PURPOSE

To ensure the security and proper use of the Town of Weymouth's telecommunications systems which includes the network, computers and peripherals, telephones, electronic mail (e-mail), facsimile machines (faxes) and the Internet.

POLICY

The Town of Weymouth provides staff with the ability to send messages and information through voice mail, fax mail, electronic mail (e-mail) and in some cases through the Internet. It is the policy of the Town of Weymouth to support the Internet Service access and email access policies of its suppliers on the Internet and email connectivity, and the Town of Weymouth will enforce those policies to the best of its ability. The Town of Weymouth also supports those elements of Internet and email polices that demand network etiquette and due consideration for user's rights to privacy and freedom from exposure to offensive material.

Internet /E-mail Usage Policy

The following policy statements apply to all users (employees, contractor, temporaries, etc.) who use the Internet and/or email with the Town of Weymouth's computing or network resources, as well as those who represent themselves as being connected with the Town of Weymouth in any way:

Electronic Communication and Computer Storage Systems are the property of the Town Data messages should be treated as confidential by other employees and should be accessed only by the intended recipient. Employees are not authorized to retrieve or read any messages or data that are not sent to them unless the intended recipient gives express permission. Also, employees should not use a code, access a file, or retrieve any stored information unless authorized to do so.

The Town of Weymouth allows exploration of the Internet and email usage, but if it is for personal purposes, it should be done on personal, not Town of Weymouth time. Use of computing resources for these personal purposes is permissible as long as it **is not** excessive and:

a. does not interfere with worker productivity; or
b. does not pre-empt any business activity.

c. Does not require the Town of Weymouth to incur any additional cost

Beyond the preceding stipulations it will be up to the individual department head or designee to determine excessive personal use.

Employees are reminded that the Internet and email systems are unsecured Communication mediums and data are not encrypted. Likewise, contact made over the Internet or via email should not be trusted with Town of Weymouth confidential information.

Any user approved for Internet or email access may connect to, view and print any Web page with a Town of Weymouth-related business purpose.

Due to the escalating numbers of extremely destructive viruses now being spread via email, e-mail attachments that are received from an unknown party should be considered suspicious, and should not be opened until the sender's identity can be confirmed. If special circumstances require the opening of the attachment it is suggested that it be saved to floppy disk in Drive A: and done so with extreme caution.

Users should clearly understand that they represent the Town of Weymouth, not themselves, on the Internet or in email when posting from or corresponding through the Town of Weymouth's resources. The same personnel policies that now guide actions with the media (i.e. television, radio, magazines, and newspapers) should be followed when posting information to the Internet or corresponding through the Town of Weymouth's email system. All communication should be regarded as "on the record" and attributable to the employee who posts, creates or forwards the information.

Some Internet sites offer files for download through their Web page. Although you may be presented with opportunities to download files, the Town of Weymouth strongly recommends that you avoid doing so. Downloading files risk consuming an excessive amount of system resources and computer viruses.

If downloading a file appears unavoidable, use discretion in judging the business use of the file and to respect copyright and licensing restrictions.

All files downloaded via the Internet must be scanned with virus detection software prior to being loaded on to the network.

If you have questions as to the risks involved in downloading files, contact the Information Technology Department or your local Network Administrator.

Electronic communication users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the Town of Weymouth. Neither should they construct a communication so it appears to be from someone else (false identity).

Internet sessions should not remain open when not actively being used.

The following activities are strictly prohibited:

a. Any use which violate U.S. state or federal regulations and civil laws
b. The transmission of materials used for commercial promotion, product endorsement, or political purposes
c. Attempts to violate the computer security systems implemented by the Town of Weymouth or other institutions, organizations, companies or individuals
d. Transmission of threatening or harassing messages
e. Accessing or sharing pornographic, sexually explicit or obscene materials
f. Interference with or disruption of network users, services or equipment
g. Propagation of Computer Viruses, Worms, Trojans or malicious Code.
h. Users may not, under any circumstances use, "*spoofing*" or "*spamming*", or any other means to disguise their identities in sending e-mail. (*Spoofing* is frequently used to hide the identity of a *spammer* or of someone who is committing unauthorized or illegal acts online). (*Spamming* is the sending of unsolicited commercial e-mail.)
i. Any activity which would either violate a Town Employee's or resident's right to privacy or expose the Town of Weymouth to financial loss
j. Activities which could expose the Town of Weymouth to financial loss, embarrassment or penalties
k. Electronic communications to non-City bulletin boards note pads and messages services with any Town of Weymouth equipment is prohibited, unless it is directly related to the user's job responsibilities.
l. to distribute chain letters
m. to access on-line gambling sites
n. to libel or otherwise defame any person
o. Mass mailing messages to parties outside of the Town of Weymouth unless prior permission has been obtained from their department head or department designee
p. Subscription to mass mailing list resulting in the receipt of daily e-mail should be limited to business purposes only.

Monitoring Access:

The Town of Weymouth reserves the right, at its discretion, to view, capture and use Internet and/or email correspondence, personal file directories and other information stored on its Town of Weymouth owned equipment. This may be necessary in order to support operational, maintenance, auditing, security and investigative activities and to comply with subpoenas and orders of courts and administrative agencies. The Town of Weymouth may read any messages or other data stored on Town of Weymouth owned equipment for any purpose, without limitation, including systems maintenance and compliance monitoring. Employees should not assume that voice mail, fax mail, email messages or Internet postings are personal or confidential. Electronic communications may be discoverable even though the messages have been deleted. Subject to certain exception in the law, electronic communications may also be considered public records. In recognition of the fact that the Town of Weymouth may perform these activities, users should pattern their Internet and email use accordingly.

