12.1 REPEAL OF INFORMATION AND COMMUNICATIONS TECHNOLOGY - CONDITIONS OF USE POLICY - 1.1.1

Attachments: 1. Information and Communications Technology - Conditions of Use policy

RECOMMENDATION

That Council REPEAL the Information and Communications Technology - Conditions of Use policy (1.1.1) at Attachment 1.

PURPOSE OF REPORT:

To seek Council approval to repeal the Information and Communications Technology - Conditions of Use Policy (1.1.1) at **Attachment 1.**

BACKGROUND:

The Information and Communications Technology - Conditions of Use policy was adopted by Council in June 2000 and last amended in November 2010. The policy provides guidelines to City employees and Council Members for the proper use of all information and communications technology facilities, including Internet access, email, facsimile and any other electronic data transfer.

The requirement of provisions outlined in clause 1.3 of the Policy Development and Review Policy were presented to Council Members though the monthly Policy Paper in October 2021.

DETAILS:

The City introduced a new Responsible use of ICT Resources procedure in June 2020. The procedure governs the operational requirements of City employees, volunteers and contract staff who use the City's ICT resources in the execution of their duties. The procedure was last reviewed in September 2021.

Council Members are not within scope of the Responsible use of ICT Resources procedure and are instead guided by the City's Code of Conduct for Council Members, Committee Members and Candidates.

The findings of Administration's review of the Information and Communications Technology - Conditions of Use policy are as follows:

1. The policy is outdated, procedural in nature and is no longer relevant to City processes.
2. For City staff, the policy has been operationally superseded by the City's Responsible use of ICT Resources procedure. The procedure addresses the policy's underpinning principles:
   a. The use of ICT facilities should be consistent with the City's business operations.
   b. Limited personal use is permitted but must not interfere with the City's business operations.
   c. Improper use of the City's ICT facilities will be addressed in accordance with this policy and may lead to disciplinary action, criminal prosecution, or both.
3. For Council Members, the policy is superseded by the City's Code of Conduct for Council Members, Committee Members and Candidates.
4. In addition, the City's Responsible use of ICT Resources procedure addresses the requirements of increasingly mobile City staff with remote work flexibility.

Administration is of the opinion that there is no longer a requirement for a documented City position.
This is consistent with other inner-City councils: City of Perth, City of Subiaco, City of South Perth, Town of Victoria Park.

CONSULTATION/ADVERTISING:

No community consultation is required for the repeal of the policy.

LEGAL/POLICY:

There is no legislative or regulatory requirement for this policy.

Section 2.7(2)(b) of the *Local Government Act 1995* provides Council with the power to determine policies.

The City’s Policy Development and Review Policy sets out the process for the development, review and repeal of the City’s policy documents.

RISK MANAGEMENT IMPLICATIONS

Low: It is low risk for Council to repeal the policy.

STRATEGIC IMPLICATIONS:

This is in keeping with the City’s *Strategic Community Plan 2018-2028*:

<u>Innovative and Accountable</u>

We are open and accountable to an engaged community.

SUSTAINABILITY IMPLICATIONS:

Repealing this policy does not impact on the achievement of specific sustainability outcomes in the *City’s Sustainable Environment Strategy 2019-2024.*

PUBLIC HEALTH IMPLICATIONS:

Repealing this policy does not impact on the achievement of the *City’s Public Health Plan 2020-2025.*

FINANCIAL/BUDGET IMPLICATIONS:

Nil

CITY OF VINCENT

INFORMATION AND COMMUNICATIONS TECHNOLOGY – CONDITIONS OF USE

POLICY NO. 1.1.1

(Adopted at the Ordinary Meeting of Council held on 13 June 2000)

POLICY NO: 1.1.1

INFORMATION AND COMMUNICATIONS TECHNOLOGY – CONDITIONS OF USE

Index

OBJECTIVES 1
POLICY STATEMENT 1
GUIDELINES AND PROCEDURES 3
1. Improper Use of ICT Facilities 3
2. Hardware 3
3. Internet 4
3.1 Introduction 4
3.2 Information Movement 4
3.3 Information Protection 5
3.4 Expectation of Privacy 5
3.5 Resource Usage 6
3.6 Public Representations 6
3.7 Access Control 6
3.8 Reporting Security Problems 8
3.9 Responsibilities 8
3.10 No Warranties 9
3.11 Encounter of Controversial Material 9
3.12 Non Business Related Use of the Internet 9
3.13 Examples of Unethical and Unacceptable Use 10
3.14 Examples of Unacceptable Material 12
4. 4.1 Purchasing 12
4.2 Hardware Standards 13
4.3 Outside Equipment 13
4.4 Relocation of ICT Equipment 13
4.5 Proper Handling of ICT Equipment 13
4.6 Hardware Standards 13
4.7 Outside Equipment 13
4.8 Relocation of ICT Equipment 13
4.8 Proper Handling of ICT Equipment 13
5. Software 14
6. Antivirus 16
6.1 Background 16
6.2 Risk Analysis 17
6.3 Protection – Anti Virus Tools 17
6.4 Virus Outbreak Procedure 17

7. Email/Fax 18
7.1 City of Vincent Property 18
7.2 Authorised Usage 18
7.3 Default Privileges 18
7.4 User Separation 19
7.5 Network Etiquette 19
7.6 User Accountability 19
7.7 No Default Protect 19
7.8 Respecting Privacy Rights 20
7.9 No Guaranteed Message Privacy 20
7.10 Regular Message Monitoring 20
7.11 Statistical Data 20
7.12 Incidental Disclosure 20
7.13 Message Forwarding 21
7.14 Deleting Electronic Messages 21
7.15 Responsibilities 21
7.16 Email Etiquette 22
8. Conditions of Use Agreement 27

POLICY NO: 1.1.1

INFORMATION AND COMMUNICATIONS TECHNOLOGY - CONDITIONS OF USE

OBJECTIVES

To provide~~s~~ guidelines for the proper usage of all information and communications technology facilities including electronic data exchange, via internal and external data networks. It includes: Internet access, E-mail, facsimile and any other electronic data transfer using City of Vincent information and communications technology facilities.

POLICY STATEMENT

This Policy applies to;

(a) all employees of the City whether they are permanent, temporary, seconded or contracted;

(b) Council Members using City equipment.

Persons are accountable for their use of the City's Information and Communications Technology (ICT) facilities. If these facilities are improperly used, persons may be subject to formal disciplinary action and, potentially, criminal prosecutions.

The network and its connections to other networks are to be used only in a manner that is consistent with these purposes and within the spirit of this Policy.

