IT-0005 Acceptable Use of Student and Employee Identification Numbers

	Policy identification number: IT-0005
	File: Information Technology Policies
	Acceptable Use of Student and Employee Identification Numbers
	Policy Summary **This policy establishes the requirements and restrictions regarding the use of Student or Employee Identification numbers.**

Policy Owner	Approval Date	Effective Date
Vice President, Finance & Administration	**June 10, 2019**	**June 10, 2019**

Search Terms	Scheduled for Review
acceptable, identification, numbers, a	**Spring 2024**

I. Policy Statement

1. General
    1. Student and Employee ID numbers (commonly regarded as the "900" number) are used to uniquely identify an individual for the purposes of academic, business, and employment processes. These ID numbers are considered "Personally Identifiable Information" and must be protected from unauthorized use.
2. Usage Requirements

All faculty, staff, employees, and departments of Fort Lewis College are expected to adhere to the following guidelines regarding the use of Student and Employee ID numbers:

1.

1. The Student or Employee ID number may not be based in any way upon an individual's SSN, Passport, or other Government Issued ID numbers.
2. The combination of a name and Student or Employee ID number is not sufficient proof of identity for the purposes of a password reset request via phone. To prevent unauthorized access, a combination of factors must be used to assure proof of identity. Information that can be reasonably determined from publicly available sources must not be used as a verification factor.
3. The combination of a name and Student or Employee ID number is not sufficient proof of identity for the purposes of an in-person password reset. A valid school or government issued photo ID is required to verify identity. This requirement can be waived in cases where the individual is known, and identification has previously been verified with a valid school or government issued photo ID.
4. The Student or Employee ID number may not be used as Login ID for electronic systems or applications. This includes but is not limited to applications such as: web portals, computer or network access systems, registration or admission systems, and email accounts.
5. Business processes and computer-based applications must be designed to ensure that the Student or Employee ID number may not be used to allow unauthorized individuals to gain access to an individual's FERPA protected education records, Personally Identifiable Information (PII), or information related to financial transactions.
6. A school official with an appropriate need to know, may use a Student or Employee ID number to gain access to an individual's FERPA protected education records or PII, provided access to this information is through a system with appropriate authentication and access control mechanisms as approved by the Information Technology Department.
7. A Student or Employee ID number used in a standalone fashion may not be substituted for a valid Skycard ID card to access meal plans, door access, or facility privileges.
8. An individual's name and Student or Employee ID number used in a standalone fashion is not sufficient proof of identity for certain types of transactions. A valid school or government issued photo ID is required for the following transactions:
    1. In-person transactions involving receipt or deposit of cash or check
    2. In-person requests to access PII, financial information, educational records
    3. In-person requests to access or modify bank account, name and address, or other information related to direct deposit, credit card transactions, refunds, or other information related to financial transactions

       This requirement can be waived in cases where the individual is known, and identification has previously been verified with a valid school or government issued photo ID.

II. Reason for Policy

Colorado State statutes identify Employee and Student ID numbers as Personally Identifiable Information. Per the statute, reasonable security procedures and practices must be implemented

and maintained to protect these data elements against unauthorized access or use. Additionally, the Federal Fair Credit Reporting Act require that appropriate measures are implemented to prevent identity theft.

III. Responsibilities

For following the policy: All employees and contracted vendors

For enforcement of the policy: Information Security Officer

For oversight of the policy: Vice President for Finance & Administration

For notification of policy: Policy Librarian

IV. Definitions

PII: Personally Identifiable Information is defined in the "Classification of Data" policy.

Stand-alone fashion: This refers to the use of an individual's name and Student or Employee ID without any additional verification factors.

Verification factor: This is information or a mechanism that can be used to verify the identity of an individual, such as passwords or photo ID cards.

V. Cross-Referenced Policies

Classification of Data Policy

Colorado Revised Statutes C.R.S. § 24-73-101

The Fair Credit Reporting Act, Part 681 "Identity Theft Rules"

U.S. Department of Education: FERPA Online Library

- Letter to University of Wisconsin-River Falls re: Student Account Identifiers https://www2.ed.gov/policy/gen/guid/fpco/ferpa/library/uwisc.html
- Letter to University of Illinois re: Use of Student ID Numbers Under FERPA https://www2.ed.gov/policy/gen/guid/fpco/ferpa/library/ryanuillinois.html

VI. Consequences of Non-Compliance

Using Student and Employee numbers improperly puts individuals at risk of identity theft and financial fraud. Fines and penalties for improper use and management of Personally Identifiable Information can be levied by State, Federal, and International entities.

Violations shall be handled consistent with College disciplinary procedures. The College may refer suspected violations of applicable law to appropriate law enforcement agencies.