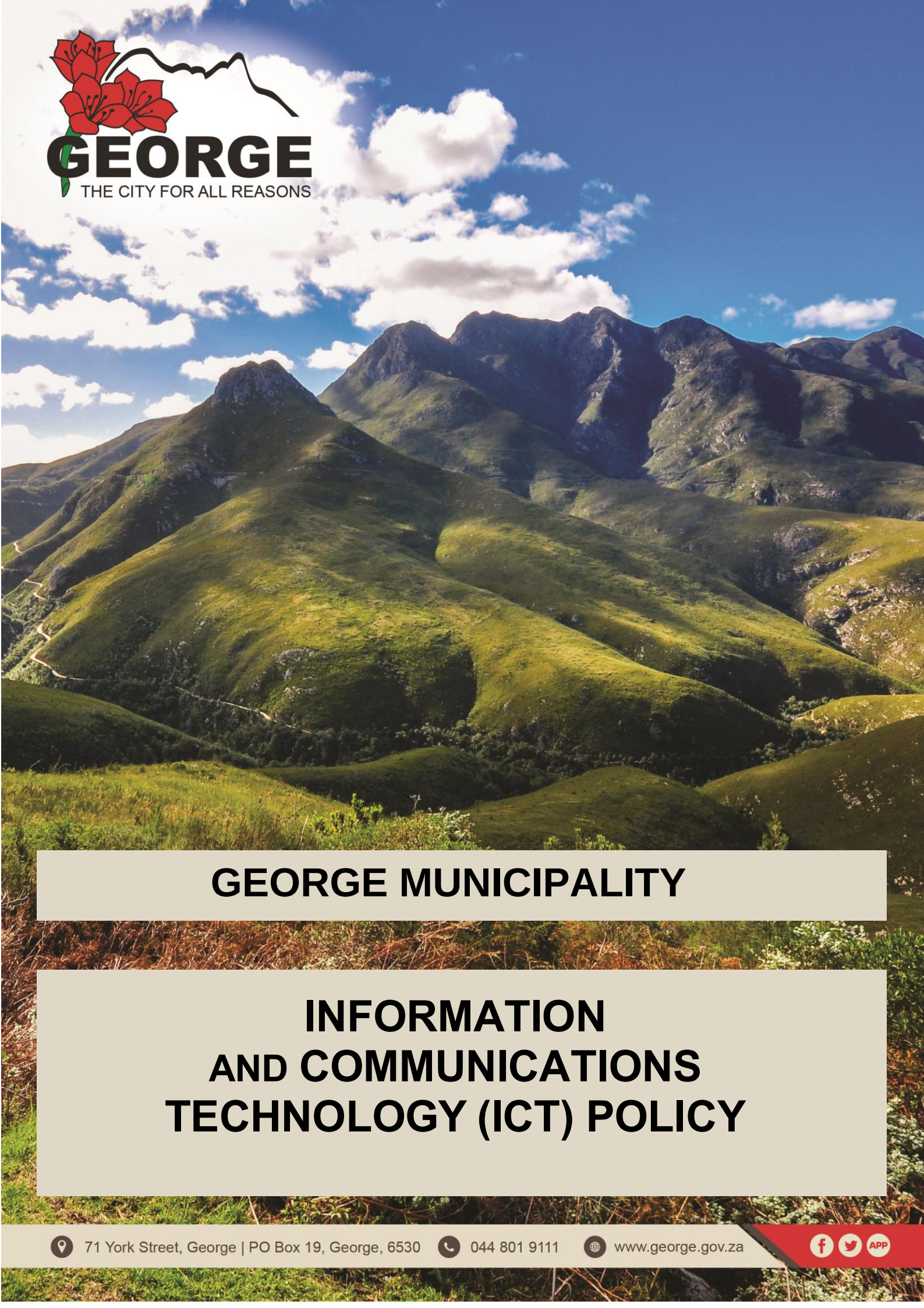

GEORGE MUNICIPALITY

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) POLICY

71 York Street, George | PO Box 19, George, 6530 044 801 9111 www.george.gov.za

Table of Contents

1 EXECUTIVE SUMMARY

Information and Communication systems and networks are an integral part of business at George Municipality. George Municipality has made a substantial investment in human and financial resources to create these systems.

The enclosed policies and directives have been established to:

a) Protect the ICT investment.
b) Safeguard the information contained within these systems.
c) Reduce business and legal risk.
d) Establish acceptable use and work ethics.
e) Set acceptable standards for the ICT infrastructure.
f) Protect the good name of the George Municipality.

In compiling this policy, procedures, international standards and benchmarks were followed.

2 ADMINISTRATION OF POLICY

The ICT Manager or delegated authority is responsible for maintaining the policy. The policy must be reviewed by the ICT Steering Committee on an annual basis and any changes approved by Council.

3 BREACH OF POLICY

Violations may result in disciplinary action.

Violations and/or failure to observe these guidelines may result in disciplinary action by the George Municipality in accordance with George Municipality's policy and Code of Conduct. The type of disciplinary action will depend upon the type and severity of the violation, whether it causes any liability or loss to the George Municipality, and/or the presence of any repeated violation(s).

