City of Mississauga

Corporate Policy & Procedure

9.13

Appendix 1

Policy Title: Data Handling Policy

Policy Number:

Draft Only – April 7, 2021

Section:	**Data Handling**	Subsection:	**Information Technology**
Effective Date:		Last Review Date:	
Approved by: **Click here to enter text.**		Owner Division/Contact: **Information Technology Division, Corporate Services Department**	

Policy Statement

All City of Mississauga Data will be handled, classified and security controlled in accordance with the criteria defined in this policy.

Purpose

The purpose of this policy is to provide direction to staff in the handling and classification of Data, as defined in this policy, in order to:

- Prevent unauthorized destruction, modification, disclosure, access, use and/or removal
- Ensure the protection and security of sensitive corporate and citizen Data
- Develop a culture of Data security amongst all staff and authorized agents
- Increase Data regulation and legal compliance, and
- Minimize risk while maximizing Data value and driving innovation

Scope

This policy applies to handling of all Data that is created, owned, leased, processed and/or stored by all City staff, elected officials, contractors, authorized agents and third-party organizations or individuals. This applies to all Data on City premises, approved cloud environments and all work locations, including both digital and paper records.

This policy does not include information on record retention. Refer to the Records Retention Schedule By-law 0097-2017, as amended.

This policy does not apply to elected officials' constituency records. Refer to the Elected Officials' Records policy for additional information.

Definitions

For the purposes of this policy:

“City” means the Corporation of the City of Mississauga.

“Confidential” means information protected due to proprietary, ethical or privacy considerations. This classification applies even if there is no law requiring this protection.

“Data” means information created, collected, processed, owned/subscribed to and/or stored on City premises, authorized cloud providers, all City devices and devices under the BYOD program. “Data” means information in any format, including but not limited to:

- Paper Records
- Emails
- Electronic documents
- Databases
- Audio/video/tape/microfiche

"Data Classification" means the characterization of information based on an assessment of business and operational, legal and regulatory requirements, and the potential impact that a loss of confidentiality, integrity or availability of such information would have on organizational operations, organizational assets, individuals, other organizations and the City.

“Data Governance Working Group” means City staff who are responsible for policy implementation and ongoing program administration.

“Data User” means an employee, elected official, contractor or third-party organization or individual who interacts with, accesses, uses or updates Data for the purpose of performing an authorized task.

“Personal Information” is information relating to an identified or identifiable individual, as defined by the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA). Personal Information includes but is not limited to:

- Race, national or ethnic origin, religion, age, gender, marital or family status
- Education, medical, criminal or employment history
- Identifying numbers, address, fingerprints, and
- An individual's personal opinions except where they relate to another individual

Personal Information does not include an individual’s name, title, work address, work telephone/cell number or position when acting in their business or professional capacity and does not apply to a corporation.

“Personal Health Information” is information relating to a person’s individual health records as in accordance with the requirements of the *Personal Health Information Protection Act* (PHIPA).

“Public” refers to Data that is open to the general public that has no existing local, national or international legal restrictions on access.

“Restricted” refers to Data protected by law or by City policies, procedures or regulations. This classification also represents Data that by default is not protected by law, but for which the information owner has exercised their right to restrict access.

“Sensitive” refers to Data intended only for employees and approved non-employees such as contractors, vendors or third-party organizations. Sensitive information is normally not accessible by outside parties without the organization’s or information owner’s express permission via an executed Data License Agreement.

Legislative Requirements

This policy is written in compliance with the *Municipal Freedom of Information and Protection of Privacy Act*, (MFIPPA), as amended and the *Personal Health Information Protection Act* (PHIPA), as amended.

Related Policies/By-Laws

Records Retention By-law 0097-17
Open Data Program Policy
Access to and Acceptable Use of Information Technology Resources
Bring Your Own Device (BYOD)

Data Handling Instructions

Data are classified into the following categories: Public, Sensitive, Restricted and Confidential. Data are classified at all stages of their lifecycle and may change over time. For example, a document may be Restricted in draft format but become Public once finalized and approved. All Data are to be handled in accordance with the following Data Classification and related Data handling instructions.

Data Classification: Public		
Description	**Examples**	**Data Handling Instructions**
Information that may be viewed by all members of the public. Information	• Publically posted media releases • Council Agendas	Data In Use Access is widely available and can be accessed by the public.
exposed **expected to cause low impact to the organization.**	• Council Minutes • Open Data • Approved website content	Data in Transit Can be transferred by email
		Data at Rest May be stored on City approved devices, BYOD devices/websites/ cloud environment. There are no restrictions on printing and copying the Data, with the exception of copyright restrictions Data Disposal No disposal restrictions after considering retention requirements