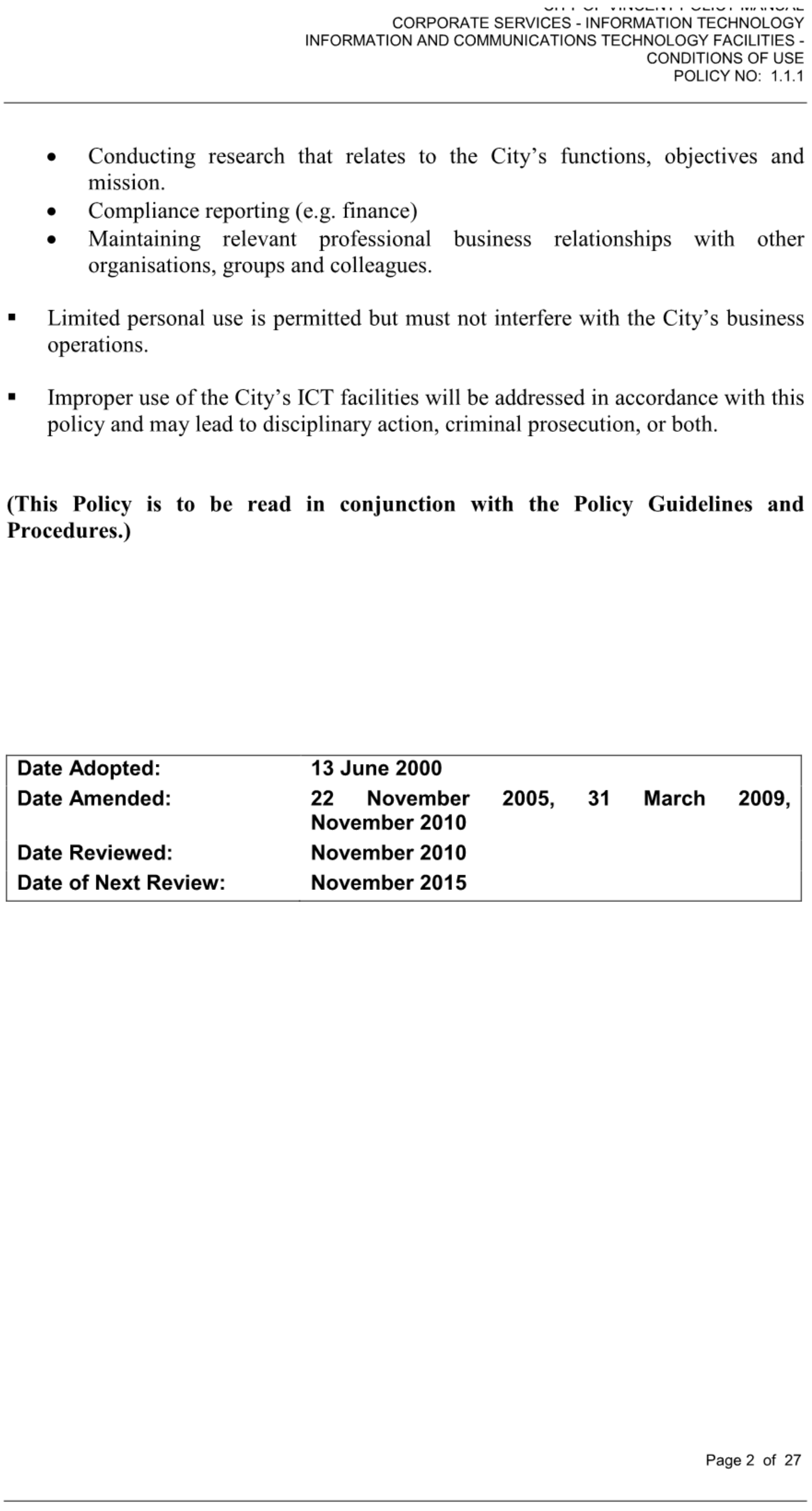
All employees will be required to sign a "Conditions of Use" statement in order to promote a common corporate understanding on acceptable use.

This policy document sets out the City's position on the proper use of its ICT facilities. The principles underpinning the proper use of the City's ICT facilities are:

- The use of ICT facilities should be consistent with the City's business operations.

  This includes, but is not limited to:

  - Access to information that relates to the City's functions, objectives and mission.
  - Access to information that relates to authorised professional employee development.
  - Business communications with external parties and organisations that relate to the City's functions, objectives and mission.



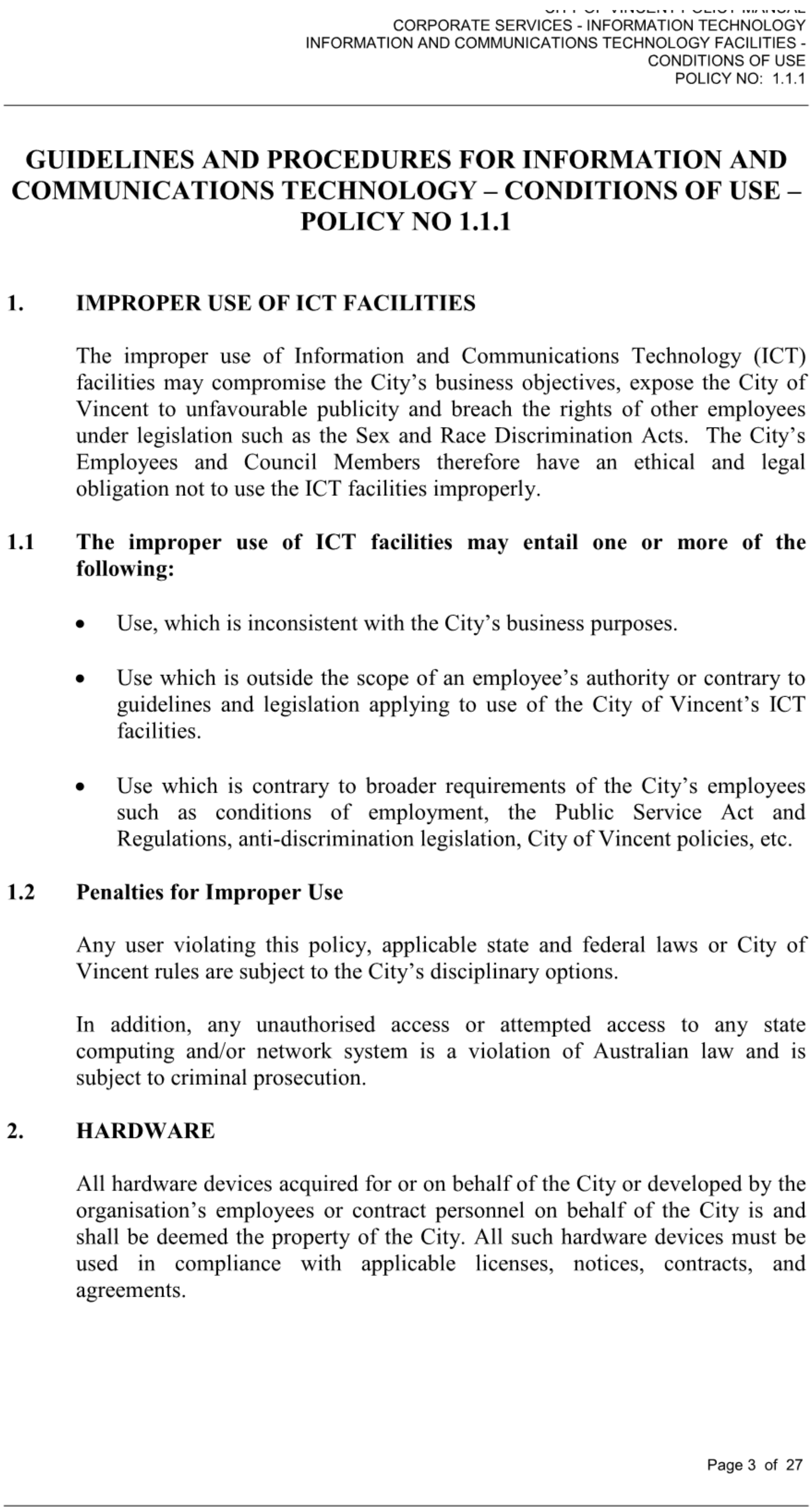
  - Conducting research that relates to the City’s functions, objectives and mission.
  - Compliance reporting (e.g. finance)
  - Maintaining relevant professional business relationships with other organisations, groups and colleagues.