4 TERMS AND DEFINITIONS

Policy: A stated course of action with a defined purpose and scope to guide decision-making under a given set of circumstances within the framework of corporate objectives, goals and management philosophies.

Form: A pre-formatted document containing instructions and placeholders for data entry to monitor progress through a Procedure and to ensure proper record-keeping.

Guideline: A collection of system specific or procedural specific "suggestions" for best

practice. They are not requirements to be met but are strongly recommended. Effective security policies make frequent references to standards and guidelines that exist within an organization

Personal computer (PC): A personal computer is a system designed to be used by one person at a time. This includes the tower/cabinet with different electronic hardware and a screen. Classifications within this category include a notebook and laptop.

Peripheral device: Any external device attached to a computer including but not limited to printers, disk drives, display monitors, keyboards, scanners or multimedia equipment.

Hardware: Any electronic device that is used to input, store, print or distribute municipal information for internal or external purposes. This includes, however, is not limited to, personal computers, local area network file servers and workstations, mainframe computers and terminals, printers, modems, scanners, backup units, portable hard drives and any other device that connects to a network or PC.

Software: Any program or operating system that allows the user of computer hardware to input, store, print or distribute municipal information for internal or external purposes. This includes, but is not limited to, personal computer operating systems, network operating systems, word processors, spreadsheets, databases, accounting systems, electronic mail, management utilities and user interfaces.

Networks: Computer systems linked together by department or location, for sharing data or applications that are stored centrally. This includes local area network workstations, wide area network workstations, minicomputer terminal, minicomputer emulated personal computers and other systems that may be connected, such as bulletin boards, intranet, internet and on-line information services.

Computer Services: Any advice, support, recommendation or contact with a computer system, regardless of form or physical characteristics, that has been purchased or otherwise obtained by the municipality. Computer services are performed by ICT or by approved outside consultants. Computer services include, but are not limited to, recommending, purchasing, configuring, installing and supporting computer systems. Support includes, but is not limited to, troubleshooting hardware and software problems, upgrading hardware or software and assisting in using application software. All computer services performed by the municipality are to be considered the property of the municipality.

His/Her: Refers also to her and she

Commercial e-mail: Means any electronic message that contains:

I. An advertisement for the sale of a product or service

II. A solicitation for the use of a toll-free number, the use of which connects the user to a person or service that advertises the sale of or sells a product or service, or
III. List of one or more websites that contain such an advertisement or solicitation.

Council computer system: All computer systems, including servers, personal computers, laptop computers, communication devices, operating systems, local area networks, wide area networks, software and other information technology created, equipment owned or licensed to the Council.

Council e-mail: The computer hardware and software supplied by the Council, including e-mail application software, routers and servers, for the sole purpose of transmitting electronic mail messages over an open or closed network.

Information System: This refers to the arrangement of people (users), data, processes, information presentation, and information technology that interacts to support day-to-day operations in an organisation as well as support the problem solving and decision-making needs of management and users.

Internet: The Internet is a worldwide global system of interconnected computer networks that allow users access to a vast array of information resources and services, and the infrastructure to support electronic mail. In addition, it supports popular services such as online chat, file transfer and file sharing, gaming, commerce, social networking, publishing, video on demand, teleconferencing and telecommunications.

Local Memory: Means the memory available on a personal computer, including without limitation the main hard disk, cache and random-access memory (RAM).

Prohibited Material: Means materials or statements which: -
* are prohibited by any legislation (national or otherwise); or
* may reasonably be construed as being, or have previously been determined by the Council in its discretion to be fraudulent, sexually explicit, profane, obscene, intimidating, defamatory, discriminatory, harassing, racially prejudicial (discrimination on the grounds of colour, gender, ethnic, race or social origin), religiously prejudicial, or constitute and infringement of a third parties' intellectual property rights.

Responsible Person: Means a person's immediate supervisor; the relevant departmental head or manager, the CIO or his/her alternate.

Server: Computers designed to support a computer network that allows users to share files, application software, and hardware.

Unauthorised Use: Means prohibited use of the Council's information system and e-mail system by anyone other than an authorised user.

User: Means any person employed by the Council on a permanent, temporary, consultancy basis, internship or any other person including councillors approved by the CIO or his/her alternate and who is authorised to access the Council's information system or e-mail system.

Username: The username assigned to a user by the Council.

Virus: Means any program code, programming instruction or set of instructions constructed with the specific purpose of damaging, interfering with or otherwise adversely affecting computer software, computer programs, data files or operations and includes, without limitation, all viruses, Trojans, worms, zombies and time bombs.

5 LEGISLATIVE FRAMEWORK

The policy was drafted bearing in mind the legislative conditions, as well as to leverage internationally recognised ICT standards.