Data Classification: Sensitive		
Description	**Examples**	**Data Handling Instructions**
Information that may be seen by all City staff but would not normally be available outside of the City. Information exposed **may result in minimal enterprise impact or loss of reputation**	• Data used by employees during the course of work, such as internal reports, procedures and memorandums • Policy interpretations • Internal procedure manuals (SOPs) •)	<u>Data In Use</u> Access is not available outside of the City network or outside of an approved cloud environment <u>Data In Transit</u> Can be transferred unencrypted internally within City's network but must be encrypted when transferred externally. Can be transferred by email to City staff <u>Data at Rest</u> Should be stored on a City network and/or an approved cloud environment. Due care should be taken if information is transferred to any City approved external and/or mobile devices <u>Data Disposal</u> Data must be disposed of in the appropriate manner as per the Records Retention By-law. Consideration should be given to Data Classification, format and retention requirements

Data Classification: Restricted		
Description	**Examples**	**Data Handling Instructions**
Information that is sensitive within the City, with access restricted to City employees only, on a need-to-know-basis. Information exposed **may result in loss of major assets or may impede the City's mission and/or reputation**	• Bid packages • Request for proposal (RFP) submissions • Acquisition strategy • Non-disclosure agreements (NDAs)	<u>Data In Use</u> Access is restricted to staff who need the information to carry out their duties <u>Data In Transit</u> Must be transferred in encrypted format. Can be transferred by email to authorized staff only and marked "Restricted". Information should not generally be transferred to external and/or mobile devices but if essential then encryption must be used <u>Data at Rest</u> Information must be held within a City network and/or approved cloud environment in locations with restricted access and appropriate security <u>Data Disposal</u> Data must be disposed of in the appropriate manner as per the Records Retention By-law. Consideration should be given to Data Classification, format and retention requirements

Data Classification: Confidential		
Description	**Examples**	**Data Handling Instructions**
Information that is extremely sensitive within the City and accessible only to designated or relevant members of staff due to its potential impact on the City. This includes Personal Information and Personal Health Information that is subject to FIPPA, MFIPPA, and PHIPA .	• Human resources information, including: – Recruitment information – Training records – Employee salaries not covered in the *Public Sector Salary Disclosure Act* – Medical records	<u>Data In Use</u> Access is strictly limited to authorized personnel only. Documents must be labelled “Confidential” (e.g. by watermarking)
If disclosed or otherwise compromised, **could reasonably be expected to affect or cause an injury to any of the interests listed in MFIPPA, including: personal information that could cause embarrassment to an individual; information that could cause economic loss to a privately or publicly owned corporation; and information that could significantly reduce the level of public trust in the City; discredit the City’s reputation, lessen the City’s competitive advantage, reduce the City’s revenue-generating potential or disclose the City’s intellectual capital to potential competitors**	• Financial information including strategy plans • Legal information, including contracts • User credentials • High-value intellectual property • Minutes of in-camera Council meetings • Testing and auditing procedures • Payment Card Information (PCI) data • Biometric data such as fingerprint scans	<u>Data In Transit</u> Must be transferred in encrypted format. Can be transferred by email to authorized staff only and marked “Confidential” <u>Data at Rest</u> Information must be held only within restricted City networks and/or approved cloud environment and protected with secure credentials, encryption and protected with granular access controls <u>Data Disposal</u> Data must be disposed of in the appropriate manner as per the Records Retention By-law. Consideration should be given to Data classification, format and retention requirements

Roles and Responsibilities

Directors

Directors are responsible for:

- Ensuring all applicable managers/supervisors are aware of this policy and of any subsequent revisions
- Ensuring compliance with this policy
- Informing the applicable commissioner when made aware of a Data breach, and
- Fostering a Data handling culture of security while maximizing Data value

Manager/Supervisor

Managers/supervisors are responsible for:

- Fostering a Data handling culture of security while maximizing Data value
- Ensuring applicable staff are aware of this policy, along with related training materials
- Ensuring staff comply with this policy
- Reporting breaches to the Data Governance Working Group and informing the applicable director
- Providing direction to staff, as required, and
- Ensuring that contracts and agreements with consultants and third-party organizations abide by this policy

Data User

Data Users are responsible for:

- Complying with this policy
- Reporting instances of non-compliance with this policy to the applicable manager/supervisor, and
- If needed, seeking clarification from management on Data handling procedures

Data Governance Working Group

The Data Governance Working Group is responsible for:

- Oversight of the implementation of this policy, logging and resolving issues
- Establishing corporate-wide training standards
- Administrating and storing all Data License Agreements with non-City contractors or third-party organizations
- Establishing Data Governance guidelines/framework (e.g. processes to follow, what to store, where to store, protocols, etc.)
- Investigating Data breaches in consultation with the Access and Privacy Officer, Office of the City Clerk, Corporate Services Department, Legal Services Division, City Manager’s Office and the IT Security Section, IT Division, Corporate Services Department, and
- Documenting and maintaining a list of all Data breaches

Compliance

Any employee who fails to comply with this policy may be subject to appropriate disciplinary action, up to and including termination of employment.

Revision History

Reference	Description
Enter previous review - e.g. GC-1234-2015	Click here to enter text.