- Limited personal use is permitted but must not interfere with the City’s business operations.

- Improper use of the City’s ICT facilities will be addressed in accordance with this policy and may lead to disciplinary action, criminal prosecution, or both.

(This Policy is to be read in conjunction with the Policy Guidelines and Procedures.)

Date Adopted:	**13 June 2000**
Date Amended:	**22 November 2005, 31 March 2009, November 2010**
Date Reviewed:	**November 2010**
Date of Next Review:	**November 2015**



GUIDELINES AND PROCEDURES FOR INFORMATION AND COMMUNICATIONS TECHNOLOGY – CONDITIONS OF USE – POLICY NO 1.1.1

1. IMPROPER USE OF ICT FACILITIES

The improper use of Information and Communications Technology (ICT) facilities may compromise the City's business objectives, expose the City of Vincent to unfavourable publicity and breach the rights of other employees under legislation such as the Sex and Race Discrimination Acts. The City's Employees and Council Members therefore have an ethical and legal obligation not to use the ICT facilities improperly.

1.1 The improper use of ICT facilities may entail one or more of the following:

- Use, which is inconsistent with the City's business purposes.

- Use which is outside the scope of an employee's authority or contrary to guidelines and legislation applying to use of the City of Vincent's ICT facilities.

- Use which is contrary to broader requirements of the City's employees such as conditions of employment, the Public Service Act and Regulations, anti-discrimination legislation, City of Vincent policies, etc.

1.2 Penalties for Improper Use

Any user violating this policy, applicable state and federal laws or City of Vincent rules are subject to the City's disciplinary options.

In addition, any unauthorised access or attempted access to any state computing and/or network system is a violation of Australian law and is subject to criminal prosecution.

2. HARDWARE

All hardware devices acquired for or on behalf of the City or developed by the organisation's employees or contract personnel on behalf of the City is and shall be deemed the property of the City. All such hardware devices must be used in compliance with applicable licenses, notices, contracts, and agreements.

3. INTERNET

All information travelling over the City's computer networks that has not been specifically identified as the property of other parties will be treated as though it is a corporate asset of the City. It is the policy of City to prohibit unauthorised access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.

In addition, it is the policy of City of Vincent to protect information belonging to third parties that has been entrusted to City of Vincent in confidence as well as in accordance with applicable contracts and industry standards.

3.1 Introduction

The new resources, new services, and interconnectivity available via the Internet all introduce new opportunities and new risks. In response to the risks, this policy describes the City's official policy regarding Internet security. It applies to all users (Council Members, employees, contractors, temporary employees, etc.) who use the Internet with the City's computing or networking resources, as well as those who represent themselves as being connected – in one way or another – with the City.

All Internet users are expected to be familiar with and comply with these policies. Questions should be directed to ITS employees. Violations of these policies can lead to revocation of system privileges and/or disciplinary action, including termination and prosecution.

3.2 Information Movement

Information/files from non-City of Vincent sources via the Internet must be screened with virus detection software prior to being opened or run. If this software contains a virus, worm, or Trojan horse, then ITS employees will attempt to eradicate the problem prior to it doing any damage to the network.

Users must not place City of Vincent material (software, internal memos, etc.) on any publicly accessible Internet computer that supports anonymous file transfer protocol (FTP) or similar services, unless the Executive Management or the Chief Executive Officer (CEO) has first approved the posting of these materials.

In more general terms, City of Vincent internal information should not be placed in any location, on machines connected to the City's internal networks, or on the Internet, unless the persons who have access to that location have a legitimate need-to-know.

All publicly writable (Common/Public) directories on the City's Internet-connected computers will be reviewed and cleared periodically. This process is necessary to prevent the anonymous exchange of information inconsistent with the City's business.

Examples include pirated software, purloined passwords, stolen credit card numbers, and inappropriate written or graphic material (i.e., erotica). Users are prohibited from being involved in any way with the exchange of the material described.

3.3 Information Protection

Wiretapping and message interception is straightforward and frequently encountered on the Internet. Accordingly, City of Vincent secret, proprietary, or private information must not be sent over the Internet unless it has first been encrypted by approved methods.

Credit card numbers, log in passwords, and other parameters that can be used to gain access to goods or services must not be sent over the Internet in readable form. Secure Link, or another encryption method approved by the City's ITS, must be used to protect these parameters as they traverse the Internet.

In keeping with the confidentiality agreements signed by all employees, the City's software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-City of Vincent party for any purposes other than business purposes expressly authorised by Executive Management or the CEO.

Exchanges of software and/or data between the City and any third party may not proceed unless a written agreement has first been signed. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected. The written agreement must be signed by an Executive Manager and/or the CEO.

Regular business practices, such as shipment of software in response to a customer purchase order, need not involve such a specific agreement since the terms are implied.

The City strongly supports strict adherence to software vendors' license agreements. When at work, or when the City's computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden.

Likewise, off-hours participation in pirate software bulletin boards and similar activities represent a conflict of interest with City of Vincent work, and are therefore prohibited. Similarly, reproduction of words posted or otherwise available over the Internet must be done only with the permission of the author/owner.

3.4 Expectation of Privacy

Employees using the City's information systems and/or the Internet should realise that their communications are not automatically protected from viewing by third parties. Unless encryption is used, employees should not send information over the Internet if they consider it to be private.

At any time and without prior notice, the City's management reserves the right to examine e-mail, personal file directories, and other information stored on the City's computers. This examination assures compliance with internal policies, supports the performance of internal investigations, and assists with the management of the City's information systems.

3.5 Resource Usage

The City's management encourages employees to explore the Internet, but if this exploration is for personal purposes, such as games, news groups, and other non-business activities, it should be done on personal, not company, time.

Use of the City's computing resources for these personal purposes is permissible so long as the incremental cost of the usage is negligible, and so long as no business activity is pre-empted by the personal use. Extended use of these resources requires prior written approval by the Director of the service area.

3.6 Public Representations

Employees may indicate their affiliation with the City in bulletin board discussions, chat sessions, and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for instance via an e-mail address.

In both case, whenever employees provide an affiliation, they must also clearly indicate that the opinions expressed are their own, and not necessarily those of the City.

All external representations on behalf of the City must first be cleared with Directors or the CEO. Additionally, to avoid libel problems, whenever any affiliation with the City is included with an Internet message or posting, written attacks are strictly prohibited.

Employees must not publicly disclose any internal information via the Internet that may adversely affect the City's customer relations or public image unless the approval of the Executive Management or the CEO has first been obtained. Responses to specific customer e-mail messages are exempted from this policy.

Care must be taken to properly structure comments and questions posted to mailing lists, public news groups, and related public postings on the Internet. If a user is working on a project, or related confidential matters, all related postings must be cleared with their Director and the CEO prior to being placed for public display on the Internet.