The following legislation, among others, were considered in the drafting of this policy:

- Constitution of the Republic of South Africa Act, Act No. 108 of 1996.
- Copyright Act, Act No. 98 of 1978
- Electronic Communications and Transactions Act, Act No. 25 of 2002
- Minimum Information Security Standards, as approved by Cabinet in 1996
- Municipal Finance Management Act, Act No. 56 of 2003
- Municipal Structures Act, Act No. 117 of 1998
- Municipal Systems Act, Act No. 32, of 2000
- National Archives and Record Service of South Africa Act, Act No. 43 of 1996
- National Archives Regulations and Guidance
- Promotion of Access to Information Act, Act No. 2 of 2000
- Protection of Personal Information Act, Act No. 4 of 2013
- Regulation of Interception of Communications Act, Act No. 70 of 2002
- Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.

The following internationally recognised ICT standards were leveraged in the development of this policy:

- Western Cape Municipal Information and Communication Technology Governance Policy Framework, 2014

- Control Objectives for Information Technology (COBIT) 5, 2012
- ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls
- King Code of Governance Principles, 2009

6 GENERAL COMMENTS

a. The Council relies heavily on the Council's computer system to conduct its business.
b. Council makes it obligatory for each user to sign an acknowledgement, as set out in Appendix "A", that he has read and understands the Council's ICT policy and accepts the responsibilities which is placed on him as a user.
c. The terms and conditions described in this policy apply to all users of the Council's computer systems wherever they may be situated.
d. The Council's computer systems are an extremely important and valuable asset, and as such, mistreatment or abuse thereof by a user may, in the Council's discretion, render such user liable for disciplinary action in accordance with the Council's disciplinary procedures, as amended from time to time.
e. It is every user's duty to use the Council's computer systems responsibly, professionally, ethically and lawfully.
f. The Council's computer system is the property of the Council and is intended to be used predominantly for legitimate Council business. Only persons authorised by the respective Director may access the Council's computer systems and only to the extent that such access is required to assist them in the performance of their work.
g. Use of the Council's computer systems is provided primarily to assist users in the performance of their work function for and on behalf of the Council.
h. All council owned electronic equipment used by users is to be considered the property of the George Municipality. All data, messages, or files created while using the equipment is also considered the property of the municipality. **The municipality reserves the express right to monitor and review all activities of the user, including information created or obtained by the user.**
i. Essential computer equipment includes: network file servers, workstations attached to networks that perform after-hours system backups and computers receiving data after-hours. It is recommended that these systems be kept on but signed off to "login" state for security purposes.
j. Users are not to place personal copies of software or data on any municipal equipment. This includes, but is not limited to, games, screen savers and questionable material. If found, the software or data will be removed, and a memorandum sent to the user's Department Manager outlining the evidence found and the action taken to remove it.
k. It is municipal policy that municipal owned software is not to be taken home and installed on a user's home computer for personal use, regardless of the software's licensing agreement.

l. Unless otherwise dictated by public disclosure laws, all information regarding the computer systems, or data created by users, are to be considered confidential. Removing of data from the municipal offices without the express consent of the Manager of the Department is considered a breach of this confidentiality and is punishable in terms of the disciplinary procedure of the municipality.
m. The user may represent the municipality in its dealing with the outside world and as such the use of the computer system - which should carry identification of the municipality - may not only negatively reflect on the name and reputation of the municipality but may also possibly bind the municipality and incur obligations and liability on behalf of the municipality and/ or the user.
n. No user may pry into the personal affairs of other users without legitimate permission for accessing their files or communication. This access will only be granted by the relevant Director or Municipal Manager.
o. Computer systems and computer resources must be managed and controlled for the benefit of the organization.
p. Equipment should be utilized for the sole purpose of an employee's functions. No forms of games are allowed on any computer equipment owned by George Municipality.

7 ACCESS AND USE

a. Access to the Councils computer system from the Councils premises shall only be attempted by way of computer equipment made available by the Council to users. Under no circumstances are users allowed to use or attempt to use their own or other computer equipment of any nature to access the Councils computer system.
b. Remote access shall be granted to users at the sole discretion of the CIO.
c. Remote access to the Councils computer system from outside the Councils premises shall only be attempted by way of remote or laptop facilities provided by the ICT Department.
d. Councillors and authorized staff will be permitted to connect through the remote access connection.
e. If problems occur on a computer being used for remote connection, it is the responsibility of the user to bring the laptop/device into the ICT Department for the problem to be analysed there. No support will be given to non-municipal computers. The Municipality will accept no responsibility for any damage done to the computer or information stored, either during transit or when being worked on.
f. Only users may access the Councils computer system, e-mail and internet facilities by means of their authorized usernames and passwords.
g. Apart from the CIO, users shall not use any other username or password.
h. Users shall not knowingly allow the use of their username and/or password by anyone else and users are alerted to the fact that they are responsible for all work saved or retrieved, messages sent or received, or transactions carried out via the internet and e-mail under their username and password.

i. Users shall not (or even attempt to) access, copy, alter or delete the files or data of any other user.
j. Users shall not access or attempt to access networks or network drives in respect of which the user has no legitimate reason to access.
k. All users require the approval from the relevant Director to access the municipality's Local Area Network/Wide Area Network and Other Information Network Resources.
l. If a person is transferred or fills another person's post (even in an acting capacity), no change will be effected by the ICT section until the HR department requests it.
m. When a person leaves the employ of the Municipality, it is the responsibility of the HR department to inform the CIO.
n. Where a person is dismissed or suspended, the HR department is responsible for ensuring that the CIO and the ICT section are informed without delay, so that the relevant access can be suspended.
o. When appropriate, users (and/or groups of users) may be allocated a fixed amount of network disk space. This will only be imposed should the network disk space be abused.
p. Usage of flash drives / memory sticks are not allowed to be used on council equipment. Traditionally these devices pose the biggest threat for spreading viruses/malware.