Revoking Access:

Use of the Internet by the Town of Weymouth's employees and hired staff is a privilege, not a right, and may be revoked at any time for inappropriate conduct. All users of the Internet are responsible for complying with the policies, guidelines and standards of conduct contained in this document. Violations may result in a revoking of Internet access privileges and or disciplinary measures.

Equipment Hardware/Software Usage Policy

Settings on all hardware, including all personal computers, laptop computers, printers, scanners and monitors shall not be changed without the authorization of the Information Technology Department or Network Administrator.

No one may add or modify software or change the configuration on computers under control of the Town of Weymouth without written approval from the Information Technology Department. Only properly licensed software may be used. Pirated or illegally copied software shall not be installed to any computer.

No one shall move or install hardware without prior notification and permission from the Information Technology Department.

The purchase of all computer and related peripheral equipment must be authorized by the Department Head or designee, and submitted to the Information Technology Department for final review and approval before purchase. This is to adhere to License Agreements, and Avoidance Regulations and standards set by the Town of Weymouth to ensure security and compatibility with the network and current system configurations.

Individually assigned Personal Computer Systems should not be used to create any offensive or disruptive messages or images. Among those which are considered offensive are any messages or images which contain sexual implications, racial slurs, gender-specific comments, or any other comment which might constitute intimidation,

hostile or offensive material based on one's sex, race, color, national origin, age, religion, sexual orientation or physical or mental disability.

Upon the request of the department head and subject to approval of the appropriate authority, monitoring of individually assigned personal computer systems may be necessary. Reasons for monitoring include, but are not limited to, review of employee productivity, investigations into claims of possible criminal activity and investigations into violations of this policy.

Executable programs imported from other sites to Town of Weymouth computers must not be used unless they have been authorized by the Information Technology Department and they have been subjected to virus detection procedures approved by Information Technology Department. The Information Technology Department may from time to time impose additional restrictions or regulations on the importing of remote files and such restrictions or regulations shall be considered part of this policy.

The following restrictions apply to the use of all Town of Weymouth computer and peripheral related equipment (including mini, micro, personal and laptop computers) whether use occurs in Town of Weymouth offices or from home or elsewhere through the use of modems:

a. Except as specified below, only use of valid, Town of Weymouth licensed commercial software is permissible.
b. Unlicensed (Non-commercial) software and free software must not be installed or used on the Town of Weymouth equipment, unless it has been reviewed and approved by the Information Technology Department or Network Administrator. ("Non-Commercial" software means software procured from an unlicensed distributor and or not publicly available, and "Free software" means software received without compensation).
c. Unlicensed copies of software must not be installed or used on any Town of Weymouth equipment.
d. All computers must be protected by either hardware or software to prevent unauthorized access and computer viruses. This includes off-premises computers, whether at home, at a consultant's office or elsewhere.

SECURITY

Each person shall maintain the confidentiality of all passwords they are entitled to and shall not use any password or user id that they are not assigned.

No person shall attempt to gain access to programs that the System Administrator or assigning authority has not granted them access to.

Any user who finds a possible security lapse on any system shall report it to the Information Technology Department.

Whenever leaving your PC unattended for extended periods of time log off the network or program you are using so as not to compromise the confidentiality of your work or tie up system resources

Credit Card numbers, telephone calling card numbers, system passwords and other information that can be utilized to gain access to Town of Weymouth services should not be transmitted using the Internet or email.

CONFIDENTIALITY

All Town of Weymouth personnel shall treat as confidential all data and information pertaining to the Town of Weymouth or any past, present or prospective client of Town of Weymouth. In addition, Town of Weymouth personnel have access to proprietary information and documents, either owned or developed by Town of Weymouth or others, including client information, correspondence, business plans, computer programs, training, policy and procedure manuals, and the like. The Town of Weymouth expects that, as a condition of employment, the Town of Weymouth personnel will keep such proprietary information strictly confidential.

Public record laws *guarantee* citizen access to governmental process and require governmental accountability. However, they do not require unlimited access to governmental databases, or direct governmental employees to use their time responding to specialized data requests free of charge. Raw computer data and specialized analyses and reports do not fall within the traditional definition of public records. The Town of Weymouth has established standard and reasonable charges for such reports, electronic products and services. Upon receiving such requests Department Heads should seek the advice of Counsel .

RESPONSIBILITIES

All Town of Weymouth personnel are required to adhere to these policy guidelines. In addition, the Town of Weymouth Department Heads, supervisors and managers are responsible for the following:

a. Ensuring the understanding of, and adherence to, these guidelines within
   their assigned areas of responsibility.
b. Ensuring that individuals in their areas of responsibility understand their obligations in the use of hardware, software, data and computer-related equipment.
c. Notifying data security administrators in the Town of Weymouth Information Technology Department of changes to

their staff, or other matters, which may have an impact on data security.

d. Working closely with the Town of Weymouth Information Technology Department to ensure:

   (a) compliance with established procedures for purchasing software and all related computer hardware,
   (b) the maintenance of a log for the purchase and installation of all software and a library of software licenses, and
   (c) full cooperation with respect to periodic software audits.
   (d) any request for reporting, updating of current software/hardware or enhancements to existing software/hardware should be brought to the Information Technology Department.

ENFORCEMENT

The use of the Town of Weymouth's telecommunication system constitutes employee consent to monitoring of systems and is conditioned upon strict adherence to this policy. Any employee who violates this policy and these guidelines, or uses the Town of Weymouth's telecommunications systems for improper purposes, will result in disciplinary action depending on the circumstances, up to and including immediate termination.

Department heads and supervisors are responsible for ensuring that all their employees using the Town of Weymouth's telecommunication systems have read this policy and understand it applicability to their activities. This policy is not intended to replace day to day administrative procedures specific to each department's operational needs.