3.7 Access Control

Unless the prior approval of the MIT has been obtained, employees may not establish Internet or other external network connections that could allow non-City of Vincent users to gain access to the City's systems and information. These connections include the establishment of multi-computer file systems, Internet home pages, FTP servers, and the like.

Likewise, unless the MIT, Directors, and CEO have approved the practice in advance, users are prohibited from using new or existing Internet connections to establish new business channels. These channels include electronic data interchange (EDI) arrangements, electronic malls with online shopping, online database services, etc.

The CEO will determine appropriate use and may deny, revoke, suspend or close any user access at any time.

3.8 Reporting Security Problems

If sensitive City of Vincent information is lost, disclosed to unauthorised parties, or suspected of being lost or disclosed to unauthorised parties, Employees must immediately notify their Manager and MIT. In case of managers, notify your Director.

If any unauthorised use of the City's information systems has taken place, or is suspected of taking place, the MIT must be notified immediately. Similarly, whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, the MIT must be notified immediately.

All unusual systems behaviour, such as missing files, frequent system crashes, misrouted messages, and the like must also be immediately reported via the Helpdesk system because it may indicate a computer virus infection or similar security problem. The specifics of security problems should not be discussed widely but should instead be shared on a need-to-know basis.

Users must not probe security mechanisms at either the City's or other Internet sites unless they have first obtained permission from the MIT. If users probe security mechanisms, alarms will be triggered and resources will needlessly be spent tracking the activity.

3.9 Responsibilities

As defined below, Employees responsible for Internet security have been designated in order to establish a clear line of authority and responsibility:

(a) ITS must establish Internet security policies and standards and provide technical guidance on PC security to all Employees.

(b) ITS employees must monitor compliance with Internet security requirements, including hardware, software, and data safeguards. Managers must ensure that their employees are in compliance with the Internet security policy established in this document. ITS employees must also provide administrative support and technical guidance to management on matters related to Internet security.

(c) ITS employees must periodically conduct a risk assessment of each production information system to determine both risks and vulnerabilities.

(d) ITS employees must check that appropriate security measures are implemented on these systems in a manner consistent with the level of information sensitivity.

(e) ITS employees must check that user access controls are defined on these systems in a manner consistent with the need-to-know.

(f) City of Vincent information owners must see to it that the sensitivity of data is defined and designated on these systems in a manner consistent with in-house sensitivity classifications.

(g) Managers must ensure that:

(i) Employees under their supervision implement security measures as defined in this document.

(ii) Employees under their supervision delete sensitive (confidential) data from their disk files when the data is no longer needed or useful.

(iii) Employees under their supervision who are authorised to use personal computers are aware of and comply with the policies and procedures outlined in all documents that address information security.

(iv) Employees and contractors under their supervision complete the pre-exit clearance process upon their official termination of employment or contractual agreement.

(v) Employees and contractors under their supervision make backup copies of sensitive, critical, and valuable data files as often as is deemed reasonable.

(h) Users of the City's Internet connections must:

(i) Know and apply the appropriate City of Vincent policies and practices pertaining to Internet security.

(ii) Not permit any unauthorised individual to obtain access to the City's Internet connections.

(iii) Not use or permit the use of any unauthorised device in connection with the City's personal computers.

(iv) Not use the City's Internet resources (software/hardware or data) for other than authorised organisation purposes.

(v) Maintain exclusive control over and use of his/her password, and protect it from inadvertent disclosure to others.

(vi) Select a password that bears no obvious relation to the user, the user's organisational group, or the user's work project, and that is not easy to guess.

(vii) Ensure that data under his/her control and/or direction is properly safeguarded according to its level of sensitivity.

(viii) Report to the MIT or ITS employees any incident that appears to compromise the security of the City's information resources. These include missing data, virus infestations, and unexplained transactions.

(ix) Access only the data and automated functions for which he/she is authorised in the course of normal business activity.

(x) Obtain supervisor authorisation for any uploading or downloading of information to or from the City's multi-user information systems if this activity is outside the scope of normal business activities.

(xi) Make backups of all sensitive, critical, and valuable data files as often as is deemed reasonable by their Manager.

3.10 No Warranties

The City is not responsible for any damages a user suffers as a consequence of an Internet session. Use of any information obtained via the Internet is at the user's own risk. All users need to consider the source of any information they obtain, and consider how valid that information may be.

The City is also not responsible for the content of any online service, its accuracy, authoritativeness, timeliness or usefulness and shall not accept responsibility for any damages arising from the use of its connection to online services. Similarly, the City cannot be held responsible for breaks in service due to technical problems outside of its control. The nature of the Internet means that some or all services will sometimes not be available without prior notice.

3.11 Encounter of Controversial Material

Users may encounter material which is controversial and which they may consider inappropriate or offensive. It is the user's responsibility not to initiate access to such material. If the user has a concern regarding this, they should contact ITS employees.

3.12 Non Business Related Use of the Internet

Limited use of the Internet facility for private purposes will be permitted but only in personal time. The City pays for Internet access on a usage basis. If access costs escalate due to excessive private use then this privilege will be withdrawn.

Personal use of the Internet is subject to the Unacceptable Use conditions detailed in this policy.

Personal Time use is defined as follows:

- Prior to 8am;
- Between 12:30pm and 1:30pm; and
- After 6pm.

Website filtering software is in use at the City. Access to certain websites during business hours is restricted. Websites found to be malicious in nature are blocked indefinitely. If you come across a website which you believe should not be blocked please put the details in an e-mail and send it to helpdesk.

Personal use of the City's ICT facilities must not interfere with business operations and, accordingly the CEO may choose to set limits on acceptable personal use. This stipulation applies equally to all of the City's ICT facilities.

Information entered on any office computer, or recorded on any hardware storage space, becomes the property of the City. This includes information of a personal kind. The City reserves the right to access any part of its ICT facilities, for any purpose, even if a person has recorded personal information on it and may choose to copy or delete personal messages. It also reserves the right to disclose personal messages for the purpose of addressing suspected violations of this policy or any legislative requirements.

3.13 Examples of Unethical and Unacceptable Use

Use of the Internet for unethical or unacceptable purposes/activities is not permitted. This includes, but is not limited to, any of the following activities:

- Violating federal or state laws, in particular Division 6 of the Censorship Act 1996.
- Violating organisational, institutional or third party copyright, licence agreements or other contracts.
- Seeking to gain or gaining unauthorised access to the resources of the Internet.
- Seeking to use or using services that incur a cost in addition to the connection fees and costs.
- Using, or knowingly allowing another use, any computer, computer network, computer system, program or software to devise or execute artifice or scheme to defraud or to obtain money, property, services or other things of value by false pretences, promises or representations.
- Without authorisation, destroying, altering, dismantling, disfiguring, preventing rightful access to, or otherwise interfering with the integrity of computer-based information and/or information resources.
- Without authorisation, invading the privacy of individuals or entities that are creators, authors, users, or subjects of the information resource.
- Disrupting the intended use of the Internet.
- Vandalising the data of another user, the Internet, or any agencies of other networks connected to the Internet. This includes, but is not limited to the creation of computer viruses.

- Unduly interfering with the work of other users of the Internet, or with their host systems, that would seriously disrupt the network or result in the loss of a user's work or system.

