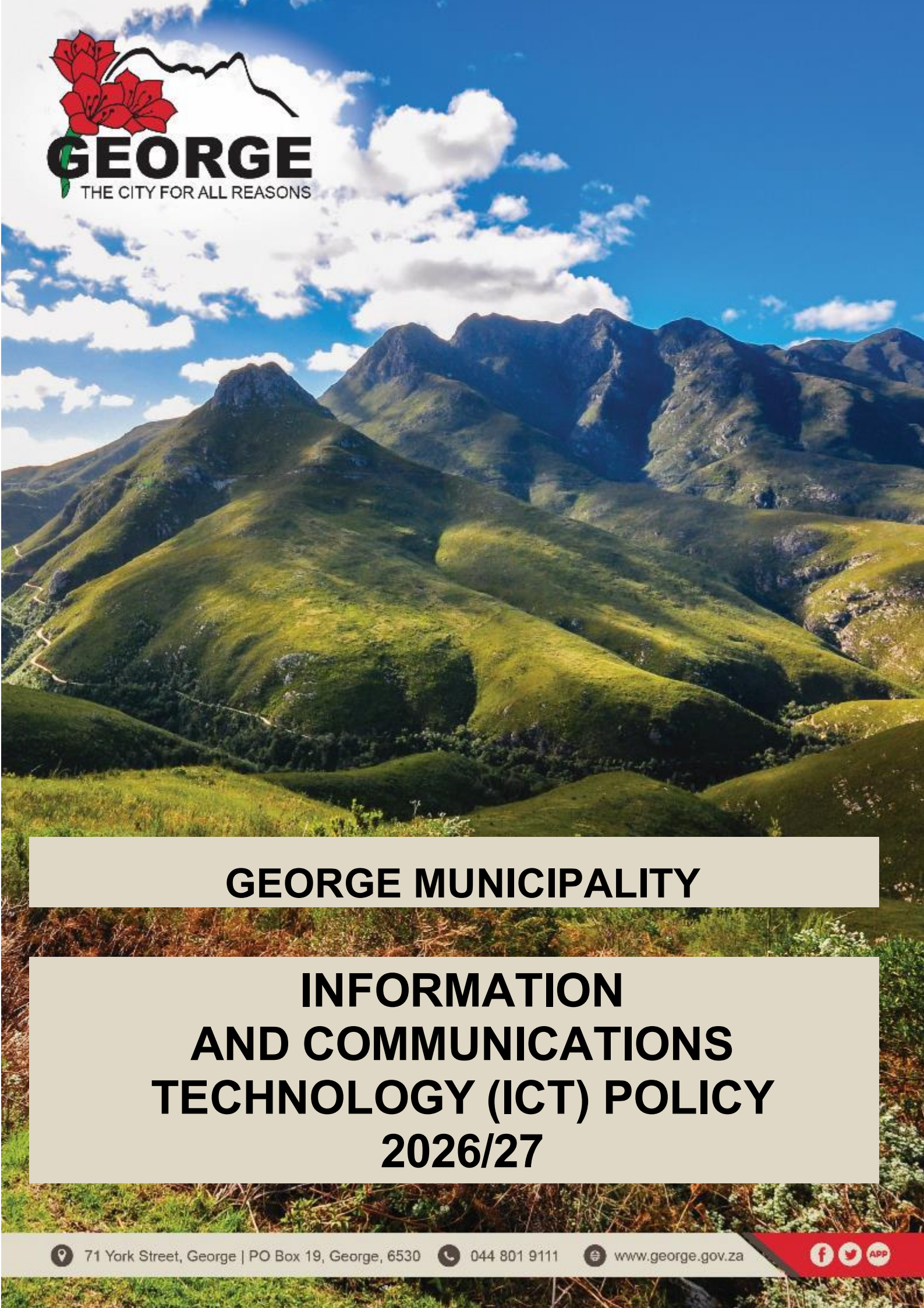

GEORGE MUNICIPALITY

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) POLICY 2026/27

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 capital, hardware, software and financial resources to create these systems.

The enclosed policies and directives have been established to, amongst other things:

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.
g) Ensure that IT value is realized and enables improved service delivery.

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

This ICT policy is also known as the Municipal Corporate Governance of ICT Policy.

2 ADMINISTRATION OF POLICY

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

If any conflict or ambiguity exists between this policy and any older version of it, or any other annexures or relevant policies, THIS policy will supersede all others in meaning, definition, and interpretation, as relevant and appropriate. Furthermore, in any other issues require interpretation or discretion related to this policy or anything other in its scope, this will reside with the CIO for final decision/clarification.

3 BREACH OF POLICY

Violations may result in disciplinary or any other appropriate action.

Violations and/or failure to observe these guidelines may result in disciplinary action by the George Municipality in accordance with the relevant 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

CIO: A chief information officer (CIO) is the corporate executive in charge of management of information technology (IT) strategy, systems, integration, technology, and implementation. This role is currently designated to be satisfied by the ICT Manager. Municipality. This CIO in the technology context may differ from the CIO in the context of access to information, documents, and records in terms of the archive legislation or PAIA legislation.

