 3
Personal wireless telephone numbers	RCW 42.56.250	RCW 9.35.005	Category 3
Personal email addresses	RCW 42.56.250	RCW 9.35.005	Category 3
Social security number	RCW 42.56.250	34 CFR §99.3	Category 4
Driver's license number	RCW 42.56.250	34 CFR §99.3	Category 4
Washington identification card number	RCW 42.56.250	34 CFR §99.3	Category 4
Payroll deductions including the amount and identification of the deduction	RCW 42.56.250	n/a	Category 3; Category 4 for garnishments and net pay
Emergency contact information of employees or volunteers of a public agency	RCW 42.56.250	n/a	Category 3
Employee Name	RCW 42.56.250	n/a	Category 2
Full Date of Birth	RCW 42.56.250	34 CFR §99.3	Category 3
Student Name	n/a	34 CFR §99.3	Category 2
EMPLID	RCW 42.56.250	34 CFR §99.3	Category 3
Account Number	RCW 42.56.250	n/a	Category 4
Credit/Debit Card number	RCW 42.56.250	34 CFR §99.3	Category 4
Mother's maiden name	RCW 9.35.005	34 CFR §99.3	Category 3
SEVIS ID	RCW 42.56.250	34 CFR §99.3	Category 4
Passport Number	RCW 42.56.250	34 CFR §99.3	Category 4

Appendix A – Regulatory References

The following references were used during the determination of Data Classifications and Personally Identifiable Information.

Regulatory References	Description	Pertains to
WaTech Data Classification Standard (SEC-08-01-S)	Includes the WaTech definition for each data classification	All data classifications
Categorizing data for a state agency	Includes WaTech's set of questions for each dta classification to help determine the level of classification	All data classifications
WaTech Encryption Standard (SEC-08-02-S)	WaTech's encryption standard per data classification	All data classifications
WaTech Data Sharing Policy (SEC-08)	WaTech's data sharing policy	Category 3 and 4
FERPA Directory Information	Defines what categories of student information may be considered public	Student Category 2
SBCTC FERPA Directory Information Policy (Chapter 3.30)	Defines what categories of student information is globally defined as directory information	Student Category 2
FIPS Pub 199	Standards for Security Categorization of Federal Information and Information Systems	All data classifications
Keep Washington Working SB 5497	Specifies that citizenship status information is highly sensitive	Category 4
OFM HRMC site	Common practices consistent with OFM Privacy Principles	Public Employee Category 2
RCW 10.93.160	Immigration and citizenship status—Law enforcement agency restrictions	Category 4
RCW 42.56.420	Information regarding the public and private infrastructure and security of computer and telecommunications	Category 3
RCW 42.56.230	Describes personal information that is exempt from public inspection	What cannot be classified as Category 1
RCW 42.56.250	Describes employment information that is exempt from public inspection	What cannot be classified as Category 1
RCW 42.56.590	Describes what data requires notification of a data breach	All data classifications
RCW 9.35.005	Defines Financial Information	All data classifications