CONESTOGA
Connect Life and Learning

DATA CLASSIFICATION PROCEDURE

Authorizer: Vice President, Finance and Corporate Services

Version: V1

Effective Date: May 25, 2022

PROCEDURE STATEMENT:

Data is a collective asset that is acquired, used, and managed by multiple stakeholders within Conestoga. This procedure sets out the principles for classifying data, regardless of form or media, to meet business needs and regulatory requirements of The Conestoga College Institute of Technology and Advanced Learning (Conestoga).

SCOPE:

This procedure applies to all data in Conestoga's control and custody including research data. Security controls are documented in internal restricted information technology practices and standards.

PROCEDURE ELABORATION:

1. Data stewards classify Conestoga's data as public, internal, or restricted.
2. Conestoga data is internal by default.
    a) If there are conflicting guidelines defining specific data classification, the data is classified according to the most restrictive protection requirement.
    b) Corporate Services will assist college stakeholders classify college data
3. Conestoga's public data is shared in open formats.
4. Datasets are regularly reviewed by Conestoga's data stewards to ensure access and security provisions correspond to the data classification.
5. Data stewards protect data from modification or deletion in accordance with approved Conestoga data governance standards.
6. Data stewards reassess and consider reclassification of data when there are major changes to systems housing data, changes to the data including new data sets, and access levels change.

The following table identifies key descriptors and controls assigned to data by classification.

	Public Data	Internal Data	Restricted Data
Description	Data that can be made available to the general public without concern	Data intended for any Conestoga user but not for the general public~~.~~	Data that is defined in regulations, legislation, or by legal contract as sensitive, and/or its release could negatively impact strategic business decisions such as budgeting, human resources, legal negotiations, etc.
Risk	Minimal inherent risk. Minimal controls are required for public data to protect it from unauthorized modification or destruction in order to have the data be a trustworthy representation of Conestoga	Moderate inherent risk. Should the data be released, any data that is not explicitly classified as public or restricted shall be treated as internal data. A reasonable level of security controls should be applied to prevent its unauthorized release, alteration, or destruction	High inherent risk. The alteration, destruction, and or unauthorized release of restricted data is likely to cause a significant material level of risk to the Conestoga, consequently the highest level of access control, secured storage, transmission requirements, and secured destruction must be always applied
Access	Access to this data can be granted to any requestor~~.~~	Access to this data can be granted to any Conestoga user	Access to this data can only be granted to users with a business need to access it and its release is limited in scope to only authorized users
Storage	No security controls required	Electronic data must be stored on **Conestoga approved systems** (i.e., shared drives, servers, cloud-based storage) with controlled role-based access Physical files must be stored in a secure Conestoga approved location	Electronic data must be stored on **Conestoga approved systems** (i.e., shared drives, servers, cloud-based storage) with controlled role-based access, and audit trail Physical files and those on portable devices (which must be password protected) must be stored

	Public Data	Internal Data	Restricted Data
			in a secure Conestoga approved location in a locked space with limited and managed access
Transmission	No Security controls required	Data must be transmitted via a secure network	Data must be encrypted during transfer and transmitted via a secure network
Destruction	Data must be securely deleted or transferred to the archives according to approved retention schedules		

DEFINITIONS:

Data

Facts, figures and statistics objectively measured according to a standard or scale, such as frequency, volumes or occurrences.

Data Stewards

Data stewards are employees responsible for maintaining and protecting defined sets of data within the various lines of business throughout Conestoga. Data stewards are not data owners, data stewards fulfill a business focused oversight role ensuring data is fit for purpose for data driven business processes. Data stewards work with others to ensure data classification rules are followed and implement processes to manage the classified data.

Dataset

A dataset is an organized collection of data. The most basic representation of a dataset is data elements presented in tabular form and may also present information in a variety of non-tabular formats, such as an extensible mark-up language (XML) file, a geospatial data file, or an image file, etc.

Information

Information is ideas, thoughts, knowledge or memories irrespective of format or medium, which may be represented in manuals, reports and similar work products and may contain data; data grouped together to have meaning is information.

Inherent Risk

The risk to Conestoga in the absence of any controls to alter either the risks likelihood or impact of a risk.

Risk

The possibility that an event could occur and adversely affect the achievement of a Conestoga objective(s).

REFERENCES:

Freedom of Information and Protection of Privacy Act (FIPPA)
Ministry of Training, Colleges and Universities Act
Ontario Colleges of Applied Arts and Technology Act
Personal Health Information Protection Act
Ontario’s Open Data Guidebook: A Guide to the Open Data Directive, 2019

RELATED DOCUMENTS:

Records and Information Management Policy

REVISION LOG:

Academic Forum	April 20, 2022
Academic Coordinating Committee	May 25, 2022