



SBCTC DATA CLASSIFICATION GUIDELINES V1.1

**Data Governance Committee
Washington Community and Technical Colleges
SEPTEMBER 2026**

TABLE OF CONTENTS

Revisions.....	3
Overview.....	4
Disclaimer	5
Category 1 – Public Information	6
Category 2 – Sensitive Information	6
Category 3 – Confidential Information	8
Category 4 – Confidential Information Requiring Special Handling.....	10
Student Data Classification Decision Tree.....	12
Employee Data Classification Decision Tree.....	13
Financial Data Classification Decision Tree	14
Personally Identifiable Information (PII)	15
Financial NonPublic Information (NPI)	16
FERPA Directory Information.....	16
Appendix A – Regulatory References	18

Revisions

Change reference	Date	Version
Updated the definition of NonPublic Information (NPI) and added reference to FERPA Limited Directory Information	9/3/2026	1.1

Overview

These guidelines include the SBCTC data classification definitions based on the WATech Data Classification policy and explain the classification framework, decision logic, and handling requirements for each category of data. The accompanying [SBCTC Data Classification Workbook](#) should be used as the operational reference for identifying the classification of specific ctcLink record and field-level data elements.

The state and federal Data Classification regulations referenced in this document apply to all data, not just ctcLink data. These guidelines support data stored in ctcLink but may be useful for classifying other externally held data.

This document provides operational guidance for classifying, managing, storing, and transmitting data for the Washington Community and Technical Colleges system. It supports secure data handling by defining four data classification categories, explaining how combinations of data should be classified, and offering decision trees for assistance in classifying new student, employee, or financial data.

The guidelines emphasize that when data elements from distinct categories are combined into a dataset, the full dataset must be treated at the highest classification level. For example, a student name combined with a Social Security number becomes a Category 4 dataset because the SSN requires the highest level of protection.

The document defines the four classification levels as follows:

- **Category 1 – Public Information:** Information that can be released publicly and does not identify individual students, employees, customers, or vendors. It does not require encryption at rest or in transit but should be reviewed for accuracy and integrity before sharing.
- **Category 2 – Sensitive Information:** Official-use information that may include personally identifiable information, such as student directory information or general employee information, unless additional privacy protections apply. Encryption is not required by standard, but encryption at rest is recommended as best practice.
- **Category 3 – Confidential Information:** Information specifically protected from disclosure by law, including certain student records, protected employee information, nonpublic financial information tied to an individual, EMPLID/name combinations, FERPA-blocked directory information, and IT infrastructure/security information. Category 3 data must be encrypted at rest and in transit, with access limited to authorized individuals.
- **Category 4 – Confidential Information Requiring Special Handling:** Highly sensitive data subject to strict legal, regulatory, or contractual handling requirements, or where unauthorized disclosure could result in serious consequences. Examples include Social Security numbers, driver's license numbers, passport numbers, account numbers, credit/debit card numbers, SEVIS IDs, and other high-risk identifiers. Category 4 data require strict access controls, masking where appropriate, monitoring, encryption at rest and in transit, and formal protections when shared externally.

The document also includes decision trees to help users classify student, employee, and financial data. These decision trees guide users through questions about whether data includes personally identifiable information, FERPA directory information, public records exemptions, financial nonpublic information, or strict handling requirements.

Additional sections define key concepts such as Personally Identifiable Information (PII), Financial Nonpublic Information (NPI) under the Gramm-Leach-Bliley Act, and FERPA Directory Information.

Overall, the guidance is designed to help colleges apply consistent data classification practices across the CTC system while supporting compliance with WaTech standards, FERPA, GLBA, Washington State RCWs, SBCTC policy, and related security requirements.

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.

Data Governance

The data classifications contained in the SBCTC Data Classification Workbook and these guidelines assume that ctclink fields are being used for their documented business purpose. Institutions should not repurpose existing fields to store different types of information, even when the field appears technically capable of doing so.

When a field is used for a purpose other than its intended design, the resulting data may be subject to different privacy, security, retention, disclosure, or regulatory requirements than those associated with the field's current classification. Such use may lead to inappropriate handling, reporting inaccuracies, compliance risks, or unauthorized disclosure of protected information.

Any proposed change to the business use of a data element should be evaluated through established data governance processes before implementation.

- Data classifications are based on the field's **intended business purpose and current use**.
- Repurposing a field can create compliance, privacy, reporting, and security risks.
- A field's existing classification may no longer be appropriate if its purpose changes.
- Changes to field usage should undergo governance review before implementation.

