KENTISH COUNCIL POLICY

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

Policy Number 02:26:2010

POLICY NUMBER	02:26:2010
OBJECTIVE	To ensure that electronic communications are properly used and are protected from a variety of threats, such as inappropriate use, fraud, copyright violation and sabotage
STATUTORY AUTHORITY	*Local Government Act 1993*
POLICY	Adopted 21/09/2010 Minute No 7.1.2 Reviewed 17/11/2015 Minute No 11.4.5
RECORD INFORMATION	This Policy replaces the following documents listed in the Kentish Council Human Resource Management Policy # 02:02:2002: - Electronic Communications Policy - Internet, Email and Passwords Policy - Use of Personal Computers Policy
REVIEW	The effectiveness of this policy will be reviewed every two years.

1. INTRODUCTION

Computer information systems and networks are an integral part of operations at Kentish Council. Council has made a substantial investment in human and financial resources to create these systems.

The enclosed policies and directives have been established in order to:

- Protect this investment.
- Safeguard the information contained within these systems.
- Reduce business and legal risk.
- Protect the good name of the Council.

2. SCOPE

This policy applies to all users of Council information systems. Reference to employees in the context of this policy should, where relevant, be read as reference also to Elected Members of Council.

3. VIOLATIONS

Violations may result in disciplinary action in accordance with Council and ASU guidelines. Failure to observe these guidelines may result in loss of access and / or disciplinary action, depending upon the type and severity of the violation, up to and including termination of employment, as well as criminal penalties whether it causes any liability or loss to Council, and / or the presence of any repeated violation(s).

4. CONTENTS

The topics covered in this document include:

- Statement of responsibility
- The Internet and e-mail
- Personal Information Protection Policy
- Computer viruses
- Spyware
- Access codes and passwords
- Physical security
- Copyrights and license agreements

5. STATEMENT OF RESPONSIBILITY

General responsibilities pertaining to this policy are set forth in this section. The following sections list additional specific responsibilities.

a. Manager responsibilities

Managers and supervisors must:

1. Ensure that all appropriate personnel are aware of and comply with this policy.
2. Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.

b. Corporate Services Department responsibilities

The IT Officer must:

1. Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policy directives.
2. Provide appropriate support and guidance to assist employees to fulfil their responsibilities under this directive.

6. THE INTERNET AND EMAIL

The Internet is a very large, publicly accessible network that has millions of connected users and organisations worldwide.

a. Policy

Access to the Internet is provided to employees for the benefit of Kentish Council. Employees are able to connect to a variety of business information resources around the world.

Conversely, the Internet is also replete with risks and inappropriate material. To ensure that all employees are responsible and productive Internet users and to protect the Council's interests, the following guidelines have been established for using the Internet and e-mail.

b. Acceptable use

Employees using the Internet are representing the Council. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

- Using Web browsers to obtain business information from commercial Web sites.
- Council research activities.
- Accessing databases for information as needed.
- Review of local government related web sites.
- For professional development and training.
- Using e-mail for business contacts.

c. Acceptable Personal use

Occasional or incidental personal use is permissible so long as, in the Council's estimation:

- It does not consume more than a trivial amount of resources;
- It does not result in disruption to any systems;
- It does not harm the Council's reputation;
- It does not represent personal opinions as those of the Council;
- It does not interfere with employee productivity; and
- It does not pre-empt, interfere or conflict with any business activity.

d. Unacceptable use

Employees must not use the Internet for purposes that are illegal, unethical, harmful to the Council, or non-productive. Examples of unacceptable use are:

- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
- Broadcasting e-mail, i.e., sending the same message to more than 10 recipients or more than one distribution list.

- Conducting a personal business using Council resources.
- Transmitting any content that is offensive, harassing, or fraudulent.
- Using your Council email to subscribe to newsletters and websites which do not relate to your work for Council. EG. Social media sites including Facebook, Ticketek, Ticketmaster, Weight loss sites, retail newsletters, eBay, flight and accommodation bookings etc. All council email addresses and email content remain the property of Kentish Council and are only permitted to be used by the individual and not any third party clients.

e. Downloads

Executable or installable program file (.exe, .msi etc) downloads from the Internet are **not** permitted unless specifically authorised in writing by the IT Officer or employee's Director. Particular care must be taken with **any** downloads from unknown or un-verified sources. If in doubt, seek advice from ICT officers prior to downloading.

f. Employee responsibilities

An employee who uses the Internet or Internet e-mail shall:

1. Ensure that all communications are for professional reasons and that they do not interfere with his/her productivity.
2. Be responsible for the content of all text, audio, or images that (s)he places or sends over the Internet. All communications should have the employee's name attached.
3. Not transmit copyrighted materials without permission.
4. Know and abide by all applicable Council policies dealing with security and confidentiality of Council records.
5. Run a virus scan on any executable file(s) received through the Internet.
6. Ensure that they protect their email address by subscribing to newsletters and websites, only for Council related work and information.
7. Avoid transmission of non-public customer information. If it is necessary to transmit non-public information, employees are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorised to receive such information for a legitimate use.

g. Copyrights

Employees using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by Council and/or legal action by the copyright owner.

h. Monitoring

All messages created, sent, or retrieved over the Internet are the property of Council and *may be regarded as public information*. Kentish Council reserves the right to access the contents of any messages sent over its facilities if Council believes, in its sole judgment, that it has a business need to do so.