8 PASSWORDS

To prevent the unauthorised access of the Councils computer system, passwords should comply with the following standards: -

a. Passwords are personal and must not be disclosed or lent to others.
b. Passwords should not be printed or stored online in any electronic form.
c. Passwords should have a minimum length of six alphanumerical characters, the use of a combination of letters, digits and characters is recommended.
d. Password may not be repeated within 12 changes of each other.
e. Use of passwords that can be guessed easily should be avoided.
f. Users will automatically be requested to change their password every 30 days.
g. Passwords must not contain the user's "Account Name" or "Full Name". Both checks are not case sensitive.
h. Passwords must contain characters from three of the following five categories:
    i. Uppercase characters of European languages (A through Z)
    ii. Lowercase characters of European languages (a through z)
    iii. Base 10 digits (0 through 9)
    iv. Non-alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/
    v. Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase.
i. Password account lockout threshold is set to 3 attempts. After 3 attempts the user will be locked out of their account and will need to log a call with the ICT helpdesk to reset their password.

j. Account lockout duration is set to 0 (forever). The password must then be reset by the system administrator.
k. Reset lock counter is set to 1440 minutes (24 hours). This will allow a user to attempt their password again after 24 hours.
l. SAMRAS and Ignite have their own unique passwords and they are not synchronised with the systems mentioned above.

9 BACK-UPS

The Municipality recognizes its need to maintain a high level of data security both internally and externally. The backup system is designed to recover from “catastrophic loss,” meaning complete destruction of a machine, set of machines, or the entire site. It also covers disk hardware failure, where only part of a machine needs recovery. The purpose is disaster recovery as opposed to covering for user mistakes.

It is assumed that: The ICT Department, and thus total disk storage, will continue to expand at a rate proportional to the previous year’s growth. The ICT Department will remain heterogeneous in computing equipment types, and that the heterogeneity is likely to increase, with all platforms requiring support.

A side effect of the backup system is the ability, in many cases, to restore individual files or sets of files for individual users. Doing this takes some time, thus priorities must be considered. Users are urged to ensure that their actions will bring about the desired results before pressing that last keystroke.

a. Data back-ups are the user’s responsibility.
b. Users are required to work on their hard-drives and back-up their data to OneDrive.
c. OneDrive has been provided as the back-up drive for each user. It is the responsibility of the user to make the necessary data backups of anything stored on the user’s hard-drive (desktop or laptop), as the ICT section cannot guarantee recovery of lost data.
d. Should the ICT section need to remove a user’s computer (for repairs, to reallocate, etc.), it is the responsibility of that user to ensure that they have made a copy of any data held on that computer. The ICT section is not responsible for such a loss and will not recover any such data that has been lost.
e. All messages on the e-mail server will be backed up regularly, but for practical reasons, no reliance should be placed on the ability of the ICT section to recover old messages which have not been saved to disk.
f. If users require a more secretive (but not necessarily secure) method of storing data, they may place a password on each file. However, should the password be lost, no-one can recover the file.

g. Employees are not allowed to make use of municipal owned storage space (i.e. servers, local hard drives, CD's, DVD's, memory sticks/flash drives/USB sticks, MP3 Players, external hard drives or any other removable media) for storing any of the following content:
    i. Private digital photos and sketches
    ii. Music files
    iii. Movie clips or full-length movies
    iv. Presentations and slide shows of entertainment nature

10 SECURITY

10.1 Physical Security

a. It is the responsibility of every user to ensure that their personal computer and associated peripheral devices are adequately protected against theft and damage.
b. In the case of a laptop computer, the user must ensure that a security cable is attached to the computer and secured to a desk or similar object.
c. In the case of a desktop computer and peripherals, the user must ensure that the office in which the desktop computer is resident is adequately secured at the close of business, or whilst unattended for any lengthy period by locking their office.
d. It is the Director's responsibility to ensure that all equipment is protected against misuse.
e. If you take any devices home, ensure that your doors are locked in the event of you leaving your premises and activate your home security system if you have one installed.
f. If you are staying in a hotel, lock these devices in a safe when you leave your room.
g. Keep these devices in your sight when passing airport checkpoints.
h. If you travel by car, lock these devices in the trunk when you leave your car.
i. Refrain from using these devices in locations that might increase the likelihood of damage and/or loss.
j. Keep food and beverages away from these devices.
k. Use a padded carrying case for these devices if available.

10.2 Logical Security

Users are responsible for ensuring the security, integrity and confidentiality of all data and information resident on the local memory of their personal computers.

In addition to the rules relating to passwords, Users shall take reasonable steps to ensure that no confidential information resident in the memory of their personal computer is:-

a. Visible during their absence from their PC.
b. Accessible by unauthorised persons.