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 or electronic form containing instructions and placeholders for data entry to monitor progress through a Standard Operating Procedure and to ensure proper record-keeping for internal and external audits, controls, and general governance.

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 organisation.

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 and in particular contexts also tablet.

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

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 or notebook/laptop.

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.

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.
IV. Attempts to harvest information and details which can be used for phishing or mailing lists.

Municipality / Municipal 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 Municipality.

Municipality / Municipal e-mail: The computer hardware and software supplied by the Municipality, including e-mail application software, routers and servers, related hardware, and network infrastructure for the sole purpose of transmitting electronic mail messages/documents/files 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 the Municipality 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).

Permission/Approval: This does not only imply traditional hard copy forms and documents physically signed but in the modern context may be via an email, memorandum, electronic system like Collaborator or even in some cases verbal/telephonic or via WhatsApp or any other communications app like Teams chat etc.

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 Municipality 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 director, the CIO or his/her alternate.

Server: Computers designed to support a computer network that allows users to share files, application software, and hardware. This could be physical on-premises servers or virtualized servers in the cloud/azure/alternative.

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

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

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

Virus/Malware: 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 and practices.

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 recognized ICT standards were leveraged in the development of this policy:

- Western Cape Municipal Information and Communication Technology Governance Policy Framework
- Control Objectives for Information Technology (COBIT)
- ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls
- King Code of Governance Principles

6 GENERAL COMMENTS

a. The Municipality relies heavily on computer systems to conduct its business.

b. The Municipality makes it obligatory for each user to sign/accept an acknowledgement that he has read and understands the Municipality's ICT policy and accepts the responsibilities which is placed on him as a user. These documents are provided at induction or when the relevant ICT hardware is received by the user.

c. The terms and conditions described in this policy apply to all users of the Municipality computer systems wherever they may be situated.

d. The Municipality's computer systems are an extremely important asset, and as such, mistreatment, or abuse thereof by a user may, in the Municipality's discretion, render such user liable for disciplinary action in accordance with the Municipality's disciplinary procedures and related policies, as amended from time to time.

e. It is every user's duty to use the Municipality's computer systems responsibly, professionally, ethically and lawfully.

f. The Municipality's computer system is Municipality intended to be used predominantly for legitimate Municipality business. Only persons authorised by the respective Director/Manager may access the Municipality'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 Municipality's computer systems is provided primarily to assist users in the performance of their work function for and on behalf of the Municipality.

h. All Municipality 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. Where unique circumstances exist to vary from this recommendation, the request to soften this requirement must be made to and approved by the CIO.

j. Users are discouraged from placing personal copies of software or data on any municipal equipment. This includes, but is not limited to, games, photos, music, personal documents, screen savers and questionable material. If found, it may be removed, and may be reported to the user's Department Manager/Director outlining the evidence found. It is recommended that permission and approval is requested from the relevant Director and CIO where applicable.

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. The before mentioned however may be allowed under unique circumstances where applications/requests are made for approval to the relevant Director in conjunction with the CIO.

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/systems without the express consent of the relevant Director of the Department is considered a breach of this confidentiality

and is punishable in terms of the disciplinary procedure of the municipality as well as any other relevant policy or legislation.

m. The user may represent the municipality in its dealing with the outside world and as such the use of the computer system may not negatively reflect on the name and reputation of the municipality and may not possibly bind the municipality and incur obligations and liability on behalf of the municipality.

n. No user may pry into the personal affairs of other users without legitimate permission for accessing their files or communication. If required with good cause such access will only be granted by the relevant Director, CIO, or Municipal Manager.

o. Computer systems and computer resources must be managed and controlled for the benefit of the Municipality.

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. The prior will however be assessed along with potential historic default software and games which are initially installed on a default Windows installation and may be of no fault of the user.

q. On any matters within the scope and ambit of this policy and within the ICT domain and discipline, all Directors/Executive are obligated to work in conjunction with the CIO and to constantly consult with the CIO on any topics and matters relating to ICT or this policy. Not even a Director/Executive has the authority to do just what he or she wishes within the ICT space without the express approval/permission/support of the CIO.

7 AUDIT MATTERS

IT Benefits Realisation Process:

An IT Benefits Realisation process is a structured approach to ensure that the anticipated benefits from investments in Information Communication Technology (ICT) are effectively identified, tracked, and realized. It involves defining clear objectives and outcomes for ICT initiatives, establishing key performance indicators (KPIs) to measure progress and success, and implementing mechanisms for monitoring and evaluating the achievement of benefits over time.

Below is the general outline of the IT Benefits Realisation process:

- Define Objectives and Expected Benefits:

  Clearly articulate the objectives of each ICT initiative and the specific benefits expected to result from its implementation. These benefits include cost savings, increased efficiency, improved customer satisfaction, or enhanced competitiveness.

