Collin College Information Technology Services (CC-TS)
Data Privacy ISP:

PURPOSE:

The purpose of the Data Privacy ISP is to establish guidelines for handling, protecting, and governing personal and sensitive information. This document ensures compliance with applicable privacy laws and regulations, reduces the risk of data breaches, and promotes responsible stewardship of personal and institutional data.

SCOPE:

This ISP applies to all faculty, staff, administrators, contractors, third-party vendors, and students who collect, access, store, transmit, or otherwise process personal or sensitive information on Collin College (CC) networks or infrastructure. This includes all data stored in CC systems, devices, cloud services, and third-party platforms.

STATEMENT:

1. Collection and Use
    a. Technology Services and other college departments must limit the collection of personal and sensitive data to what is necessary for legitimate business, educational, or operational purposes.
    b. Data must be used only for the purposes for which it was collected, unless explicit consent or a lawful exception applies.

2. Storage and Access Controls
    a. All personal and sensitive data must be stored on approved college network storage or secure cloud platforms with contractual safeguards.
    b. Local device storage (e.g., device hard drives, removable media) is prohibited for sensitive data unless explicitly approved by the CIO/IRM.
    c. Access to personal and sensitive data is restricted to authorized personnel with a legitimate business need.

3. Protection and Security
    a. Encryption must be used for sensitive data both in transit and at rest.
    b. Multifactor authentication (MFA) is required for systems that contain or provide access to sensitive data.
    c. Confidential data transmissions must use secure protocols (e.g., TLS, VPN).

4. Sharing and Third Parties
    a. Internal sharing of personal and sensitive data requires authorization from the Data Owner.
    b. External sharing must be done through a secure portal (preferred) or through secure encrypted email.

5. Retention and Disposal
    a. Data retention schedules are the responsibility of the Data Owner and must comply with any applicable regulations.
    b. When data reaches the end of its retention period, or is no longer required, it must be securely destroyed in a manner that prevents reconstruction (e.g., secure wipe, shredding).

6. Incident/Breach Response
    a. Any suspected or confirmed unauthorized access, use, disclosure, or loss of personal or sensitive data must be immediately reported to CC-TS Information Security.
    b. CC-TS will initiate the Incident Response Plan, including notification requirements as mandated by law.
        i. Loss of personal or sensitive data that affects more than 50+ users must be reported to TX Department of Information Resources.
        ii. Loss of personal or sensitive data that affects more than 250+ Texas residents must be reported to the Texas AG.

7. Training and Awareness
    a. Data Owners are responsible for ensuring users under their supervision understand and comply with this ISP.
    b. CC employees and contractors who handle sensitive and personal information must annually:
        i. Agree to and sign a data use agreement.
        ii. Complete training on data privacy and information security.

DEFINITIONS:

Data Owner
The individual or department with primary responsibility for classifying, approving access to, and ensuring proper handling of data. The Data Owner determines which data are considered personal, confidential, or sensitive and ensures compliance with applicable laws, regulations, and institutional policies.

Personal Data
Any information relating to an identified or identifiable individual. Examples include, but are not limited to, names, addresses, telephone numbers, email addresses, identification numbers, and account information.

Sensitive Data
A subset of personal data that requires heightened protection due to its confidential nature or regulatory requirements. Examples include Social Security numbers, driver's license numbers, health records (HIPAA), student records (FERPA), financial data (GLBA, PCI), authentication credentials, and other information designated as confidential by law or policy.

Confidential Data
Data that, if improperly disclosed, modified, or destroyed, could adversely affect Collin College,

its students, faculty, staff, or partners. Confidential data may overlap with sensitive data and includes information classified as non-public by the institution.

Third-Party Vendor

Any external service provider, contractor, or business partner that processes, stores, or transmits Collin College's personal or sensitive data on behalf of the institution. Vendors must comply with CC contractual, privacy, and security requirements.

Implementation Information

Review Frequency:	Annually
Responsible Person:	CIO/IRM
Approved By:	Dr. David Stephens
Approval Date:	10/6/2025

Revision History

Version:	Date:	Description:
1.0	9/19/2025	Initial document