Reasonable steps shall include:-

a. It is recommended that systems that are kept on, are signed off to a “login” state for security purposes.
b. Requiring passwords to open files containing confidential information.

10.3 Saving and Removal of Data

a. Users are strictly prohibited from saving Council data, confidential information or files onto disk, CD-ROM or any electronic or other storage media and removing them from the Council’s premises.
b. A user requiring access to Council data, confidential information or files whilst in any location other than at the Council premises, shall obtain the express permission of the relevant Director.
c. The remote use of Council data, confidential information or files may only be used by users in the performance of their work functions.
d. Council’s data, confidential information or files will remain the property of the Council always.
e. The user further undertakes to protect and safeguard the aforementioned data, information and files in a diligent and conscientious manner, and to perform a comprehensive virus scan where the data or information has been used on a personal computer or other device not belonging to the Council, prior to re-introducing data or information onto a Council PC or Council computer system.
f. It is every user’s responsibility to assure that his information is updated to safeguard against computer failures and the loss of data, the ICT department will not be held accountable for loss of data.

11 MAINTENANCE AND FAULTS

11.1 Computer System Maintenance

The technical staff in the ICT Section shall carry out all maintenance and support of the Council computer system and peripherals. Accordingly, users may under no circumstances: -

a. Attempt to repair the PC in their use, or those of other users.
b. Allow an unauthorised technician to perform any support, repair or maintenance on the Council computer system.

11.2 Faults

If users have software problems or faulty equipment, then the following procedures must be followed:

a. Report all ICT problems to the ICT Department (044-8019147) or via email on itsupport@george.gov.za . A job card will be issued to an available technician, and the problem will be seen to as soon as possible.
b. To assist timeously, the ICT department may require remote access to a user's machine to resolve the problem.
c. In the case of faulty equipment which cannot be fixed on site, a period of 7 days is needed to evaluate and assess the extent of the fault and to determine whether the equipment should be repaired or replaced.
d. All ICT equipment must be procured through the ICT department. Special request items will require motivation.
e. If there is no equipment available to replace faulty hardware, an alternative or temporary solution will be made where possible.
f. The ICT department will not be responsible for loss of data on computer equipment, due to hardware or software failures.

12 SOFTWARE

The Council has licensed or developed software for use on the Council computer system. This software is proprietary to the Council. To protect its proprietary interests and to ensure compliance with the terms of applicable licences, users are expressly prohibited from:-

a. George Municipality and its employees are legally bound to comply with the Copyright Act 8 of 1978 and all proprietary software license agreements. Noncompliance can expose George Municipality and the responsible employee(s) to civil and/or criminal penalties.
b. Copying Council software for use on anything other than the Council owned and supplied PC without the written permission of the CIO.
c. No person may install any software onto his or her computer, all installation must be done by the ICT Department, this includes the downloading of any program files from the Internet.
d. If at any stage a user believes that a software product, whether freeware, shareware or proprietary software, would assist in the furtherance of the Councils business then a motivation should be sent to the CIO.
e. Modifying, revising or adapting any Council software.
f. All new software must be tested, reviewed and approved by the ICT department prior to deployment on municipal equipment.
g. Users are referred to Appendix "B" of this policy for a list of approved software. This list will be updated on a regular basis.
h. Altering, or attempting to alter, yours or any others user's system configuration is prohibited.

i. Should anyone receive a CD or a disk that provides a demo of software or any other item, it must be presented to the ICT section, which will install them correctly for the user, and uninstall it when the usage has expired.
j. The ICT section may refuse to install any software should they believe that is not appropriate for the Municipality's ICT systems.
k. The ICT Department will provide software for staff members per their job requirements.
l. No person may copy, load or run any software that is not properly licensed.

13 HARDWARE

a. The appropriate department personnel will contact the relevant Director with a computer hardware need, including information from the department on the purpose and use of the computer hardware, the Director will give a written request to the CIO.
b. The CIO will establish the specifications of required ICT equipment based on the request and operational function to be performed.
c. Procurement of all ICT equipment is completed by the ICT Department.
d. The ICT Department arranges for installation and configuration of all computer hardware.
e. No outside equipment may be connected to the council's network without the CIO's permission.
f. No person may open a computer or carry out any hardware installations, repairs, modifications, etc. All such work must be carried out by the ICT section.
g. **All** Municipal ICT equipment remains the property of the ICT department and must be returned to ICT when an employee leaves the Municipality.