- Transmitting, or causing to be transmitted, any communications that may be construed as harassment or disparagement of others based on the criteria of anti-discrimination legislation and the City's policy.

- Compromising the privacy of users and/or the City's network.

- Seeking to create a false identity or forged e-mail address or header, or otherwise attempting to mislead others as to the identity of the sender or the origin of a message sent via Internet.

- Using ones account (or the facilities and capabilities of the Internet) to conduct any business or activity for commercial purposes or financial gain, including publishing material which contains any advertising or any solicitation of other network users or discussion group of list members to use goods or services.

- Publishing on or over the Internet any information, which violates or infringes upon the rights of any other person or any information of an abusive, profane nature or material likely to be sexually offensive to an average person.

- Accessing, distributing or storing of unlawful, harassing, libellous, abusive, threatening, harmful, vulgar, obscene, malicious, restricted or otherwise objectionable material of any kind or nature.

- Using one's account for obtaining illegally distributed copies of software.

- Using one's account for political lobbying.

- Using one's account to harass or defame another person.

- Seeking or gaining unauthorised access to any resource or entity.

- Seeking to use the Internet for any criminal or illegal activities (defined as a violation of State, Commonwealth or International Law).

- Seeks to engage in Obscene Activities as defined in the 1995 Censorship Bill.

- Wastefully using finite resources or obstructing other people's work by consuming gratuitously large amount of system resources (disk space, CPU time, bandwidth). The sending of chain letters or broadcasts messages or individuals and any other types of use that would cause congestion of the networks or otherwise interfere with the work of others is expressly forbidden. Unbridled and open-ended use of the Internet in terms of access cannot be accommodated.

- Propagation of any form of malicious software (viruses, worms, Trojan horses, applets etc).
- Transmission of any material that may infringe the intellectual property rights or other rights of third parties, including trademark, copyright or right of publicity.
- Seeking to participate in network games or other such frivolous activity.
- Participating in illegal online file sharing activities.

3.14 Examples of Unacceptable Material

Improper use includes the entry, storage and transmission of unacceptable material.

Unacceptable material includes but is not limited to:

- Material that breaches the requirements of anti-discrimination legislation such as the Racial Discrimination Act 1975, the Sex Discrimination Act 1984 and the Disability Discrimination Act 1992.
- Unauthorised written or pictorial material, including material a reasonable person would consider objectionable, offensive, harassing, obscene or restricted.
- Files larger than 3 MB for email and attachments.
- Chain mail.
- Unauthorised executable files.
- Any material that violates copyright legislation.

Restricted material means articles dealing with matters of sex, drug misuse, crime, cruelty, violence or abhorrent phenomena, which would be unsuitable for a minor to see, hear or read.

Objectionable material includes: Any media classified RC or refused publication; child pornography; articles promoting crimes and/or violence; and articles that describe or depict coercion to submit to sexual conduct, acts of necrophilia, torture, bestiality, or the use of excrement in a sexual act.

4.1 Purchasing

All purchasing of the organisation’s ICT hardware devices shall be centralised with Information Technology Services (ITS) to ensure that all equipment conforms to corporate hardware standards. All requests for corporate ICT hardware devices must be submitted to the manager for that service area for approval. The request must then be sent to ITS, which will then determine standard hardware that best accommodates the desired request.

4.2 Hardware Standards

The following list shows the standard hardware distribution for the City's ICT (excluding test computers) that are fully supported by ITS:

- Desktops - will be provided to employees who work primarily from the office.
- Laptops - will only be provided to employees on availability and "sign out" basis.
- Monitors - will be provided for both desktop and laptop systems. 15 inch through to 21 inch monitor, depending on job requirements
- Printers - Employees will be given access to a network laser printer and a multi-function copier for printing purposes.
- Telephones
- Two – way radios

Employees needing ICT hardware other than what is stated above must request such hardware from ITS. Each request will be considered on a case-by-case basis.

4.3 Outside Equipment

No outside equipment may be connected into the City's network without the permission of the Manager Information Systems (MIT). No personal hardware or software is allowed. This policy is enforced to reduce problems with equipment, software failure, damage to data files, and the introduction of viruses.

To restrict access to the City's data and/or programs and prevent virus transmission, personal disks not belonging to the City are not to be used on the City's computers, unless otherwise stated.

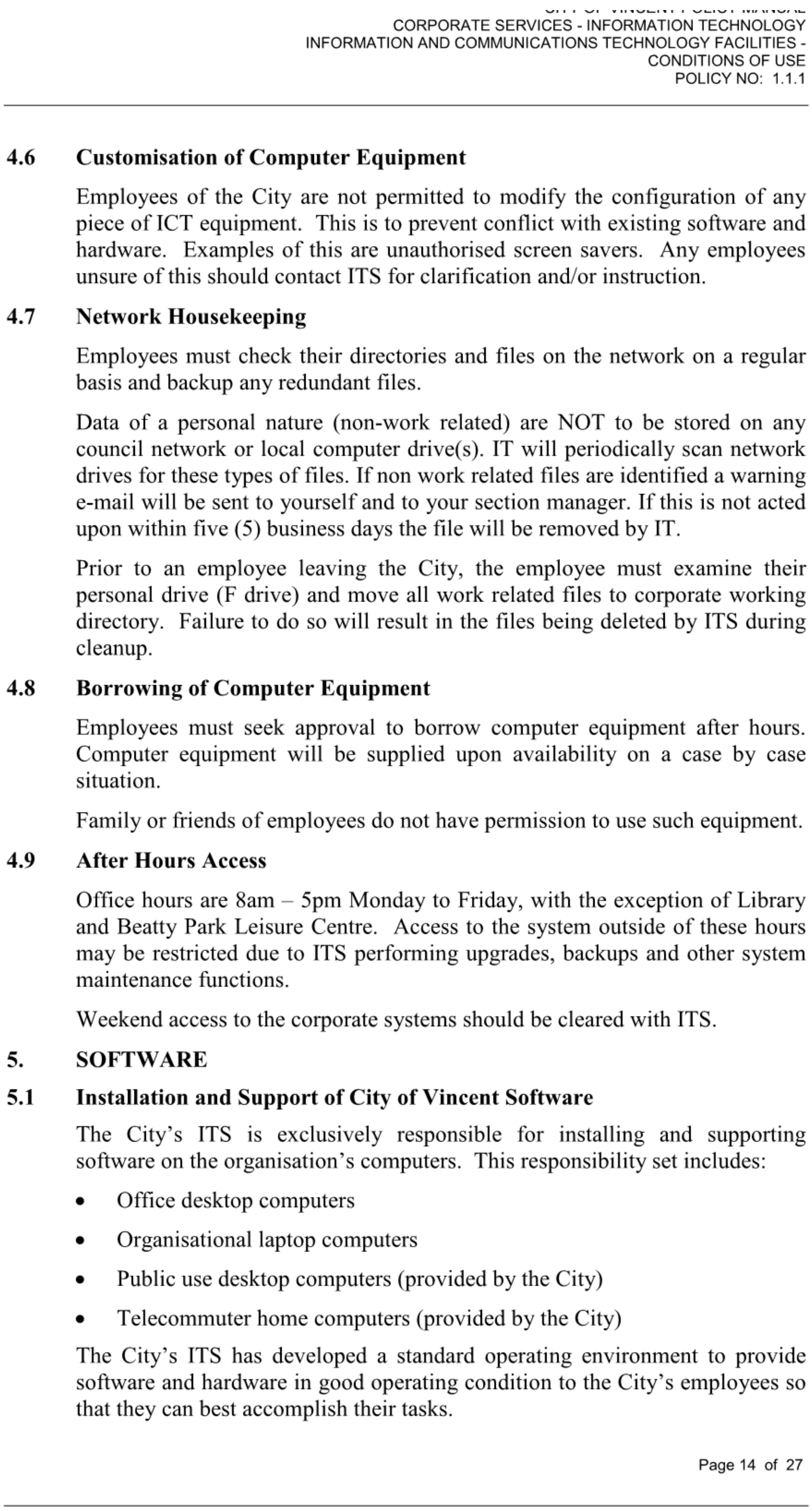
4.4 Relocation of ICT Equipment

ICT equipment must not be relocated without prior knowledge and consent of ITS employees.