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](#)

SBCTC Definition

Public information refers to any institutional data that does not identify an individual student, employee (other than class instructors), customer, or vendor. Examples include program offerings, class catalogs, retirement benefits offered, and summary-level financial statements.

Managing

- All Category 1 data share the same security needs and requirements.
- Category 1 data does not include information about people (students, employees, or customers) except for 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](#)

SBCTC Definition

Category 2 information includes personally identifiable information (PII) about individual students, employees, customers, or vendors. It is intended for official use only.

This information is not specifically protected from disclosure by law; however, it is generally not released to the public unless requested through an appropriate process.

This category includes:

- Student FERPA directory information
- Student FERPA limited directory information
 - Student EMPLID and Name when used to communicate with the student or with CTC staff
- Employee information not explicitly classified as Category 3 or Category 4
- Aggregated financial data not classified as Category 1, Category 3, or Category 4

This category excludes:

- All personally identifiable information for students who have requested a FERPA block or employees who have requested data privacy protection.
- Financial transactions that identify an individual (non-public information or NPI)

Refer to the [SBCTC Data Classification Workbook](#) for specific data elements classified as Category 2.

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.

All Category 2 data share the same security needs and requirements **except for**:

- The combination of EMPLID and Name
 - Regulatory Reference: [RCW 42.56.590](#)
 - 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
 - [Listing of FERPA directory information data elements](#)
- Employee 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

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 employee asked for data protection.
 - Regulatory Reference: [RCW 42.56.250](#)
- Data should not be provided/transmitted if the student has requested a FERPA block.
- Student email addresses and EMPLID are considered limited directory information. The disclosure of limited directory information is only authorized for the purpose of communicating with students or community and technical college staff when:
 - The recipient is a student, college or SBCTC employee, contractor, or authorized agent acting within the scope of assigned responsibilities
 - The information is needed to conduct an official institutional function
 - The disclosure is consistent with FERPA and institutional privacy and security requirements
 - Regulatory Reference: [SBCTC Policy Manual Chapter 3.30.10](#)
- [RCW 42.56.590](#) – Personal Information – Notice of Security Breaches - States that the combination of Name and Student ID/Employee ID when used in good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure.

Category 3 – Confidential Information

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](#)

SBCTC Definition

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

This includes:

- Student information not classified as Category 2 or 4
 - See [SBCTC Data Classification Workbook](#)
- Employee information protected by the Public Records Act [RCW 42.56](#)
 - See [SBCTC Data Classification Workbook](#)
- Non-Public Personal Information (NPI) that includes student/employee/customer Name or EMPLID combined with a financial transaction
 - See [Gramm-Leach-Bliley Act](#)
- Non-public personal information as defined in [RCW 42.56.590](#)
- FERPA directory information if a FERPA block has been requested
 - See [SBCTC Policy Manual Chapter 3.30.10](#)
- Public employee information if data protection has been requested
 - See [RCW 42.56.250](#)
- Information about the infrastructure and security of computer and telecommunication networks as defined in [RCW 42.56.420](#)

Managing

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

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](#)
 - 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

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](#)

SBCTC 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 [SBCTC 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
- In ctcLink, it requires unique security and query roles
- For access to ctcLink 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
- Generally, Yes/No indicators (such as a Student Group) that do not provide details are considered Category 3, not Category 4