14 PRINTERS

a. All users that require printing facilities will have access to a printer.
b. All special purpose printing requirements must be discussed with the CIO.
c. No person may open a printer or carry out any hardware installations, repairs, modifications, etc. All such work must be carried out by the ICT department. The only exception is to replace an ink cartridge or correcting paper jams, which may be carried out by the user.
d. Network printers will be made available to staff within proximity and not based on departmental or directorate boundaries.
e. The Municipality will provide ink and toner cartridges for official printers only.
f. If any damage occurs with the printer, the user needs to notify the ICT helpdesk.
g. Users may not print multiple copies of the same document – the printer is not a copier and typically costs more per page to use. If you need multiple copies, print one good copy on the printer and use the photocopier to make additional copies.

h. Users are to try to limit paper usage by taking advantage of duplex printing (i.e. double-sided printing) features offered by some printers and other optimization features (e.g. printing six PowerPoint slides per page versus only one per page).
i. Avoid printing large files, as this puts a strain on network resources and interferes with the ability of others to use the printer.
j. Avoid printing e-mail messages. This is wasteful. Instead, use the folders and archiving functionality in your e-mail application to organize and view your messages.
k. Use the print preview option instead of printing a document to see what it looks like. This is wasteful.
l. Many printers do not support certain paper types, including vellum, transparencies, adhesive labels, tracing paper, card stock, or thicker paper. If you need to use any of the paper types, consult with the ICT section.
m. Colour printing is typically not required by general business users. Given the selective need, as well as the high cost per page to print colour copies, colour printers are minimized. Should you require colour copies, consult with the ICT section.
n. Replacement of Toners relating to the photocopiers will be the responsibility of the ICT Section and the service provider/s concerned.

15 VIRUS PROTECTION

Users are alerted to the fact that Viruses can cause substantial harm to the Councils computer systems. The damage caused is often not limited to hardware or software but can result in monetary loss to the Council because of lost production, maintenance and recovery of work. Therefore: -

a. The CIO is to ensure that the latest approved antivirus protection software has been installed on the PC, that it is permanently enabled and that the newest signature update is available.
b. Should any data be received by a user via disk; CD-Rom, internet, e-mail or any other source, a comprehensive scan of that data should be performed prior to loading that data to the computer system.
c. However, it still remains the responsibility of the user to make sure that their antivirus packages are up to date and if not, to contact the ICT section immediately.
d. If a virus is detected, the CIO must be notified immediately.

16 INTERNET USAGE

Users granted Internet access via the Council computer system are required to complete “Addendum A” to have Internet access, obtain the signature of their relevant Director and forward it to the CIO for activation. Due to the nature of the Internet, it is essential that Users

comply with the following rules. Failure to do so could have serious economic, financial and security consequences for the Council and may result in the personal liability of the User: -

a. Users may not use Council Internet access to conduct any other business than that of the Council except as otherwise authorized by the relevant Director who shall inform the CIO or his/her designated alternate in writing thereof.
b. Users may not use Council Internet access to host or display personal web pages.
c. User's internet access / usage can be monitored without prior notification if George Municipality deems this necessary. If there is evidence that a user is not adhering to the guidelines set out in this policy, George Municipality reserves the right to take disciplinary action, including termination and/or legal action.
d. Users using the Internet are representing George Municipality. Users are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner.
e. Users must not use the Internet for purposes that is illegal, unethical, non-productive or harmful to George Municipality.
f. No user may use a computer to access or download any inappropriate item, which may - inter alia - include:
    i. Any item which carries any defamatory, discriminatory or obscene material.
    ii. Any item which carries any sexually explicit message, images, cartoons or jokes.
    iii. Any item which contain religious, racist or sexist slurs.
    iv. Any item which may be seen to be insulting, disruptive, and offensive to other people.
g. Users may not browse or download any documents or images not related to Council business.
h. Users may not subscribe to or participate in Chat Groups, Bulletin Boards, Newsgroups, or discussion groups that are not work related and have not been approved in advance by the relevant Director in consulting with the CIO;
i. Unless specifically authorised otherwise, Users may not transact on behalf of the Council via the Internet (i.e. purchase of goods or services).
j. Downloading of data via File Transfer Protocol (FTP) Websites is permitted if it is work-related and prior permission has been obtained from the Relevant Director in consultation with the CIO or his/her designated alternate.
k. Users are strictly prohibited from posting sensitive information such as Usernames, passwords, security codes or Server-specific information which could assist third parties wishing to gain unauthorised access to the Council computer system.
l. Users are prohibited from publishing or transmitting confidential information on or via the Internet. If a situation exists where prohibited information must be transmitted, written approval will be required from the relevant Director and the CIO or his/her designated alternate prior to the transmission or publication of such information on or via the Internet.
m. Users may not knowingly introduce viruses into the Council computer system.
n. Subscriptions to online services are limited only to services that will enhance and promote the business of the Municipality and subject to Municipal Manager's approval.

o. Electronic Banking and other such personal services is permitted to all users but the Municipality will not be held liable for any activities pertaining to these services.
p. This privilege regarding personal services may be revoked if it found that its use is impacting negatively on the performance of the employee.
q. Anyone seen abusing the internet, must be reported to the CIO.