- Identify Key Performance Indicators (KPIs):

Establish measurable KPIs that align with the defined objectives and expected benefits. These KPIs should be specific, quantifiable, and relevant to the goals of the ICT initiative. For example, if the objective is to reduce operational costs, KPIs could include metrics such as ICT expenditure as a percentage of revenue or the average time to resolve ICT issues.

- Baseline Measurement:

  Conduct a baseline assessment of current performance levels for each KPI to provide a benchmark for comparison. This could involve gathering data on relevant metrics before the implementation of the ICT initiative.

- Monitor and Track Progress:
  Implement systems and processes for ongoing monitoring and tracking of performance against the established KPIs. This may involve regular reporting, dashboards, or automated alerts to highlight deviations from expected outcomes.

- Evaluate and Adjust:

  Regularly evaluate progress towards the identified benefits and adjust as necessary. If deviations from expected outcomes are identified, analyse the root causes and take corrective actions to realign the initiative with its objectives.

- Document Results:

  Document the realised benefits achieved through the ICT initiative, including any quantitative improvements and qualitative impacts. This documentation provides evidence of the value delivered by ICT investments and informs future decision-making processes.

- Communicate and Celebrate Success:

  Communicate the achieved benefits to stakeholders across the Municipality to demonstrate the value of ICT investments. Celebrate successes and recognize the contributions of team members involved in driving positive outcomes.

By implementing an IT Benefits Realisation process, the Municipality can ensure that their investments in ICT deliver tangible value and contribute to overall business objectives. This process also facilitates accountability, transparency, and continuous improvement in ICT governance and decision-making.

The above is achieved and satisfied by the ICT performance measurements and indicators which are regularly monitored and reported on and reviewed. The various strategic and operational projects are monitored and reported on at the regularly held ICT steering committee which consists of role-players from all Directorates and the entire senior management executive team.

IT Value and performance measurement processes:

Establishing IT value and performance measurement processes is essential for the Municipality to assess the effectiveness of their ICT investments and ensure alignment with strategic objectives. Following is a framework for these processes:

- Define IT Value Drivers:

  Identify the key drivers of value that ICT can deliver to the Municipality. These may include improving operational efficiency, enabling innovation, enhancing customer experience, or supporting strategic growth initiatives. Each value driver should be linked to specific business objectives.

- Develop Key Performance Indicators (KPIs):

  Define a set of KPIs that reflect the performance of ICT in delivering value to the Municipality. These KPIs should be aligned with the identified value drivers and measurable over time. Examples of ICT KPIs include system availability, response time, project delivery time, customer satisfaction, and return on investment (ROI).

- Establish Baselines and Targets:

  Determine baseline measurements for each KPI to provide a starting point for performance evaluation. Set targets or benchmarks that represent desired levels of performance or improvement. These targets should be realistic, achievable, and aligned with the Municipality's goals.

- Implement Measurement Mechanisms:

  Put in place mechanisms for collecting, analysing, and reporting data on the defined KPIs. This may involve deploying monitoring tools, conducting surveys, analysing financial data, or using other data sources relevant to ICT performance.

- Monitor Performance:

  Continuously monitor performance against the established KPIs to track progress and identify areas for improvement. Regularly review performance data to ensure that ICT initiatives are delivering the expected value and adjust strategies as needed.

- Conduct Performance Reviews:

  Periodically conduct formal reviews of ICT performance to assess the effectiveness of ICT investments and initiatives. These reviews may involve analysing trends, comparing actual performance to targets, identifying root causes of performance gaps, and making recommendations for improvement.
- Integrate with Governance Processes:

  Integrate ICT value and performance measurement processes into broader governance frameworks, such as ICT governance or enterprise performance

management. Ensure that there is clear accountability for ICT performance and that relevant stakeholders are involved in decision-making processes.

- Communicate Results:

  Communicate the results of ICT performance measurement efforts to key stakeholders, including senior management, ICT leaders, and business unit managers. Provide insights into the value that ICT is delivering to the Municipality and highlight areas of success as well as opportunities for improvement.

- Continuous Improvement:

  Foster a culture of continuous improvement by using performance data to identify best practices, learn from past experiences, and drive innovation in ICT processes and investments.

By implementing robust ICT value and performance measurement processes, the Municipality can effectively evaluate the contribution of ICT to business success, optimize resource allocation, and drive continuous improvement in ICT performance and outcomes.

As with the above paragraph on IT Benefit Realisation, this section on IT Value and Performance Measurement Processes are very similar and mostly addressed by the same mechanisms as previously mentioned regarding the performance management system, the ICT KPI's and baselines, reporting and oversight by the executive management team and steering committee.

ICT Acquisition and Disposal Processes

Developing comprehensive ICT acquisition and disposal processes is critical for ensuring that the Municipality procures and manages technology assets efficiently, securely, and in compliance with relevant policies and regulations. Here's the framework to guide the development of these processes:

- Policy Scope and Objectives:

  Begin by clearly defining the scope and objectives of the ICT acquisition and disposal processes. This may include specifying the types of technology assets covered (e.g., hardware, software, services), as well as the goals of the processes, such as optimizing costs, minimizing risks, and supporting business needs.

