Acceptable Use of Information Technology Policy

Policy Number	POL-2
Effective	August 13 2001
Review Date	January 20 2018
Final Approver	Corporate Management Team
Training Course Code	CCAUIT
Document State	CURRENT

1.0 Purpose

This policy establishes standards for the use of the City's IT in compliance with the law and City policies including but not limited to the Employee Code of Conduct Policy, the Recorded Information Management Policy and Records Retention Bylaw and MFIPPA. The goal of this policy is to ensure that IT is used wisely and to protect the City from damaging, inappropriate or illegal activity that may compromise the City, its reputation or the integrity of its systems, networks, information and services.

2.0 Persons Affected

2.1 This policy applies to:

2.1.1 employees volunteers, students, Vendors and anyone using the City's IT or any third party with whom the City has a service level agreement to provide IT;

2.1.2 the CMT;

2.1.3 the CIO; and

2.1.4 Supervisors/Managers/Directors.

3.0 Policy Statement

3.1 It is the policy of the City to ensure that:

3.1.1 IT shall be used primarily for City business purposes;

3.1.2 IT shall be protected from illegal or damaging activity;

3.1.3 IT shall be used efficiently and effectively while being maintained and preserved;

3.1.4 IT shall not be used to copy, transmit, process or store information that is harmful including information that is discriminatory, defamatory, harassing, insulting, offensive, pornographic or obscene or that violates copyright law;

3.1.5 confidential or proprietary corporate information shall be protected from unauthorized access and used in accordance with applicable policies, regulations and the law;

3.1.6 use of IT and/or access to corporate information shall be authorized by the City;

3.1.7 the purchase of new IT shall be in accordance with the Purchasing Policies and Procedures Bylaw 2000-134; and

3.1.8 personally owned technology shall not be used by an employee for City business, unless authorized.

Employees

3.2 Any employee who breaches this policy may be subject to discipline up to and including dismissal.

4.0 Responsibilities

4.1 CMT members are collectively and individually responsible for approving and directing compliance with this policy.

4.2 The CIO:

4.2.1 shall receive and resolve any conflicts, issues or concerns relating to this policy;

4.2.2 shall establish procedures, protocols and controls to safeguard the availability and acceptable use of Information Technology;

4.2.3 may monitor IT, for the purposes of systems administration and support at his/her discretion, at any time, without notice to the user, and without the user's knowledge;

4.2.4 shall investigate and report the use of IT that may be involved in a suspected security breach, contravention of City policies or the law; and

4.2.5 shall, in consultation with the Clerk where required, ensure the confidentiality, integrity and accessibility of data collected in accordance with the law.

4.3 All users shall:

4.3.1 use IT in a respectful and ethical manner that is consistent with the law and the City's policies, including the Employee Code of Conduct Policy, the Recorded Information Management Policy and Records Retention Bylaw and MFIPPA;

4.3.2 report any suspected breach of security or contravention of this policy to the CIO; and

4.3.3 not misuse IT or attempt to circumvent or subvert IT security measures.

4.4 Supervisors/Managers/Directors, in their respective department or division shall:

4.4.1 implement and provide training on this policy and related procedures to their employees;

4.4.2 assign IT and authorize access to employees as required for operations;

4.4.3 report any breach of this policy to the CIO; and

4.4.4 ensure all employees, contractors, consultants, business partners and other authorized users comply with this policy.

4.5 Employees shall:

4.5.1 not use IT for personal use that in any way interferes with their work or City business;

4.5.2 keep IT secure and free from damage or loss; and

4.5.3 report theft, loss or unauthorized disclosure of confidential or proprietary information to his/her supervisor immediately.

Breach of Policy

4.6 Employees are responsible for compliance with this policy and shall be aware that any employee who breaches this policy may be subject to discipline up to and including dismissal.

5.0 Approval Authority

Role	Position	Date Approved
Quality Review	Research & Policy Analyst	12/10/2015
Subject Matter Expert	CIO	12/04/2015
Legal Review	Senior Legal Counsel	12/04/2015
Final Approval	CMT	01/06/2016

6.0 Revision History

Effective Date	Revision #	Description of Change
11/06/2013	1	CIO comprehensive review

01/06/2016	2	comprehensive reivew and transferred to new corporate policy template (formerly computer use policy)
11/09/2016	3	section 3.2 and 4.6 amended as per direction from Director, Legal Services. Previous wording: 3.2 Any employee who breaches this policy may be subject to review under the Code of Conduct and/or discipline proceedings up to and including dismissal. 4.6 Employees shall be aware that non-compliance of this policy is subject to discipline, up to and including dismissal. as directed and approved by the Director of Legal Services
11/30/2016	4	added new section 3.1.7 re: IT purchases and 3.1.8 re: use of personally owned technology changed "contractor of the City" to "Vendor" in section 2.1.1 as requested and approved by the CIO
01/20/2017	5	annual review. no changes
05/05/2017	6	edited title of Employee Code of Conduct Policy (was Code of Conduct Policy)

7.0 Appendix

Information for this section has not yet been provided.

Related Definitions

Vendor
as per the Purchasing Bylaw 2000-134, as amended, means any party selected to provide Goods or Services to the City.

MFIPPA
means the Ontario Municipal Freedom of Information and Protection of Privacy Act, 1990 that governs how the City collects, uses, discloses and disposes of information and Records.

IT
means Information Technology and the City's digital applications and systems, including computing, telecommunications infrastructure and end user devices used for the creation, processing, transmittal and storage of data.

CMT
means the Corporate Management Team.

Clerk
means the person appointed by the City as the Clerk in accordance with section 228(1) of the Municipal Act, 2001.

City
or Corporation means The Corporation of the City of Kingston.

CIO
means the Chief Information Officer.

Related information

Recorded Information Management Policy and Records Retention Schedule Bylaw - 2008-182

Application Login Security Procedure

Purchasing Policies and Procedures Bylaw - 2000-134

Employee Code of Conduct Policy

How Do I...

Protect my computer password

Find technical support

Start a corporate technology project with IS&T