17 E-MAIL USAGE

a. E-mail is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner.
b. The Council e-mail system may not be used:
   i. to initiate or forward any chain-message or other message which asks the recipient to forward such message to multiple other users unless required for work purposes;
   ii. to send frequent unsolicited Commercial e-mail to persons with whom the sender does not have a prior relationship;
   iii. to send frequent and/or numerous e-mail messages with the intention of disrupting or inconveniencing the receiver;
c. The use of the Council e-mail facilities to send, download, display or store prohibited material is strictly prohibited.
d. No user may use email to send any inappropriate items, which may - inter alia - include:
   i. Any item which carries any defamatory, discriminatory or obscene material.
   ii. Any item which carries any sexually explicit message, images, cartoons or jokes.
   iii. Any item which contains religious, racist or sexist slurs.
   iv. Any item which may be seen to be insulting, disruptive, and offensive to other people.
e. No employee shall knowingly receive or store e-mail or any form of electronic communication containing Prohibited material.
f. If any employee is uncertain as to whether any material or statement constitutes Prohibited material, such employee must obtain clarification from the relevant Director without delay.
g. E-mail containing Prohibited material which has been inadvertently received shall be deleted by the employee receiving such e-mail, immediately that he or she becomes aware of the content thereof and the incident must be reported to the relevant Director and the CIO or his/her designated alternate without delay.
h. Although by its nature e-mail seems to be less formal than other written communication, the same laws apply, and therefore must follow the communication policy of George Municipality.
i. No users may send e-mail messages using another person's e-mail account.
j. All users are expected to read their E-mail regularly.
k. E-mail messages are written business records and are subject to George Municipality's rules and policies for retaining and deleting business records.

l. You must have no expectation of privacy in anything you create, send or receive on the Council's computer system. Your e-mails can be monitored without prior notification if it is deemed necessary. If there is evidence that you are not adhering to the guidelines set out in this policy, George Municipality reserves the right to take disciplinary action, including termination and/or legal action.
m. All e-mail accounts maintained on the council's e-mail system are property of George Municipality.
n. No users should forward e-mail from outside that is "spam" – i.e. chain- letters, requests for help with worthy causes, etc.
o. All users are expected to undertake house-keeping of their e-mail systems on a regular basis. This involves deleting or archiving (as appropriate) messages that are no longer required. All attachments which need to be kept should be saved to disk, and the e-mail deleted. Users are also required to empty the "Deleted items" folder on a regular basis.
p. The e-mail system is not a system to archive important information or messages; this should be saved to the relevant disks or network drives. The ICT section will not take responsibility for lost / archived or missing email messages.
q. No spamming is allowed and software is in place to monitor and prohibit this action.
r. Users may not to disguise their identity while using the Council e-mail system.
s. Users may not alter the "From" line or any other indication of the origin of an e-mail message.
t. When communicating to many recipients, especially external of the municipality, the email addresses must be placed in the "Bcc" section of the email. This is to protect email addresses from spammers.
u. E-Mail signatures must be aligned to the George Municipality corporate identity and must not contain personal slogans or sayings.

17.1 E-Mail personal use

Although George Municipality's e-mail system is meant for business use, George Municipality allows use of e-mail for personal use if certain guidelines are adhered to:

a. Personal use of e-mail should not interfere with work.
b. Personal e-mails must also adhere to the guidelines in this policy.
c. Personal e-mails are kept in a separate folder with an appropriate name.
d. The forwarding of chain letters, junk mail, jokes and executables is strictly forbidden.
e. No mass or chain mailings, i.e. messages containing instructions to forward the message to others.
f. All messages distributed via the Council's e-mail system, even personal e-mails, are George Municipality's property.

17.2 Legal risks of e-mail

a. If you send or forward e-mails with any libellous, defamatory, offensive, racist or obscene remarks, you and George Municipality can be held liable.
b. If you unlawfully forward confidential information, you and George Municipality can be held liable.
c. If you unlawfully forward or copy messages without permission, you and George Municipality can be held liable for copyright infringement.
d. If you send an attachment that contains a virus, you and George Municipality can be held liable.

18 MONITORING, ACCESS TO AND DISCLOSURE OF E-MAIL AND INTERNET USE

18.1 Monitoring

The Council computer system is provided to employees, at Council expense, for the employees' use on Council business. To protect its rights and interests, the Council has procured a software monitoring application, which routinely monitors all Internet usage and e-mail traffic on the Council e-mail system. The application is designed to alert the CIO or his/her alternate to any prohibited use of the Council e-mail system and furthermore identifies forbidden words, strategic phrases relating to strategic projects and confidential files of the Council. Thus, whilst all e-mail will not be routinely read, those e-mails identified by the software as potentially infringing this policy may be accessed and read by the CIO or his/her alternate. The Council reserves the right to access and read the contents of e-mail messages and track Internet Usage in the following circumstances: -

a. Insofar as it is required by law or by legal obligations to third parties to do so,
b. If it has a legitimate business need or reason to do so,
c. To protect its interests if it reasonably suspects that an employee has committed or is committing a crime that might be aimed at or attributable to the Council,
d. If it is of the bona fide opinion that such access or disclosure may be necessary to investigate a breach of the security of the e-mail system or of this policy,
e. If, subject to the restrictions set out below, the Council will not seek to obtain access to the contents of any employee's e-mail files without the permission of the employee concerned.

Should the CIO or his/her alternate encounter indications of illegal activity or violations of Council policy or security, the CIO or his/her alternate shall investigate further and report any finding to the Municipal Manager.

Employees must ensure that all business-related e-mail messages that should be available to other employees of the Council are also available. The employee consents to access by the Council to protect system security or the Councils proprietary rights.