Storing

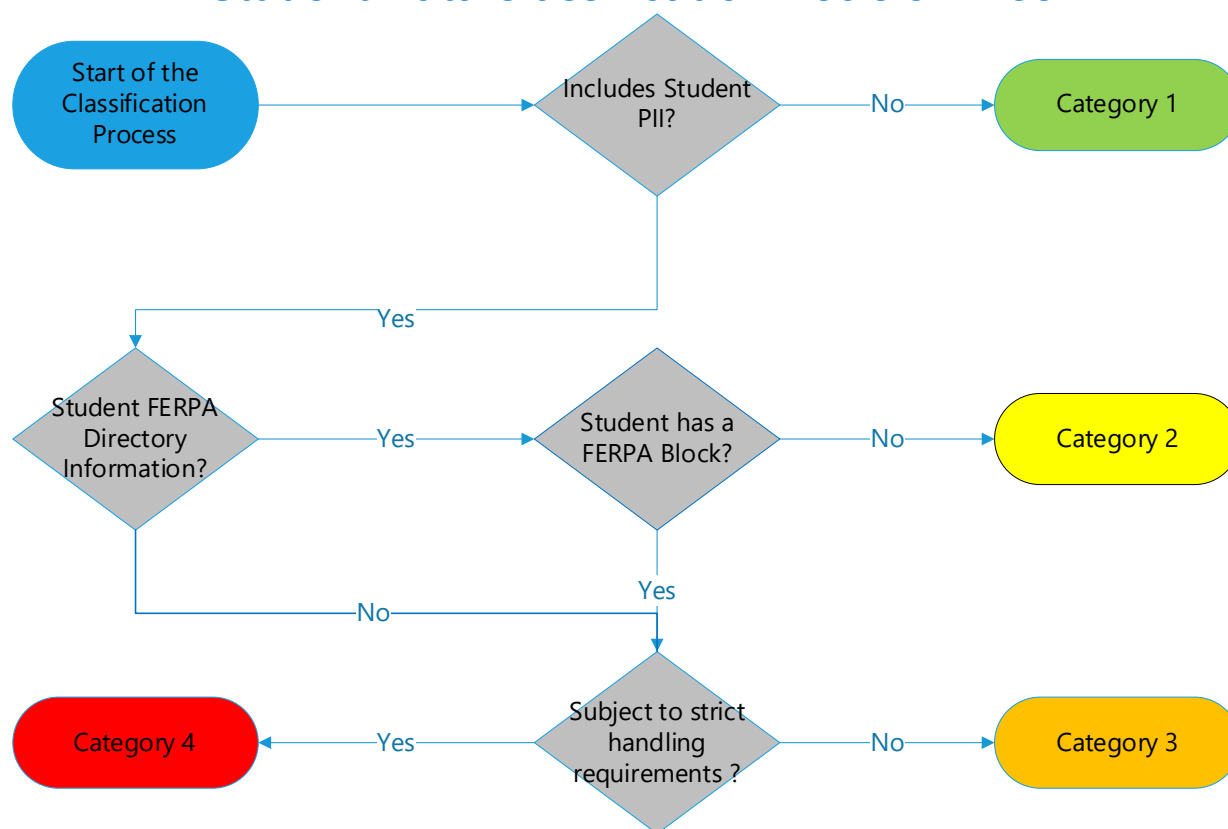
- Category 4 data must be encrypted at rest. All data is encrypted while at rest within ctcLink.
 - Regulatory Reference: [WaTech Encryption Standard](#)
- Data must be stored using encryption algorithms from FIPS 140-3 Security Requirements for Cryptographic Modules
- Encryption algorithms are used 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

Regulatory Reference: [WaTech Data Sharing Policy](#)

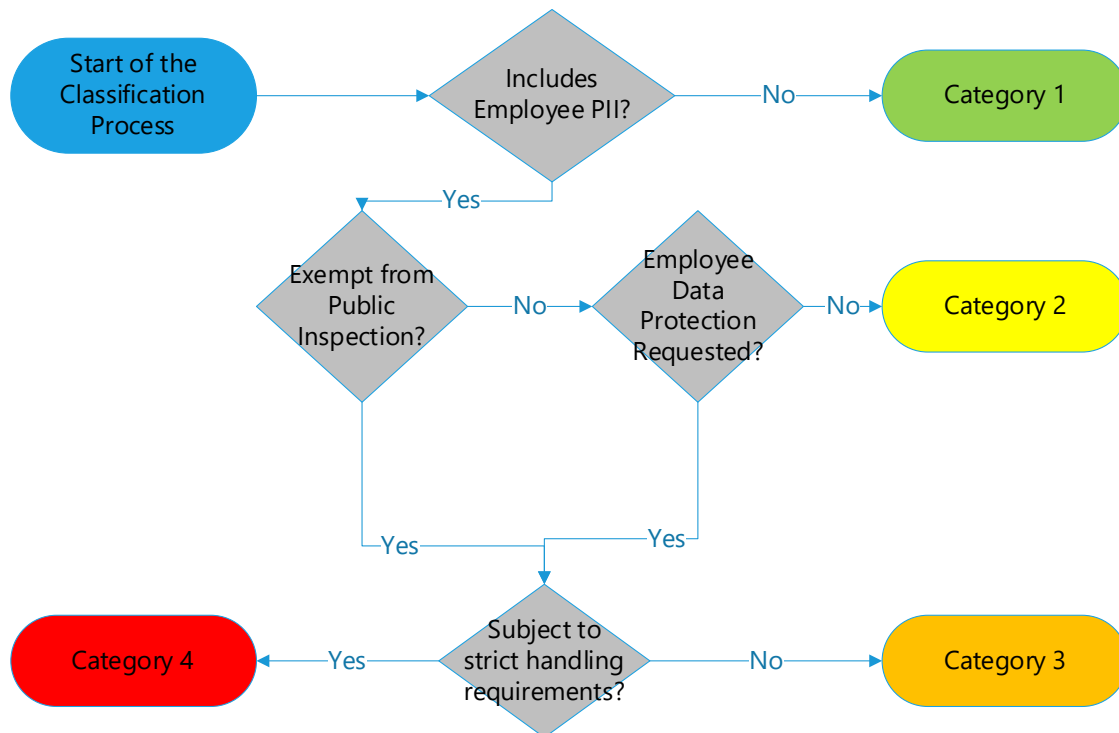
Student Data Classification Decision Tree



Steps for illustration above.