4.5 Proper Handling of ICT Equipment

Standard measures are required to maintain cleanliness and ensure the safety with ICT equipment.

- One should avoid eating and drinking over all ICT equipment.
- All care must be taken when using ICT equipment.



4.6 Customisation of Computer Equipment

Employees of the City are not permitted to modify the configuration of any piece of ICT equipment. This is to prevent conflict with existing software and hardware. Examples of this are unauthorised screen savers. Any employees unsure of this should contact ITS for clarification and/or instruction.

4.7 Network Housekeeping

Employees must check their directories and files on the network on a regular basis and backup any redundant files.

Data of a personal nature (non-work related) are NOT to be stored on any council network or local computer drive(s). IT will periodically scan network drives for these types of files. If non work related files are identified a warning e-mail will be sent to yourself and to your section manager. If this is not acted upon within five (5) business days the file will be removed by IT.

Prior to an employee leaving the City, the employee must examine their personal drive (F drive) and move all work related files to corporate working directory. Failure to do so will result in the files being deleted by ITS during cleanup.

4.8 Borrowing of Computer Equipment

Employees must seek approval to borrow computer equipment after hours. Computer equipment will be supplied upon availability on a case by case situation.

Family or friends of employees do not have permission to use such equipment.

4.9 After Hours Access

Office hours are 8am – 5pm Monday to Friday, with the exception of Library and Beatty Park Leisure Centre. Access to the system outside of these hours may be restricted due to ITS performing upgrades, backups and other system maintenance functions.

Weekend access to the corporate systems should be cleared with ITS.

5. SOFTWARE

5.1 Installation and Support of City of Vincent Software

The City's ITS is exclusively responsible for installing and supporting software on the organisation's computers. This responsibility set includes:

- Office desktop computers
- Organisational laptop computers
- Public use desktop computers (provided by the City)
- Telecommuter home computers (provided by the City)

The City's ITS has developed a standard operating environment to provide software and hardware in good operating condition to the City's employees so that they can best accomplish their tasks.

5.2 Current Software

The City's ITS, in coordination with all other service areas, has decided upon the following software standards:

<u>Operating System</u>

- Microsoft Windows XP SP2

<u>Productivity Applications</u>

- Microsoft Office 2003
    - Word
    - Excel
    - PowerPoint
    - Access
    - Outlook
- MapInfo
- Authority
- DocManager

<u>Accessories</u>

- Microsoft Internet Explorer
- Adobe Acrobat Reader
- Trend OfficeScan Corporate Edition

5.3 The current software can exist in any one of the following scenarios:

(a) From the ITS created SOE (Standard Operating Environment) which is applied to all council desktop computers

(b) The City's ITS installation procedure that provides for the following:

- Installation options
- Upgrade considerations (if applicable)
- Data conversion (if applicable)

(c) A shortcut to a network application (not truly an installation)

(d) An automated installation through an information technology services developed solution that may be used in a rapid-deployment scenario or silent-install situation

(e) A terminal application, Citrix application, or other thin-client type of application accessible via the City's intranet page or desktop link.

5.4 Software cannot be present on City of Vincent computers in the following scenarios:

(a) An installation of a software not carried out by ITS employees.

(b) Software purchased for one's own computer.

(c) A pirated copy of any title.

(d) Any other title than what is on the current software list of this policy.

(e) Any means not covered by the ways that software can exist on City of Vincent computers.

5.5 Software Licensing

Majority of the software titles on the City's current software list are not freeware; therefore, the cost of software is a consideration for most titles and their deployment.

It is the aim of ITS to ensure licensing is kept accurate and maintained. To address this, the ITS service area is responsible for purchasing software licenses for the following software categories:

- Desktop operating system
- Productivity Applications
- Internet software
- Accessories

Other software categories (workgroup-specific titles) are the purchasing responsibility of the workgroup in which they serve. However, the application(s) are still installed and supported to an extent by ITS.

To control costs, licensing costs are a factor in the decision-making processes that go into client software planning and request approval.

5.6 Software Requests

If a user would like additional software, a request to his or hers manager should be put in writing.

This formal request should be then forwarded onto the Manager of Information Technology for action.

6. ANTIVIRUS

6.1 Background

A virus is a program designed to replicate itself without permission. In addition, some make great efforts to avoid detection, damage programs and/or data and transfer information and/or funds out of the company to third parties. Viruses usually try to avoid detection by disguising themselves as a legitimate program or attaching themselves to a trusted program like E-mail messages. Viruses are not only "executable" programs, but may also be contained in the "macros" used by programs such as document macros in word processors, spread sheets etc.

There are four main types of Virus:

- Hoax

  Hoax viruses, which may best be described as another form of "Spam", are of more nuisance value than anything else but again can be time consuming.

- Non Malicious

  Non-malicious viruses do not cause any actual damage and have more nuisance value than anything else, nevertheless they too can be very time consuming and therefore expensive to eradicate from a system.

- Malicious

  Malicious viruses will damage systems in some way, whether it is erasing hard disks, tampering with Word document templates, or some other destructive process.

- Security Breaching

  Security breach viruses may transfer internal files and information out of your company to a third party without your permission.

6.2 Risk Analysis

After assessing the City's of Vincent ICT infrastructure, ITS have recognised following areas of virus threat:

- File and Print Servers
- Desktops - including laptops
- Internet - Web browsing
- Email
- External storage media – Floppy disk, CD-ROM, ZIP disk.

6.3 Protection – Anti Virus Tools

As the threat posed by malicious virus continually increases, ITS are constantly exploring new methods to enhance the protection afforded to users by existing systems.

6.4 Virus Outbreak Procedure

The following is a guideline to follow when dealing with a virus outbreak:

***Note:* These actions should be carried out by an ITS employees.**

- Locate the virus in the environment and find out what the virus is called.
- Ascertain the threat.
- Get information on the virus from http://www.antivirus.com
- Take appropriate actions to control the outbreak.

- Estimate the scale of infection, allocate the required resources, and clean the virus.
- Validate data integrity.
- Contact any other business (units).

The steps above will help you deal with any virus outbreak. Most important is to understand the infection mechanism of the virus and any possible payload. This will allow you to take appropriate actions when dealing with the virus.