Council may also access an employee's Mailbox at any time for the purpose of ensuring that the required process of the Council can be carried out (eg if an employee is absent, moved or left employment).

All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the

receiver. Employees have no guarantee of privacy when using Council provided computing resources or the Internet. **This means don't put anything into your e-mail messages that you wouldn't want to see on the front page of the newspaper or be required to explain in a court of law.**

i. Breaches

All material viewed via the internet is copied to a proxy server; therefore material can be traced to the requester. Therefore, it is imperative not to breach the Council's Code of Conduct as the Council and yourself can be embarrassed.

7. PERSONAL INFORMATION PROTECTION POLICY

Council currently has a separate Personal Information Protection Policy in compliance with the Personal Information Protection Act, 2004. Employees are required to read this policy and conform to Council's Policy Statement.

8. COMPUTER VIRUSES

Computer viruses are programs designed to make unauthorised changes to programs and data. Therefore, viruses can cause destruction of corporate resources.

***a.* Background**

It is important to know that:

Computer viruses are much easier to prevent than to cure.
Defences against computer viruses include protection against unauthorised access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

b. IT responsibilities

IT shall:

1. Install and maintain appropriate antivirus software on all computers.
2. Respond to all virus attacks, destroy any virus detected, and document each incident.

c. Employee responsibilities

These directives apply to all employees:

1. Employees shall not knowingly introduce a computer virus into Council computers.
2. Employees shall not load items of unknown origin.
3. Portable media shall be scanned for viruses before they are read.
4. Any employee who suspects that his/her workstation has been infected by a virus shall **immediately power off** the workstation and call the IT Officer.

9. SPYWARE

Spyware and adware can compromise system performance and allow sensitive information to be transmitted outside the organisation. Spyware installation programs can launch even when users are performing legitimate operations, such as installing a Council-approved application. As a result, combating spyware requires user vigilance as well as IT management and control.

a. **IT responsibilities**

1. Install and update appropriate anti-spyware software on all computers.
2. Respond to all reports of spyware installation, remove spyware modules, restore system functionality, and document each incident.

b. Employee responsibilities

These directives apply to all employees:

1. Employees shall not knowingly allow spyware to install on Council computers.
2. Employees shall perform anti-spyware updates and run anti-spyware programs regularly, as directed by the IT Officer.
3. Employees shall immediately report any symptoms that suggest spyware may have been installed on their computer.

10. ACCESS CODES AND PASSWORDS

The confidentiality and integrity of data stored on Council computer systems must be protected by access controls to ensure that only authorised employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties.

a. IT responsibilities

The IT Officer shall be responsible for the administration of access controls to all Council computer systems. The IT Officer will process adds, deletions, and changes upon receipt of a written request from the end user's supervisor.

Deletions may be processed by an oral request prior to receipt of the written request The IT Officer will maintain a list of administrative access codes and passwords and keep this list in a secure area.

b. Employee responsibilities

Each employee:

1. Shall be responsible for all computer transactions that are made with his/her User ID and password.
2. Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that others know them. Passwords should not be recorded where they may be easily obtained.
3. Will change passwords in accordance with the prevailing ICT password management procedures.
4. Should use passwords that will not be easily guessed by others.
5. Should log out when leaving a workstation for an extended period or setup a password-protected screensaver.
6. Should not attempt to access the accounts of other users.

c. Manager's responsibility

Managers and supervisors should notify the IT Officer promptly whenever an employee leaves Council or transfers to another department so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination.

11. PHYSICAL SECURITY

It is Council policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorised access, and environmental hazards.

a. Employee responsibilities

The directives below apply to all employees:

1. Portable storage devices should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up.
2. Servers, storage, network and other business critical devices should be held in limited-access, secured locations accessible only to authorised employees. Such devices should be protected by an uninterruptible power supply (UPS). A surge suppressor should protect other computer equipment.
3. Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.
4. Since the IT Officer is responsible for all equipment installations, disconnections, modifications, and relocations, employees are not to perform these activities. This does not apply to temporary moves.
5. Employees shall not take shared portable equipment such as laptop computers out of the office without the informed consent of their Director or IT Officer. Informed consent means that the IT Officer knows what equipment is leaving, what data is on it, and for what purpose it will be used.
6. Employees should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may result.

12. COPYRIGHTS AND LICENSE AGREEMENTS

It is Kentish Council's policy to comply with all laws regarding intellectual property.

a. **Legal reference**

Kentish Council and its employees are legally bound to comply with all proprietary software license agreements. Non-compliance can expose Kentish Council and the responsible employee(s) to civil and/or criminal penalties.

b. ***Scope***

This directive applies to all software that is owned by Kentish Council, licensed to Kentish Council, or developed using Kentish Council resources by employees or vendors.

c. ***IT responsibilities***

The IT Officer will:

1. Maintain records of software licenses owned by Kentish Council.
2. Periodically (at least annually) scan Council computers to verify that only authorised software is installed.

d. ***Employee responsibilities***

Employees shall not:

1. Install software unless authorised by IT. Only software that is licensed to or owned by Kentish Council is to be installed on Kentish Council computers.
2. Copy software unless authorised by IT.
3. Download software unless authorised by IT.

e. Violations

Violations of copyright law may expose Council and the responsible employee(s) to significant civil and criminal liabilities, including but not limited to:

- Liability for damages suffered by the copyright owner
- Profits that are attributable to the copying