Saint Michael's College

Data Classification Standard

1.0 Purpose

This standard serves as a supplement to the Information Security Plan and Data Policy. The objective of this standard is to assist data stewards with classifying data according to the level of security required to protect personal and institutional data. In descending order of sensitivity, these categories are "Confidential", "Internal Use," and "Public." All Data, whether physical documents, electronic databases, or other collections of information, are to be assigned to a Security Classification level according to the most sensitive content contained therein.

2.0 Definitions

2.1 Data: Data is a discrete body of information created, collected and stored in connection with the operation and management of the College and used by members of the College having authorized access as a primary source. Data includes electronic databases as well as physical files.

2.2 Security Classification: Categories by which data is classified according to its sensitivity ("Confidential", "Internal Use" and "Public")

3.0 Confidential Data

3.1 Confidential data includes sensitive personal and institutional information, and must be given the highest level of protection against unauthorized access, modification or destruction. Unauthorized access to personal confidential data may result in a significant invasion of privacy, or may expose members of the College community to significant financial risk.

3.2 Confidential data shall include:

- Student Information
  (1) Social Security number
  (2) Personal financial information (credit cards, bank accounts, wire transfers, payment history, financial aid/grants, student bills)
  (3) Date of birth
  (4) Medical/health records
  (5) Grades (including test scores, assignments, and class grades)
- Employee Information
  (1) Social Security number
  (2) Personal financial information (salary, credit cards, bank accounts, wire transfers, retirement accounts)
  (3) Date of birth
  (4) Insurance benefit information
  (5) Medical/health records, other than general information about worker's compensation claims

- Business/Vendor Data
  (1) Social security number
  (2) Credit card information
  (3) Contract information
- Donor/Alumni Information
  (1) Social Security number
  (2) Personal financial information
  (3) Financial information (credit card numbers, bank account numbers, amount / what donated)

4.0 Internal Use Data

4.1 Internal Use data includes information that is less sensitive than confidential data, but that, if exposed to unauthorized parties, may have an indirect or possible adverse impact on personal interests, or on the finances, operations, or reputation of Saint Michael's College. Internal use data must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Internal use data is information that is restricted to members of the college community who have a legitimate purpose for accessing such data.

4.2 Internal Use data may include, but is not limited to:

- Employee or student email addresses
- General information about employee worker's compensation claims
- Strategic plans
- Financial plans and forecasts
- Donor information
  (1) Name
  (2) Family information
  (3) Medical information
  (4) Telephone / fax numbers
  (5) E-mail / URLs

5.0 Public Data

Public data is information that is generally available to the public, or that, if it were to become available to the public, would have no material adverse effect on individual members of the College community or upon the finances, operations, or reputation of Saint Michael's College. It is defined as information with no existing local, national or international legal restrictions on access or usage. Public data, while subject to disclosure rules, is available to all members of the College community and to all individuals and entities external to the College community.

6.0 Guidelines for Classification

6.1 If you are evaluating data you are responsible for, you can apply the Confidentiality, Integrity, and Availability (CIA) criteria.

- Confidentiality: The need to strictly limit access to data to protect the College and individuals from loss.
- Integrity: Data must be accurate, and users must be able to trust its accuracy.
- Availability: Data must be accessible to authorized persons, entities, or devices.

6.2 If you determine that any of the three factors (Confidentiality, Integrity or Availability) are required, your data should be considered to be Confidential.

Need for...	Confidential	Internal	Public
Confidentiality	Required	Recommended	Optional
Integrity	Required	Recommended	Optional
Availability	Required	Recommended	Optional