18.2 Unauthorised use to be reported

Authorised Users shall not knowingly permit the unauthorised use of the Council e-mail system. Any Unauthorised use of the Councils e-mail system must be reported without delay to the relevant Director in which the Unauthorised use occurred, and to the CIO or his/her alternate without delay.

18.3 Consequences and Violation

a. The terms and conditions of this policy have the force and effect of Councils Standard Conditions of Service, the Audit Regulations and such legislation as may be applicable.
b. Penalties for contraventions of this Policy may expose the User to disciplinary action in accordance with the Councils Standard Conditions of Service as amended from time to time.
c. Management reserves the right to discipline offenders in terms of this Policy.
d. A User who contravenes the terms and conditions of this policy understands that he or she will be acting outside of the course and scope of his or her employment as such conduct is expressly forbidden by the Council.

19 3G – DATA USAGE

a. The purpose of providing a 3G device is to enable the following functions:
   i. Accessing the internet and web-based e-mail while not connected to the municipal network (off-site) usually due to being out of town; and
   ii. Remote network/server support (for ICT personnel).
b. 3G connectivity is provided to all Councillors, Directors, Deputy-Directors, MM and ICT officials. Connections to other officials are approved by the relevant Director, if sufficient funds are available on the budget.
c. The 3G device and sim card must be returned to the ICT department upon leaving the employment of George Municipality, or if the Director considers that an official no longer requires the use of such a device.
d. By receiving a 3G sim card, the user accepts responsibility for the safeguarding thereof for the period it is assigned to him. If the device or sim card is lost, the ICT department

must be notified immediately. If there is a cost incurred for a new sim card, this will be for the user's account.

e. Since the usage of 3G devices gives access to Internet and E-mail functionality, the user must abide by the policies and procedures already described in those sections dealing with internet and e-mail in the ICT policy.
f. 3G connectivity is provided by a single service provider and there are varying levels of connectivity based on geographical location. The strength/availability of connectivity is not within the ICT department's control.
g. 3G contracts are managed by the ICT Department and the costs associated with the contract are for the relevant department's cost. Any costs associated with exceeding the package procured will be for the user's own personal account.
h. All user accounts are capped, if a user reaches their cap before the month end, the user will need to provide proof of available funds to the ICT department before adding additional data for the rest of the month.

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) POLICY

This Policy is effective from the date of approval by the Council, as per the approved system of Delegations of the George Municipality.

Signed at GEORGE on the **day** of ___**May 2023.**

DR MR GRATZ
MUNICIPAL MANAGER

20 ANNEXURE A – SYSTEMS AND NETWORK ACCESS APPLICATION

MUNISIPALITEIT GEORGE MUNICIPALITY
ICT Systems & Network Access

First Name:_____**Surname**_____

Known as :_____
(Please use block letters)

Employee number / I.D Number:

Directorate	
Department	
Section	
Job Title	
Immediate Supervisor	

I require access to the following systems of council to perform the functions of my job:

System	Yes	No
Office 365		
Internet		
Network		
Pre-paid vending		

System	Yes	No
SAMRAS		
GIS		
Ignite		
Collaborator		

Other software not listed above:

_____

Provide motivation for software requested that is not listed:

I do hereby declare the following:

a) I have read and understand the terms and conditions of the ICT Policy.
b) I am sufficiently trained in the use of the Councils' Computer Systems to comply with the terms and conditions of the ICT Policy.
c) I am aware that I have no expectation of privacy in accordance with the terms and conditions of the ICT Policy and hereby consent to monitoring of my e-mail and internet usage as described in the ICT Policy.
d) I am aware that the terms and conditions of the ICT Policy have the force and effect of Council Standard Conditions of Service and that disciplinary action may be taken against me for violation of the terms and conditions of this Policy.

Signature	**Date**
Manager/Director Signature	**Date**
Manager / Director Name:	

THIS DOCUMENT WILL BE PLACED IN OUR ICT FILE.

21 ANNEXURE B – APPROVED SOFTWARE

ALL MICROSOFT PRODUCTS	
ADOBE: Acrobat Reader Trend Micro: Antivirus WINZIP WINRAR SAMRAS FlexGen TadLink Novel Groupwise Collaborator ESRI - GIS Software 3G Software Altech Netstar Google Chrome SCADA AllyCAD AutoCAD InDesign iMindMap iMQS VEEAM VLC Media Player VMWare PMAX (metering) MAP 120 (metering) MAP 110 (metering)	PQRM (quality of supply) OSPRY Lite (quality of supply) Netlog (logging) Elog (logging) Teamviewer (remote desktop viewing) AcSELerator RTAC (Comms) AcSELerator Quickset (protection) AcSELerator Architecture (protection comms) AcSELerator Analytic Assistant (fault analysis) Settings Assistant (Comms processing) Adroit (SCADA) Notepad ++ (programming) SEL Compass (protection) Wireshark (network monitoring) Genius suite (printing) OS2030 (multiplexers) Test Universe (testing) FRAnalizer (testing) Omicron CPC (testing) MPC (load control) ROP (load control) ABB (protection) ecControl (load management) Look@Lan (network ping) TransportX (oil testing) About Time (time syncing)

(This list is open to amendment/addition at the CIO's discretion)