# Canvey Island Town Council

## Computer and Information Security Policy

The spread of electronic communications and access to multiple sources of information and access through the internet is an increasingly necessary part of work for everyone. This accessibility brings huge advantages, but also brings risks in its wake that need to be taken into account.

You are responsible for the security and proper use of your computer hardware, software and data and must ensure that you comply with the General Data Protection Regulations and Council policies. It is important to understand security concepts and be aware of the policies, procedures, rules and guidelines concerning their use and security. These are described in this policy with additional material being circulated from time to time in the future. The policy includes computers and mobile phones.

All computers provided by the Council must not be used for Personal use and are the property of Canvey Island Town Council and shall only be used with the council's best interests in mind. As such, they shall **not** be used for the access or distribution of material considered obscene.

The Council recognises that access to professional information by e-mail, fax or through web sites is a necessary requirement of the job of the Clerk to the Council and other staff and is permitted. Staff and users are expected to use technology in a courteous, reasonable and responsible manner.

The following activities are not acceptable and anyone found to be involved in them may face disciplinary action and in certain instances the matter will be considered to be gross misconduct:

- Receiving, sending, or displaying offensive messages or pictures
- Using obscene, threatening or violent language
- Improper use of e-mail and mobile phones
- Damaging computers, computer systems or computer networks
- Violating copyright laws
- Intentionally wasting limited resources
- Employing the system for commercial purposes, including gambling
- Employing the system for illegal activities

Be careful when addressing email – know who you are sending to and apply common sense before assuming a message is valid (Mail and news can be forged).

The Council encourages electronic communications with local, national and international organisations. The Council cannot control and is not responsible for the accuracy or content of information gathered over the Internet. Security is maintained by appropriate software, internal computer security settings and passwords.

It is a requirement of the Council and the duty of all staff to avoid deliberate use of the Council's Internet connections and technology for inappropriate personal use. Staff should immediately alert the Town Clerk of any suspect material found stored on any computer or elsewhere on the premises.

The computer equipment and software must be used as installed. Staff and users may not install / uninstall, delete or change anything on Council computers. Any requirements to change anything should be authorised by the Town Clerk. The Council uses a virus-checker on the computers. Staff are forbidden to load disks that

have not been virus checked by the system. This includes but is not limited to ipods, USB keys/sticks, pen drives, data vaults, MP3/media players, Flashcards and PDA's.

Access to chat rooms and gaming are not permitted on Council computers.

***Canvey Island Town Council maintains its right to inspect any and all files stored in private and or common access areas of its network, on individual computer hard drives as well as all removable peripheral equipment (e.g. mobile phones, memory sticks, zip discs, floppy discs, CDs etc.) and may implement monitoring systems that help manage the use of its Internet and e-mail systems.***

***All email correspondence should be kept and maintained securely and under no circumstance should any correspondence be deleted unless deemed as junk mail or in line with the Councils Retention and Disposal Policy.***

***Canvey Island Town Council places a high level of trust on employees to observe the requirements of this Policy, however if there is any evidence that this Policy is being abused, Canvey Island Town Council reserves its right to investigate alleged breaches and take appropriate disciplinary action in accordance with its Disciplinary Procedures.***

***Copyright***

***The Copyright, Design and Patents Act 1988 is applicable to all types of creations, including software programs, databases, text, graphics and sounds by an author or an artist. This will include any that are accessible through the Councils IT facilities. Only software authorised by the Council and for which a valid license has been purchased should be installed on a Council PC or laptop. Any uploading or downloading of information which is not authorised by the copyright owner or any substantive extraction of information from a database which is not authorised by the database owner will be deemed to be an infringement of their rights.***

***Some types of infringement give rise to criminal offences, the penalties for which may amount to a term of imprisonment or an unlimited fine. It is also possible for the copyright owner to claim compensation or to have infringing activities prevented by injunction.***

***Employees must not make, transmit or store an electronic copy of copyright material without the permission of the owner.***

***Security***

***Employees are required to observe the following:***

a) ***PCs / Terminals should be logged off the network when left unattended for any period of time. They should be switched off on leaving in the evening. PC's holding sensitive data must have a password installed.***
b) ***Where employees are provided with computers/phones, which are portable in nature they must ensure that such devices, when not in use in the office or at home or when traveling are safeguarded against accident and theft when in transport. If left in a vehicle for any time they must be secured in a locked boot.***
c) ***Where employees are provided with User-I.D.'s and passwords to access the Councils computer systems, they must not be disclosed to anyone, unless expressly directed to do so by the Town Clerk.***

d) ***All passwords will be kept by the Town Clerk and secured in a sealed envelope signed by the Town Clerk. This envelope should not be opened by any person apart from the Town Clerk or Town Mayor to the Council.***
e) ***In the event that an employee encounters a computer virus, or suspects that they have, they should leave the computer as it is and immediately contact the Town Clerk. Under no circumstances should the suspected infected computer be utilised.***
f) ***Only the Town Clerk can change or authorise changes to hardware or software configurations.***
g) ***All data media e.g. floppy disks, tapes etc that are obsolete must be destroyed on site.***
h) ***Users of portable and stand alone computers are responsible for the backup of data held and ensuring that adequate virus scanning software is in use.***
i) ***Record playback facilities on the keyboards must not be used for log on procedures.***
j) ***Employees are responsible for keeping your PC / laptop and mobile phone in a good state of cleanliness and ensure that they are not adorned with unnecessary decoration. Employees should take all reasonable steps to ensure that computers and data media are not exposed to damage from spillages.***

**THIS POLICY MUST BE COMPLIED WITH AT ALL TIMES.**

I have read the above policy and agree to abide by these instructions.
I will discuss any concerns with the Town Clerk.

Signed ……..

Print Name …… Date ……../……/……

(Staff are issued with two copies of this policy, one to retain and one to sign and return to the Town Clerk.)

*Note: This policy has been based on advice from the Society of Local Council Clerks and their understanding of the law and practice at the present time.*

Amended by Full Council 21st May 2018 – next review date May 2022 or when regulations change