- Procurement Planning:

  Establish a structured approach to planning ICT procurements based on business requirements and strategic objectives. This involves identifying technology needs, conducting market research, defining selection criteria, and developing procurement plans that outline timelines, budgets, and resource requirements.

- Vendor Selection and Evaluation:

  Define criteria and procedures for selecting vendors and evaluating proposals during the procurement process. This may include conducting competitive bidding, evaluating vendor qualifications and capabilities, assessing technical and functional requirements, and performing due diligence on potential suppliers.

- Contract Negotiation and Management:

  Develop processes for negotiating contracts with selected vendors and managing contractual relationships throughout the lifecycle of the agreement. This includes defining contract terms and conditions, negotiating pricing and service levels, establishing performance metrics and reporting requirements, and ensuring compliance with legal and regulatory requirements.

- Asset Acquisition and Deployment:

  Specify procedures for acquiring, receiving, and deploying ICT assets into the Municipality's infrastructure. This may include processes for purchasing, receiving, inventory management, configuration, installation, and testing of hardware, software, and related components.

- Security and Compliance:

  Integrate security and compliance considerations into the ICT acquisition process to mitigate risks related to data breaches, cybersecurity threats, and regulatory non-compliance. This involves conducting security assessments, enforcing security standards, ensuring data privacy and protection, and verifying vendor compliance with relevant regulations and industry standards.

- Lifecycle Management:

  Establish processes for managing the entire lifecycle of ICT assets, from acquisition through disposal. This includes asset tracking and inventory management, maintenance and support, software licensing and renewal management, and end-of-life planning.

- Disposal and Decommissioning:

  Define procedures for decommissioning and disposing of ICT assets at the end of their lifecycle in a secure, environmentally responsible manner. This may involve data sanitization, hardware recycling or disposal, license deactivation, and contract termination.

- Documentation and Records Management:

  Document all activities related to ICT acquisition and disposal processes, including procurement decisions, contracts, asset inventories, disposal records, and compliance documentation. Maintain accurate and up-to-date records to support auditing, reporting, and accountability requirements.

- Training and Awareness:

  Provide training and awareness programs to ensure that staff involved in ICT acquisition and disposal processes understand their roles and responsibilities, as well as relevant policies, procedures, and best practices.

It is to be noted that Training remains a Human Resources function under the Directorate of Corporate Services. ICT has little control over what training is approved or considered, budgeted and planned. The Human Resources section has an official defined as the Training Officer and Skills Development Facilitator whom is tasked with arranging training of all staff in all needed aspects. ICT does not have the skills, capacity and resources to train all municipal staff.

By implementing robust ICT acquisition and disposal processes, the Municipality can streamline operations, reduce risks, optimize resource utilization, and ensure the effective and compliant management of technology assets throughout their lifecycle.

To address further gaps identified in the Information and Communication Technology (ICT) Strategy Plan & Strategy, it is essential to incorporate the following components:

Review and Update Frequency:

Clearly define the frequency of review for the ICT Strategy Plan and Policy. This ensures that the plan remains relevant and aligned with Municipality goals and changing business needs. Consider conducting periodic reviews at least annually or more frequently if significant changes occur in the business or technology landscape.

The strategy is reviewed annually and the current plan in use is reviewed on a monthly and two monthly bases by the ICT Steering Committee and the Executive Management Team.

IT Risks Mitigation:

Include a section in the ICT Strategy Plan that outlines the key ICT risks faced by the Municipality and strategies for mitigating these risks. This may involve identifying potential threats to data security, system availability, regulatory compliance, and other critical areas, and developing risk mitigation measures and contingency plans to address them.

ICT Risks is included in the internal audit and risk management frameworks. The risk register of Municipality specifically also includes a section of ICT risks, and it is updated at least annually.

Structure of IT Environment:

Provide an overview of the current structure and architecture of the IT environment, including network infrastructure, hardware and software systems, data centres, and cloud services. Describe how these components are interconnected and organized to support business operations and achieve strategic objectives.

George Municipality has minimal on premise servers left while most are running virtually in the Azure Microsoft Cloud hosted in Johannesburg and replicated to the Cape Town data centre. We are currently using a 300 meg Internet Primary Vodacom line which is Fibre based and backed up by a 300 meg Microwave link also from Vodacom. Our LAN use a combination of CAT5, CAT5e and CAT6 cable and we also have several fibre lines and links between most sites and buildings. We are a enterprise Microsoft client and our 800+ users all have standardized HP Laptops, and use mostly the Microsoft software and security stack. We use the SAMRAS financial system from Solvem, and Collaborator Document Management system by Business Engineering and Ignite for our Performance Management System. We have several smaller systems and vendors managed by the various user departments.

IT Services Delivery:

Clearly define the portfolio of IT services that the IT department is responsible for delivering to the Municipality. This may include services such as network management, help desk support, software development, infrastructure maintenance, and cybersecurity operations. Specify service levels, performance metrics, and service delivery models to ensure alignment with business needs and expectations.