1. Start with the Student related data element or dataset being classified.
2. Determine whether the data includes student [PII](#).
 - If no, classify the data as **Category 1 – Public Information**.
 - If yes, continue to the next step.
3. Determine whether the student PII is [FERPA directory information](#).
 - If no, skip to Step 5.
 - If yes, continue to the next step.
4. Determine whether the student has requested a FERPA block.
 - If no, classify the data as **Category 2 – Sensitive Information**.
 - If yes, continue to the next step.
5. Determine whether the data is subject to strict handling requirements.
 - If no, classify the data as **Category 3 – Confidential Information**.
 - If yes, classify the data as **Category 4 – Confidential Information Requiring Special Handling**.

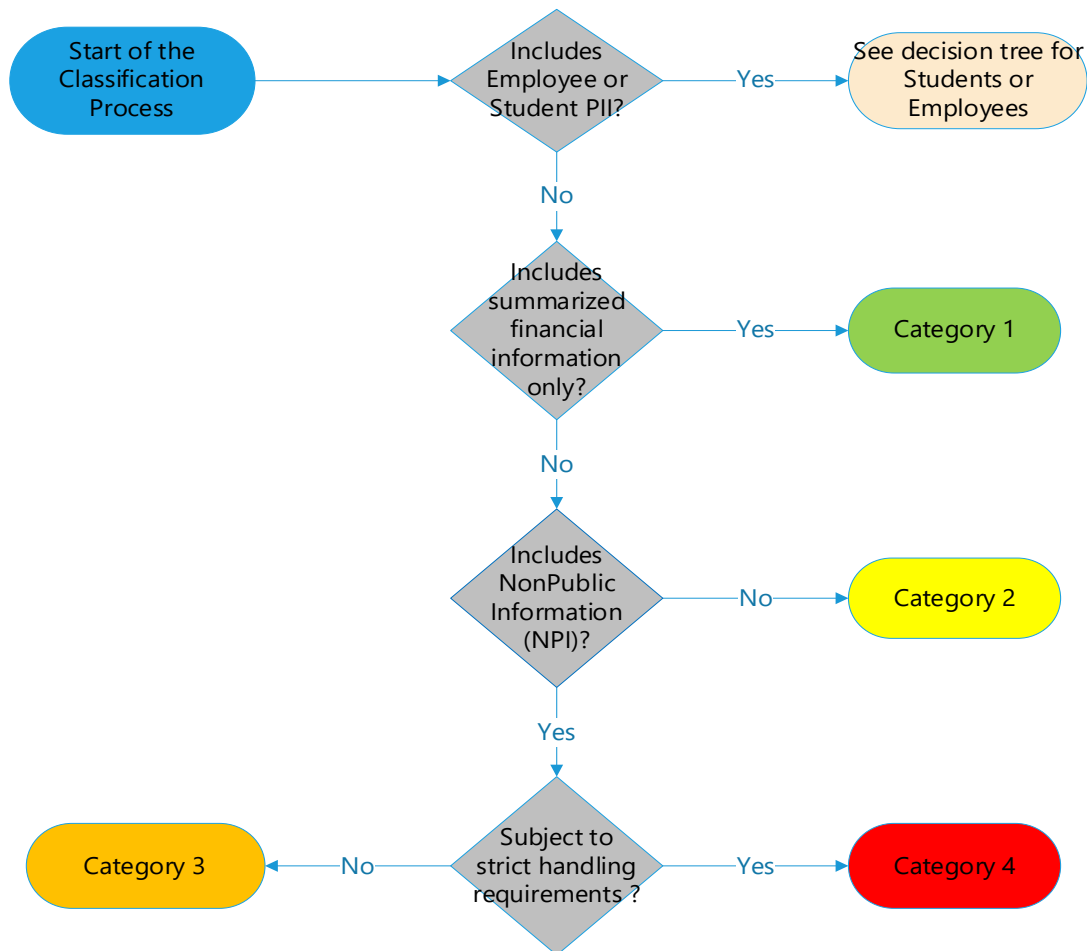
Employee Data Classification Decision Tree



Steps for illustration above:

1. Start with the Employee data element or dataset being classified.
2. Determine whether the data includes employee [PII](#).
 - If no, classify the data as **Category 1 – Public Information**.
 - If yes, continue to Step 3.
3. Determine whether the data is exempt from public inspection under the [Public Records Act](#).
 - If no, continue to Step 4.
 - If yes, continue to Step 5.
4. Determine whether the employee has requested data privacy protection.
 - If no, classify the data as **Category 2 – Sensitive Information**.
 - If yes, continue to Step 5.
5. Determine whether the data is subject to strict handling requirements.
 - If no, classify the data as **Category 3 – Confidential Information**.
 - If yes, classify the data as **Category 4 – Confidential Information Requiring Special Handling**.

Financial Data Classification Decision Tree



Steps for illustration above.

1. Start with the financial data element or dataset being classified.
2. Determine whether the data includes student or employee [PII](#).
 - If yes, use the appropriate student or employee decision tree to classify the data.
 - If no, continue to Step 3.
3. Determine whether the data includes summarized financial information only.
 - If yes, classify the data as **Category 1 – Public Information**.
 - If no, continue to Step 4.
4. Determine if the data includes [NonPublic Information \(NPI\)](#).
 - If yes, classify the data as **Category 2 – Sensitive Information**.
 - If no, continue to Step 5.
5. Determine whether the data is subject to strict handling requirements.
 - If no, classify the data as **Category 3 – Confidential Information**.
 - If yes, classify the data as **Category 4 – Confidential Information Requiring Special Handling**.

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 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 2
Account Number	RCW 42.56.230	n/a	Category 4
Credit/Debit Card number	RCW 42.56.230	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

*Student EMPLID is considered Limited Directory Information (Category 2).

Financial NonPublic Information (NPI)

Under the Gramm-Leach-Bliley Act (GLBA), Nonpublic Personal Information (NPI) is any information that results from a transaction between the customer and the institution involving a financial product or service rendered that identifies the customer, student or employee and includes a description of services rendered and an amount.

Services rendered generally refer to:

- Services provided under a contract or agreement
- Activities that involve access to, processing of, maintenance of, or use of customer information.
- Business functions that support the delivery of financial products or services.

Examples could include:

- Hosting services
- Student financial aid administration
- Loan servicing
- Payment processing
- Information technology and cybersecurity support
- Third-party reporting or analytics services

FERPA Directory Information

FERPA Directory Information is described in the [SBCTC Policy Manual Chapter 3.30](#) as information contained within a student's education record that, if disclosed, would not be considered harmful or an invasion of privacy.

Below is a list of the college system's global FERPA Directory Information including the associated ctcLink record and field names.

Data	Record Name	Field Name
Student's Name	VCS_BIO_PRIORITY	NAME_PREFIX
		NAME
		FIRST_NAME
		MIDDLE_NAME
		LAST_NAME
		NAME_SUFFIX
Major Field of Study	ACAD_PLAN	DESCR
Enrollment Status	STDNT_CAR_TERM	ACADEMIC_LOAD
Dates of Attendance	STDNT_ENRL and TERM_TBL	TERM_BEGIN_DT
		TERM_END_DT
Participation in recognized sports	EXTR_ACTVTY_TBL	DESCR Where EXTRA_ACTVTY_TYPE = ATHL

Degree or certificate earned	ACAD_DEGR	DEGREE
	ACAD_DEGR_PLAN	ACAD_PLAN
	ACAD_PLAN_TBL	TRNSCR_DESCR
Term degree or certificate awarded	ACAD_DEGR	COMPLETION_TERM
Honors	HONOR_AWARD_CS	DESCRFORMAL
	ACAD_DEGR_HONS	DESCR

SBCTC designates student identification number (EMPLID) and student email address, including both the college-assigned email address and the student's personal email address, as **Limited Directory Information**. Access to and disclosure of this information is restricted to Washington State Community and Technical College employees and authorized agents who require it to perform official institutional duties, including communications necessary to support student services, instruction, operations, and other legitimate educational interests.

Appendix A – Regulatory References

The following regulatory 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 classification to help decide 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
Gramm-Leach-Bliley Act	Consumer Financial Information Privacy Rule	Category 3
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	Public Records Act	Public Employee Category 3
RCW 42.56.420	Information about 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 or 2
RCW 42.56.250	Describes employment information that is exempt from public inspection	What cannot be classified as Category 1 or 2
RCW 42.56.590	Describes what data requires notification of a data breach	All data classifications



[CC BY 4.0](https://creativecommons.org/licenses/by/4.0/), unless otherwise noted.

Washington State Board for Community and Technical Colleges