An up to date list of the current virus can be found from "http://www.antivirus.com". This site also includes a mailing list, which can be joined to find out about new viruses as they are discovered.

7. EMAIL/FAX

7.1 City of Vincent Property

As a productivity enhancement tool, the City encourages the business use of electronic communications (voice mail, e-mail, and fax). Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of the City, and are not the property of users of the electronic communications services.

7.2 Authorised Usage

The City's electronic communications systems generally must be used only for business activities. Incidental personal use is permissible so long as it does not:

- consume more than a trivial amount of resources;
- interfere with employee's productivity; or
- generate any business activity.

Users are restricted from using the City's electronic communications systems for charitable endeavours, private business activities, or amusement/entertainment purposes unless expressly approved by the CEO or Directors. Employees are reminded that the use of corporate resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.

7.3 Default Privileges

Employee privileges on electronic communications systems must be assigned so that only those capabilities necessary to perform a job are granted. This approach is widely known as the concept of "need-to-know." For example, end users must not be able to reprogram electronic mail system software.

7.4 User Separation

These facilities must be implemented where electronic communications systems provide the ability to separate the activities of different users. For example, electronic mail systems must employ user-IDs and associated passwords to isolate the communications of different users. Fax machines that do not have separate mailboxes for different recipients need not support such user separation. All Employees and authorised contractors must have unique usernames and passwords to access the e-mail system.

7.5 Network Etiquette

All users of electronic data exchange facilities are expected to abide by the generally accepted rules of etiquette. These include, but are not limited to, the following:

- Compliance with the City's standards and regulations for employee conduct.
- Not engaging in activities, which are prohibited under State or Commonwealth Law.
- Nor using the network in such a way that disrupts the use of the network for other users.

  This applies specifically to vandalism and harassment

7.6 User Accountability

Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorised user. To do so exposes the authorised user to claim responsibility for actions the other party takes with the password.

If users need to share computer resident data, they should utilise message-forwarding facilities, public directories on local area network servers, and other authorised information-sharing mechanisms. To prevent unauthorised parties from obtaining access to electronic communications, users must choose passwords that are difficult to guess (not a dictionary word, not a personal detail, and not a reflection of work activities).

7.7 No Default Protection

Employees are reminded that the City's electronic communications systems are not encrypted by default. If sensitive information must be sent by electronic communications systems, encryption or similar technologies to protect the data must be employed. See ITS employees if this requirement is needed.

7.8 Respecting Privacy Rights

Except as otherwise specifically provided, employees may not intercept or disclose, or assist in intercepting or disclosing, electronic communications.

The City is committed to respecting the rights of its employees, including their reasonable expectation of privacy.

However, the City is also responsible for the servicing and protection of its electronic communications networks. To accomplish this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing electronic communications.

7.9 No Guaranteed Message Privacy

The City cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, others can access electronic communications in accordance with this policy.

7.10 Regular Message Monitoring

It is the policy of the City NOT to regularly monitor the content of electronic communications. However, the content of electronic communications may be monitored and the usage of electronic communications systems will be monitored to support operational, maintenance, auditing, security, and investigative activities. Users should structure their electronic communications in recognition of the fact that the City will filter and block emails and internet access in line with this document.

7.11 Statistical Data

Consistent with generally accepted business practice, the City collects statistical data about electronic communications. As an example, call-detail-reporting information collected by telephone service providers indicates the numbers dialled, the duration of calls, the time of day when calls are placed, etc. Using such information, ITS employees monitors the use of electronic communications to ensure the ongoing availability and reliability of these systems.

7.12 Incidental Disclosure

It may be necessary for ITS employees to review the content of an individual employee's communications during the course of problem resolution. IT employees may not review the content of an individual employee's communications out of personal curiosity or at the insistence of individuals who have not gone through the proper approval channels (i.e. Manager, Director, CEO etc).

7.13 Message Forwarding

Recognising that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. Sensitive information must not be forwarded to any party outside the City without the prior approval of a Manager, Director or the CEO. Blanket forwarding of messages to parties outside the City is prohibited unless the prior permission of the CEO has been obtained.

7.14 Deleting Electronic Messages

Users are required to delete their personal electronic message no longer needed for business purposes from storage media. Not only will this increase scarce storage space; it will also simplify record management and related activities. If the City is involved in a litigation action, all electronic messages pertaining to that litigation will not be deleted until the CEO or his/her designated representative has communicated that it is legal to do so.

To avoid excessive load on the mail server, users must: perform regular clean-ups of their E-mail and FAX messages:

- E-mail in **Sent Items** and **Inbox** folders.
- E-mail in **Trash folder** at every re-start of the PC (default)

7.15 Responsibilities

As defined below, Employees responsible for electronic mail security have been designated in order to establish a clear line of authority and responsibility:

- ITS must establish e-mail security policies and standards and provide technical guidance on e-mail security to all City of Vincent employees.
- ITS must monitor compliance with personal computer security requirements, including hardware, software, and data safeguards. Managers must ensure that their Employees are in compliance with the personal computer security policy established in this document. ITS must also provide administrative support and technical guidance to management on matters related to e-mail security.
- Managers must ensure that Employees under their supervision implement e-mail security measures as defined in this document.

7.16 Email Etiquette

It is expected that the users of the City's email facility adhere to the email etiquette outlined below:

(1) Be concise and to the point

Do not make an e-mail longer than it needs to be. Remember that reading an e-mail is harder than reading printed communications and a long e-mail can be very discouraging to read.

(2) Answer all questions, and pre-empt further questions

An email reply must answer all questions, and pre-empt further questions – If you do not answer all the questions in the original email, you will receive further e-mails regarding the unanswered questions, which will not only waste your time and your customer's time but also cause considerable frustration. Moreover, if you are able to pre-empt relevant questions, your customer will be grateful and impressed with your efficient and thoughtful customer service.

(3) Use proper spelling, grammar & punctuation

This is not only important because improper spelling, grammar and punctuation give a bad impression of your company, it is also important for conveying the message properly. E-mails with no full stops or commas are difficult to read and can sometimes even change the meaning of the text. And, if your program has a spell checking option, why not use it?

(4) Make it personal

Not only should the e-mail be personally addressed, it should also include personal i.e. customized content. For this reason auto replies are usually not very effective. However, templates can be used effectively in this way, see next tip.

(5) Use templates for frequently used responses

Some questions you get over and over again, such as directions to your office or how to subscribe to your newsletter. Save these texts as response templates and paste these into your message when you need them. You can save your templates in a Word document, or use pre-formatted emails.

(6) Answer swiftly

Customers send an e-mail because they wish to receive a quick response. If they did not want a quick response they would send a letter or a fax. Therefore, each e-mail should be replied to within at least 24 hours, and preferably within the same working day. If the email is complicated, just send an email back saying that you have received it and that you will get back to them. This will put the customer's mind at rest and usually customers will then be very patient!

(7) Do not attach unnecessary files

By sending large attachments you can annoy customers and even bring down their e-mail system. Wherever possible try to compress attachments and only send attachments when they are productive. Moreover, you need to have a good virus scanner in place since your customers will not be very happy if you send them documents full of viruses!

(8) Use proper structure & layout

Since reading from a screen is more difficult than reading from paper, the structure and lay out is very important for e-mail messages. Use short paragraphs and blank lines between each paragraph. When making points, number them or mark each point as separate to keep the overview.