The ICT section provides the general array of services listed above, within their capability and capacity. Several service providers and specialist vendors also exist in the space to fill gaps in capacity and skills. Service levels, performance metrics and defined and included in our performance management system and this policy.

Facilities Utilized by IT:

Describe the physical facilities and resources used by the IT department to support its operations, such as data centres, server rooms, office space, and equipment. Include information on security measures, environmental controls, and disaster recovery capabilities to ensure the availability and resilience of IT infrastructure.

ICT have a server room, as well as an office for the manager, one for the hardware workshop and one bigger space for the technicians. There is also a storeroom for parts. We use the same standard equipment as normal staff members, are defined above. The server room is protected by all the standard requirements being fire detection and prevention, raised floors for flooding, air conditioning for cooling, and biometric access control. Disaster recovery is satisfied by multiple backups across devices and into the cloud and replicated over data centres in multiple towns as well.

Planning Guidelines and Constraints:

Outline the planning guidelines and constraints that inform the development of the ICT Strategy Plan. This may include factors such as expected business growth, financial

constraints, regulatory requirements, technological trends, and Municipality priorities. Consider how these factors influence resource allocation, technology investments, and strategic decision-making within the ICT department.

ICT planning is informed by the organisation IDP planning and vision of Municipality, combined with expected budget and staff growth and expansion. ICT does constant research and remains updated on market and security trends and risks and plans for it accordingly within its capacity and resource constraints. The ICT Steering Committee is the strategic guide and forum to influence ICT and make critical decisions for ICT to execute.

Resource Requirements:

Identify the human, financial, and technological resources required to implement the ICT Strategy Plan effectively. This includes staffing levels, skill sets, budgetary allocations, hardware and software investments, and other resource requirements necessary to support IT initiatives and deliver expected outcomes.

These aspects are constantly accessed and reviewed and applications are annually made for additional staff capacity as the budget allows. Training is requested annually also but is also dependent on resource availability and budget constraints. Constant market research and policy influence hardware and software decisions.

By incorporating these components into the ICT Strategy Plan & Policy, The Municipality can ensure that their ICT strategy is comprehensive, adaptive, and aligned with business objectives. Regular review and updates to the plan, along with consideration of IT risks, infrastructure, services, facilities, planning guidelines, and resource requirements, enable the Municipality to effectively leverage technology to drive innovation, efficiency, and competitiveness.

To address the gaps identified in the Disaster Recovery Plan (DRP), it is crucial to take the following steps:

Approval and Finalization of the DRP:

Ensure that the DRP is formally approved by relevant stakeholders, including senior management, ICT leadership, and other key decision-makers. Finalize the document to reflect any updates or changes based on feedback received during the review process.

The DRP is covered by the clarification provided in the policy document on backups and the current scenario and status quo of our backups in the cloud, with replication between Johannesburg and Cape Town. Management and the ICT Steering Committee are aware if the current approach and are satisfied with the assurance the current solution provides.

Inclusion of Planned Maintenance and Testing:

Incorporate a section in the DRP that outlines planned maintenance activities and testing procedures for disaster recovery preparedness. Specify the frequency of DRP tests, such as annual, semi-annual, or quarterly tests, and describe the methodologies, scenarios, and objectives of each test.
The current solution for George Municipality does not require regular testing and none are required based on the current configuration, setup and services utilised.

Business Impact Analysis (BIA):

Conduct a comprehensive Business Impact Analysis (BIA) to assess the potential impact of ICT disruptions and disasters on critical business processes, systems, and functions. Identify key business processes, dependencies, and recovery priorities to prioritize resources and efforts for disaster recovery planning and testing.

The risk for ICT disruptions are severe, but the probability is incredible low making the risk below the threshold for concern. The only dependence for constant service is an Internet connection of which we have a primary, secondary and tertiary solution, as well as LTE dongles and internet access for staff, whom can also use their own personal home internet or any internet source like a coffee shop to work. Our system is universal and accessible from anywhere.

Disaster Recovery Testing:

Schedule and conduct regular disaster recovery testing exercises to validate the effectiveness of the DRP and ensure readiness to respond to IT disasters. These tests should simulate various disaster scenarios, such as hardware failures, data breaches, natural disasters, and cyberattacks, and evaluate the organization's ability to recover critical systems and data within predefined recovery time objectives (RTOs) and recovery point objectives (RPOs).

The current George Municipality modus operandi does not require the above steps which are irrelevant in a cloud-based solution like we have.

Risk Mitigation and Business Continuity:

Develop strategies and measures to mitigate the risks associated with the lack of a tested DRP, including financial losses, reduced productivity, and unavailability of critical business services. Implement measures such as redundant systems, data backups, emergency response protocols, and business continuity planning to minimize the impact of IT disruptions and ensure continuity of operations in the event of a disaster.

The prior response on the prior paragraph provides the confirmation that these issues have been sufficiently addressed, mitigated and are covered by the policy and the current practices.

Training and Awareness:

Provide training and awareness programs to educate staff on their roles and responsibilities in disaster recovery planning and testing. Ensure that all relevant personnel are familiar with the DRP, testing procedures, and escalation protocols to facilitate effective response and recovery efforts during emergencies.

