COVENANT COLLEGE

Data Classification Policy

The purpose of this Data Classification Policy is to provide the basis for protecting the confidentiality of data at Covenant College by establishing a framework for classifying institutional data. Classification of data into categories will aid Covenant in determining security controls for the protection and use of data to ensure:

1. Only authorized personnel will have access to sensitive and restricted information,
2. The College's statutory, regulatory, legal, contractual, and privacy obligations are met,
3. The College's proprietary data is protected as required,
4. Data is appropriately available for decision-making as required, and
5. Relevant data and information are shared with the necessary safeguards.

All data must be classified into one of three classifications:

- Public Data
- Covenant Sensitive Data
- Covenant Restricted Data

Data may exist in any format (i.e. electronic, paper) and includes, but is not limited to, all academic, administrative, and research data. If particular documents or data types are not explicitly addressed within this policy, each unit or department should classify its data by considering the potential for harm to individuals or the College in the event of unintended disclosure or loss. This risk should be weighed against the need to encourage open discussion, improve efficiency and further Covenant's goals of the creation and dissemination of knowledge. The Information Security Task Force may assist with the classification process. Departments should be particularly mindful to protect restricted personal information, such as Social Security Numbers, drivers' license numbers and financial account numbers, disclosure of which may create the risk of identity theft.

Everyone with access to Covenant College Data should exercise good judgment in handling sensitive information and seek guidance from management as needed. Data owners are responsible for appropriately classifying data. Data users are responsible for complying with data use requirements.

Public Data

Public information is defined as information that is intended for public disclosure or information that may be shared with anyone without adverse impact on Covenant College's mission, safety, finances, or reputation. Such information may be disclosed by the institution for any purpose at its discretion, but is not required to be disclosed except where required by federal and state regulations.

The Covenant issued Banner ID should be used with a person's name to identify a specific individual in any form of electronic communication. Under no circumstances should Personally Identifiable Information (PII) be used in electronic communication. PII would include an individual's full legal name, social security number, full date of birth, driver's license number, or passport number.

Covenant designates the following categories of information as public or "directory information." All other information is sensitive or restricted and may be released outside Covenant only with the individual's written permission.

Student	Employee	Donor/Constituent
Biographical: ● Name ● Campus address ● Campus telephone number ● Covenant College Email address ● Covenant Banner ID ● Photograph and video	Biographical: ● Name ● Campus address ● Campus telephone number ● Covenant College Email address ● Covenant Banner ID	Biographical: ● Name ● Personal Email address (opt-in) ● Graduation Year ● Level of giving ● Gifts in honor or memorial information

Enrollment: ● Dates of attendance ● Enrollment status ● Class level ● Previous institution(s) attended ● Major field of study ● Awards and honors ● Degrees conferred (including dates) Athletic: ● Past and present participation in officially recognized sports and activities ● Physical factors (height, weight of athletes) ● Place of birth	● Photograph and video Employment: ● Dates of employment ● Employment status ● Job title	● Covenant Banner ID ● Photograph and video
Campus-wide: ● Official statements and press releases ● Campus maps ● Policy and procedure manuals designated by the owner as public ● Job-postings		

Currently enrolled students may withhold disclosure of directory information under FERPA by submitting a written request to withhold disclosure to the Office of Records. No information — public, private or restricted — on an applicant's record may be released outside Covenant, except to an agent designated by the applicant, until the applicant becomes a registered student and has an opportunity to initiate a suppression of information.

Donors may withhold disclosure of directory information by notifying the Development Office.

Transmission and storage: When practical, public data should only be shared via systems which the College maintains full administrative control, which includes the ability to remove or modify the data in question. Information systems such as web servers must be properly secured to prevent the unauthorized modification of published public data. Interactive access to databases containing public data, such as online directories or library catalogs should be properly secured to impede bulk downloads or entire collections of data.

Covenant Sensitive Data

Sensitive information is defined as information that requires a moderate level of confidentiality and/or could cause moderate or limited risk of financial loss, legal liability, public distrust, or harm if disclosed.

By default, all institutional data that is not explicitly classified as restricted or public should be treated as sensitive. Covenant designates the following categories of information as sensitive or "confidential information." Please note this is not an exhaustive list.

Student	Employee	Donor/Constituent
Biographical: ● Personal Email address ● Personal telephone number ● Personal address	Biographical: ● Ethnic background ● Personal Email address ● Personal telephone number ● Personal address	Biographical: ● Personal telephone number ● Personal Email address (did not opt-in) ● Personal address
Campus-wide: ● Meeting minutes ● Audit reports		

- Security incident information
- Competitive business information
- Grants and Contracts

Transmission and storage: Sensitive data must be stored carefully to prevent disclosure when not in use. It must not be disclosed to parties outside the College without explicit written authorization by an appropriate data owner. It must not be stored on any cloud-based information systems not managed or contracted by the College. When practical, sensitive data should only be shared via systems which the College maintains full administrative control, which includes the ability to remove or modify the data in question. Information systems such as web servers must be properly secured to prevent the unauthorized modification of published sensitive data. Interactive access to databases containing sensitive data, should be properly secured.

Covenant Restricted Data

Restricted information is defined as information that is regulated by federal or state law or regulations. Loss of confidentiality of this data could have a significant adverse impact on Covenant's mission, safety, finances, or reputation. All information that requires Covenant to self-report to the government if it is inappropriately accessed is considered restricted. No information on financial aid records may be released outside Covenant except as authorized or required by federal and state regulations.

Covenant designates the following categories of information as restricted. Please note this is not an exhaustive list.

Student	Employee	Donor/Constituent
Biographical: ● Social security number ● Full date of birth ● Passport number ● Driver's license number or state-issued identification card number Admission: ● Admissions forms ● FAFSA forms and supporting documentation ● I-9 forms Payroll: ● Pay stubs, ● Direct deposit forms ● Tax forms Academic: ● Grades Medical: ● Insurance forms ● Medical records Student Records: ● Disciplinary records ● Counseling records ● Title IX records	Biographical: ● Social security number ● Full date of birth ● Passport number ● Driver's license number or state-issued identification card number HR Records: ● Background checks ● I-9 forms ● Pay stubs ● Direct deposit forms, garnishments ● Tax forms ● Termination or layoff records ● Unemployment insurance claims ● Title IX records ● Salary or hourly pay rates Medical: ● Insurance and benefit enrollment forms ● Workers' compensation records ● FMLA leave certifications ● Reasonable accommodations under ADA	Biographical: ● Social security number ● Full date of birth ● Passport number ● Driver's license number or state-issued identification card number Financial: ● Bank account information (note: Credit card information is handled by a secure third party and is not stored by Covenant College)

Campus-wide:

- Budgets (actual and itemized not projected aggregated), financial information
- Covenant College credit card numbers

Transmission and storage: Restricted data must never be transmitted via email or text. Strong passwords must be used to access restricted data and it must be stored on devices which have protection and encryption measures. Restricted data must be protected by IT-approved encryption when stored on any device or media that are not physically tethered to the College (mobile devices, optical or flash media, or backup tapes). It must be protected by IT-approved encryption when transmitted across public networks such as the Internet and should be protected by multi-factor authentication whenever such capabilities exist. When queried from a remote location, restricted data must be accessed via an IT-approved secure (VPN like) connection. It must be stored only in an area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other individuals not on a need-to-know basis.

Created May 2016
Revised February 2020
Revised February 2024
Reviewed April 2025