(9) Do not overuse the high priority option

We all know the story of the boy who cried wolf. If you overuse the high priority option, it will lose its function when you really need it. Moreover, even if a mail has high priority, your message will come across as slightly aggressive if you flag it as 'high priority'.

(10) Do not write in CAPITALS

IF YOU WRITE IN CAPITALS IT SEEMS AS IF YOU ARE SHOUTING. This can be highly annoying and might trigger an unwanted response in the form of a flame mail. Therefore, try not to send any email text in capitals.

(11) Don't leave out the message thread

When you reply to an email you should include the original email in your reply, in other words click “Reply” instead of “New Message”.

(12) Add disclaimers to your emails

It is important to add disclaimers to your internal and external emails, since this can help protect the organisation from liability. City of Vincent automatically inserts a standard disclaimer on all external emails.

(13) Read the email before you send it

A lot of people don't bother to read an email before they send it out, as can be seen from the many spelling and grammar mistakes contained in emails. Apart from this, reading your email through the eyes of the recipient will help you send a more effective message and avoid misunderstandings and inappropriate comments.

(14) Do not overuse Reply to All

Only use Reply to All if you really need your message to be seen by each person who received the original message.

(15) Mailings > use the Bcc: field or do a mail merge

When sending an email mailing, some people place all the email addresses in the To: field. There are two drawbacks to this practice: (1) the recipient knows that you have sent the same message to a large number of recipients, and (2) you are publicising someone else's email address without their permission. One way to get round this is to place all addresses in the Bcc: field. However, the recipient will only see the address from the To: field in their email, so if this was empty, the To: field will be blank and this might look like spamming. You could include the mailing list email address in the To: field, or even better, if you have Microsoft Outlook and Word you can do a mail merge and create one message for each recipient. A mail merge also allows you to use fields in the message so that you can for instance address each recipient personally. For more information on how to do a Word mail merge, consult the Help in Word.

(16) Take care with abbreviations and emoticons

In business emails, try not to use abbreviations such as BTW (by the way) and LOL (laugh out loud). The recipient might not be aware of the meanings of the abbreviations and in business emails these are generally not appropriate. The same goes for emoticons, such as the smiley :-). If you are not sure whether your recipient knows what it means, it is better not to use it.

(17) Be careful with formatting

Remember that when you use formatting in your emails, the sender might not be able to view formatting, or might see different fonts than you had intended. When using colours, use a colour that is easy to read on the background.

(18) Take care with rich text and HTML messages

Be aware that when you send an email in rich text or HTML format, the sender might only be able to receive plain text emails. If this is the case, the recipient will receive your message as a .txt attachment. Most email clients however, including Microsoft Outlook, are able to receive HTML and rich text messages.

(19) Do not request delivery and read receipts

This will almost always annoy your recipient before he or she has even read your message. Besides, it usually does not work anyway since the recipient could have blocked that function, or his/her software might not support it, so what is the use of using it? If you want to know whether an email was received it is better to ask the recipient to let you know if it was received.

(20) Do not ask to recall a message

Biggest chances are that your message has already been delivered and read. A recall request would look very silly in that case wouldn't it? It is better just to send an email to say that you have made a mistake. This will look much more honest than trying to recall a message.

(21) Do not copy a message or attachment without permission

Do not copy a message or attachment belonging to another user without permission of the originator. If you do not ask permission first, you might be infringing on copyright laws.

(22) Do not use email to discuss confidential information

Sending an email is like sending a postcard. If you don't want your email to be displayed on a bulletin board, don't send it. Moreover, never make any libellous, sexist or racially discriminating comments in emails, even if they are meant to be a joke.

(23) Use a meaningful subject

Try to use a subject that is meaningful to the recipient as well as yourself. For instance, when you send an email to a company requesting information about a product, it is better to mention the actual name of the product, e.g. 'Product A information' than to just say 'product information' or the company's name in the subject.

(24) Use active instead of passive

Try to use the active voice of a verb wherever possible. For instance, 'We will process your order today', sounds better than 'Your order will be processed today'. The first sounds more personal, whereas the latter, especially when used frequently, sounds unnecessarily formal.

(25) Avoid using URGENT and IMPORTANT

Even more so than the high-priority option, you must at all times try to avoid these types of words in an email or subject line. Only use this if it is a really, really urgent or important message.

(26) Avoid long sentences

Try to keep your sentences to a maximum of 15-20 words. Email is meant to be a quick medium and requires a different kind of writing than letters. Also take care not to send emails that are too long. If a person receives an email that looks like a dissertation, chances are that they will not even attempt to read it!

(27) Don't send emails containing libellous, defamatory, offensive, racist, obscene remarks

By sending or even just forwarding one libellous, or offensive remark in an email, you and your company can face court cases resulting in multi-million dollar penalties.

(28) Don't forward virus hoaxes and chain letters

If you receive an email message warning you of a new unstoppable virus that will immediately delete everything from your computer, this is most probably a hoax. By forwarding hoaxes you use valuable bandwidth and sometimes virus hoaxes contain viruses themselves, by attaching a so-called file that will stop the dangerous virus. The same goes for chain letters that promise incredible riches or ask your help for a charitable cause. Even if the content seems to be bona fide, the senders are usually not. Since it is impossible to find out whether a chain letter is real or not, the best place for it is the recycle bin.

(29) Keep your language gender neutral

In this day and age, avoid using sexist language such as: 'The user should add a signature by configuring his email program'. Apart from using he/she, you can also use the neutral gender: "The user should add a signature by configuring the email program'.

(30) Don't reply to spam

By replying to spam or by unsubscribing, you are confirming that your email address is 'live'. Confirming this will only generate even more spam. Therefore, just hit the delete button or use email software to remove spam automatically.

(31) Use cc: field sparingly

Try not to use the cc: field unless the recipient in the cc: field knows why they are receiving a copy of the message. Using the cc: field can be confusing since the recipients might not know who is supposed to act on the message. Also, when responding to a cc: message, should you include the other recipient in the cc: field as well? This will depend on the situation. In general, do not include the person in the cc: field unless you have a particular reason for wanting this person to see your response. Again, make sure that this person will know why they are receiving a copy.

8. CONDITIONS OF USE AGREEMENT

I, ………………………………………………………….………………… (block letters), have read and understood and agree to abide by the Conditions of Use for information technology and telecommunication facilities including Internet Usage, Electronic Mail and Fax. I agree to co-operate with reasonable security investigations. I acknowledge that I have been given and have read a copy of the Information Technology and Telecommunication usage policy. It is understood that I will not, or will not attempt to:

1. use the Council's Computing Infrastructure for any illegal or objectionable purposes (as defined by the WA Censorship Act);

2. attempt to breach the security of the computing system, including, but not limited to, altering software settings.

I understand that should violation of this agreement occur, disciplinary action may be taken and it will be deemed a breach by me of the terms of my employment. Breaching any of the Conditions of Internet Use, will result in permanent removal of online services access, a report to Chief Executive Officer, and where necessary, recommendation for disciplinary action including possible termination of employment, and/or prosecution by the City of Vincent or other appropriate authority.

Name (please print): ____

__________________________________ Date:_______________________
Signature