The above is not needed in the context of George Municipality's current technology solution and architecture.

Documentation and Reporting:

Document all activities related to DRP approval, testing, and implementation, including test results, findings, and corrective actions taken. Maintain accurate and up-to-date records to support auditing, reporting, and compliance requirements.

Same comment as prior paragraph above.

By addressing these areas and ensuring the approval, testing, and documentation of the DRP, organizations can enhance their readiness to respond to IT disasters and minimize the potential impact on critical systems, data, and business operations. This proactive approach helps mitigate risks, improve resilience, and safeguard against financial losses and productivity disruptions resulting from service disruptions or disasters.

The current solution for George addresses sufficiently all the risks identified above and they are mitigated to an acceptable level for the ICT Steering Committee, Management and Municipality.

After careful review and consideration, we would like to confirm that all aspects mentioned in Section 21 of the ICT Security Controls Policy have been sufficiently addressed. Upon further internal assessment and consultation with relevant stakeholders, we have determined that our existing incident response planning and preparation, logging incident management activities, handling of forensic evidence, response procedures including escalation and communication protocols, maintenance of appropriate contacts with authorities and external interest groups, implementation of information security event reporting forms, and establishment of feedback mechanisms for incident reporters are comprehensive and aligned with industry best practices.

We are confident that our current policies and procedures provide adequate safeguards to detect, respond to, and mitigate security incidents effectively. Therefore, we believe that no further modifications or additions to Section 21 of the ICT Security Controls Policy are required at this time and will be scrapped in a forthcoming review.

IGNITE

It is to be noted that Ignite has two sections which are managed by two different sections from the ICT section:

Individual Performance – Is the responsibility of the HR department under Corporate Services

Organisation Performance – Is the responsibility of the IDP (Integrated Development Plan) department under Planning and Development.

Ignite is a hosted platform and web-based system which is hosted by the service provider and thus has no ICT infrastructure or need internally. Access is granted to it via the same user access request form which is utilized for all access requirement requests, currently done through the relevant Collaborator module, with full audit trail.

User access reviews are the responsibility of the relevant section in conjunction with the management of the relevant Directorates in which the various end users reside. An annual review should at least be done by the relevant sections in conjunction with the departments.

User Access Management:

It is to be noted that the procedures stipulated in this reviewed and amended ICT Policy supersede the requirements of prior outdated policies. As an example the New User Registration, Terminated User Removal and User Permission/Role Changes sections in 9.2, 10.3, 11.4 of the ICT User Access Management Policy which are in conflict with this policy are deemed replaced. These processes are now all automated and done via Collaborator electronically.

Also note that Section 17 of the User Access Management Policy is also rescinded as the (new) service provider has changed and developed its own internal controls for review. This affects the generated user and administrator logs and program change logs which are dealt with in the same fashion.

8 ACCESS AND USE

a. As required the Municipality will provide remote access to users on the approval of the CIO.

b. The Municipality will consider and authorise staff/vendors/providers as needed should require connecting through the remote access connection/VPN as needed.

c. If problems occur on a remote computer connection, it is the responsibility of the user to bring the laptop/device into the ICT section for the problem to be analysed there, unless the problem can be resolved remotely or virtually or any other way. The Municipality will accept no responsibility for any damage done to the computer or information stored, either during transit or when being worked on. Staff and personnel are expected to employ proper due diligence, care, security and safety of The Municipality’s assets removed from the premises.

d. Users may only access the Municipality's computer system, e-mail, and internet facilities by means of their own authorised usernames and passwords. The only variance would be where a unique situation exists which justifies a different handling which is brought to the attention of the CIO and has received approval.

e. Apart from the CIO and authorised ICT personnel, users shall not use any other username or passwords other than their own Municipal user details.

f. 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/documents/files sent or received, or transactions carried out via the internet and e-mail/system under their username and password.

g. Unauthorised users shall not access, copy, alter or delete the files or data of any other user.

h. Users shall not access or attempt to access networks resources or network drives in respect of which the user has no legitimate reason to access.

i. All users require the approval from the relevant Director and CIO to access the municipality's Local Area Network/Wide Area Network and Other Information Network Resources.

j. If a person is transferred or fills another person's post (even in an acting capacity), no change will be affected by the ICT section until the HR department requests it.

k. When a person leaves the employ of the Municipality, it is the responsibility of the HR department to inform the ICT section to make the relevant changes and/or terminations.

l. Where a person is dismissed or suspended, the HR department is responsible for ensuring that the ICT section is informed without delay, so that the relevant access can be suspended, unless an alternative arrangement or request was considered and approved by the relevant Director in conjunction with the CIO.

m. Usage of flash drives / memory sticks are discouraged to be used on Municipality equipment unless permission and approval is obtained from the relevant Director and CIO. The reason for the prior approval is because traditionally; these devices pose the biggest threat for spreading viruses/malware.

9 PASSWORDS

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

a. Passwords are personal and must not be disclosed or revealed to others.

b. Passwords should not be printed or stored online in any electronic form which can potentially be accessed by unauthorised individuals or persons.

c. Use of passwords that can be guessed easily should be avoided.

d. Passwords must not contain the user's “Account Name” or “Full Name”. Both checks are not case sensitive.

e. SAMRAS and Ignite and other systems may have their own unique passwords and they may not be synchronized with the users normal AD username and password.

f. The traditional and historic approach of regular monthly password changes every 30 days has been replaced by the best practice modern recommendations. The new norm is one complex/complicated/difficult password (which does not change) but is further supported by another layer of protection/security using Multi Factor Authentication (MFA) using SMS, voice, app approvals or one-time pins. This has been applied in George Municipality as a standard, replacing the old historic manner of password management. The provision of the cellphone number of the user to the ICT section is thus compulsory for self-service password resets and authentication.

10 BACK-UPS

The Municipality recognizes its need to maintain a high level of data security both internally and externally. The backup systems are designed to prevent “catastrophic loss”. The purpose is disaster recovery as opposed to covering for user mistakes and errors.

George Municipality is moving towards Microsoft Azure cloud use and functionality, and this has changed the past and historic practices for traditional backup and disaster recovery. Servers are mostly in the cloud which suffer no risk for environmental damage, electrical failures or loss and mitigates the need for traditional disaster recovery and redundancy practices. Servers in the cloud are based in the Microsoft Johannesburg data centre and duplicated/replicated to the Microsoft data centre in Cape Town. Backups are made in the cloud and whatever on premise physical remaining servers are also backed up to cloud storage. The George municipal Municipality and executive senior management is completely satisfied and assured in the current technology solution which replaced the historic practices of manual and physical backups and physical disaster recovery and replication sites.

All virtual servers in the cloud (Azure) are backed up daily as scheduled. Furthermore, they are replicated over multiple virtual machines, in the data centre and replicated across two towns 1500 km apart. The Management Team, the ICT Steering Committee and Municipality are satisfied that backups and redundancy are sufficiently addressed.

This backup practice and guidelines mentioned and confirmed in this policy replace that in any other policy and this policy supersedes any other on these aspects or topics.

a. Data back-ups remain primarily the user’s responsibility, supported by the ICT section.

b. Users currently work on their hard-drives and back-up their data to OneDrive/SharePoint/File Server. The intention is that users will start working primarily on the cloud systems and solutions to reduce the risk for hardware failure and loss.

c. OneDrive/SharePoint/File Server has been provided as a back-up solution 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 and can only assist by providing resources and mechanisms to do so.

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 any loss and cannot assure recovery of any such data that may been lost.

e. All messages/files/documents 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 such items 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, be aware that no-one may be able to recover the file.

g. Employees should not 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, documents and sketches
   ii. Music files
   iii. Movie clips or full-length movies
   iv. Presentations and slide shows of entertainment nature

   The determination of the extent of the above misuse being acceptable or not; would lie with the assessment of the CIO if unclear.

11 SECURITY

11.1 Physical Security

a. It is the responsibility of every user to ensure that their computer and associated peripheral devices are adequately protected/secured against theft and damage.

b. In the case of a laptop computer, the user should ensure that a security cable is attached to the computer and secured to a desk or similar solid object.

c. In the case of a desktop computer and peripherals, the user should 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 as best possible.

d. It is the users' responsibility to ensure that their 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/theft.

j. Keep food and beverages away from these devices to prevent accidents and damage.

k. Use a padded carrying case for these devices if available.

11.2 Logical Security

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

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

a. Visible during their absence from their PC.

b. Accessible by unauthorised persons.

Reasonable steps shall include: -

a. Systems that are kept on, are signed off to a "login/locked" state for security purposes. Where unique circumstances exist to vary from this recommendation, the request to soften this requirement must be made to and approved by relevant Director in conjunction with the CIO.

b. Requiring passwords to open files containing confidential information.

11.3 Saving and Removal of Data

a. Users are strictly prohibited from saving Municipality data, confidential information or files onto disk, CD-ROM or any electronic or other storage media and removing them from the Municipality's premises without permission, which is not in line with their work or job function.

b. A user requiring access to Municipality data, confidential information, or files whilst in any location other than at the Municipality premises, shall obtain the express permission of the relevant Director and CIO.

c. The remote use of Municipality data, confidential information or files may only be used by users and authorised individuals/companies in the performance of their work functions.

d. Municipality's data, confidential information or files will remain the property of the Municipality.

e. As and when possible, the user further undertakes to protect and safeguard the data, information and files in a diligent and conscientious manner, and to perform a comprehensive virus/malware scan where the data or information has been used on a personal computer or other device not belonging to the Municipality, prior to re-introducing data or information onto a Municipality PC, network or any municipal computer system.

f. It is every user's responsibility to assure that his information is safeguarded against computer failures and the loss of data, the ICT section will not be held accountable for loss of data. All users are obligated to consult with ICT to ensure they are aware of the tools and methods at their disposal to properly safeguard their data.

12 MAINTENANCE AND FAULTS

12.1 Computer System Maintenance

Only the correct authorised technical staff from the ICT Section shall carry out maintenance and support of the Municipality computer system and peripherals. Accordingly, users may under no circumstances (unless authorised by the CIO): -

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 Municipality computer system.

12.2 Faults

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

a. Report all ICT problems to the ICT section (044-8019147) or via email on itsupport@george.gov.za . The internal extension for ICT which can be dialled is 1266. A job card/ticket will be issued to an available technician, and the problem will be seen to as soon as possible. A ticket/reference number will be provided to the user which they can use to follow up on progress of their reported issue.

b. To assist timeously, the ICT section may require remote access to a user's machine to resolve the problem.

c. In the case of faulty equipment which cannot be repaired on site, a period of up to 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 in conjunction with the ICT section. Special request items will require motivation and approval between the relevant Director and CIO.

e. If there is no equipment available to replace faulty hardware, an alternative or temporary solution may be made available as possible.

f. The ICT section will not be responsible for loss of data on computer equipment, due to hardware or software failures.

13 SOFTWARE

The Municipality has licensed, procured or developed software for use on the Municipality computer systems. This software is proprietary to Municipality. To protect its proprietary interests and to ensure compliance with the terms of applicable licenses, 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 Municipality software for use on anything other than the Municipality owned and supplied PC without the permission of the CIO.

c. No person may without the permission of the CIO install any software onto his or her computer, all installation must be done by the ICT section, 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 Municipality's business then a motivation should be sent to the relevant Director and CIO for approval and consideration.

e. Modifying, revising or adapting any Municipality software is prohibited.

f. All new software must be tested, reviewed and approved by the ICT section prior to deployment on municipal equipment.

g. Altering, or attempting to alter, yours or any others user's system configuration is prohibited.

h. 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 first, which will install them correctly for the user, and uninstall it if practical when the usage has expired.

i. The ICT section may refuse to install any software should they believe that is not appropriate for the Municipality's ICT systems or creates any problems or risk for the Municipality.

j. The ICT section will in conjunction with the relevant directorate as far as possible provide appropriate software for staff members per their job requirements.

k. No person may copy, load, or run any software that is not properly legally licensed.

14 HARDWARE

a. 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 assist with the establishment of the specifications of required ICT equipment/specification based on the request and operational function to be performed as best practically possible within their ability and expertise.

c. Procurement of all ICT equipment is completed by the relevant department in conjunction with the ICT section.

d. The ICT department may arrange or facilitate installation and configuration of all computer hardware as best possible or may make a suitable arrangement to do so in conjunction with the relevant department or service provider.

e. Outside equipment should not be connected to the Municipality's network without the CIO's permission.

f. No unauthorised person may open a computer/device or carry out any hardware installations, repairs, modifications, etc. All such work must be carried out by a competent person from or provided by the ICT section.

g. All municipal ICT equipment remains the property of the Municipality and must be returned to the ICT section when an employee leaves the Municipality.

15 PRINTERS

a. All users that require printing facilities will have access to a printer as far as practically possible under the relevant circumstances.

b. All special purpose printing requirements must be discussed with the CIO for consideration and approval.

c. No unauthorised and unqualified person may open a printer or carry out any hardware installations, repairs, modifications, etc. All such work must be carried out by the ICT section, or a competent provider arranged in conjunction with ICT. The only exception is to replace an ink cartridge or correcting paper jams, which may be carried out by the user only if they are sufficiently skilled and abled to do so without causing any damage.

d. Network printers will be made available to staff within proximity and may not be based on departmental, building or directorate boundaries.

e. The Municipality will provide ink and toner cartridges for officially approved and procured printers only.

f. If any damage occurs to a printer, the user needs to notify the ICT helpdesk as soon as possible to assist.

g. Users must refrain from printing multiple copies of the same document and make all attempts to reduce printing.

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). If they are uncertain how to do this, they are welcome to contact the ICT section for assistance.

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 and save costs to Municipality.

k. Use the print preview option instead of printing a document to see what it looks like. This is a less wasteful alternative.

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 first.

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 and printing are to be minimized.

n. Replacement of Toners relating to the photocopiers will be the responsibility of the relevant service provider/s concerned.

o. At all costs please do not print documents unnecessarily or create manual paper-based procedures and systems. Digital and automated systems are preferred as it saves costs, is faster and safer when using centralized or cloud storage, servers, and

systems. If uncertain about any of this, please feel free to contact the ICT section for advice.

16 VIRUS/MALWARE PROTECTION

Users are alerted to the fact that viruses and malware can cause substantial harm to the Municipality's computer systems, networks, data, reputation, and cost money. The damage caused is often not limited to hardware or software but can result in further losses to the Municipality because of lost production, man hours, maintenance, and recovery of work.

Therefore: -

a. The CIO is to ensure that as best possible the latest approved antivirus/malware protection software has been installed on the PC, that it is permanently enabled and that the newest signature update is available as best practical and possible.

b. Should any data be received by a user via disk; CD-ROM, flash drive, USB, 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 or network of Municipality.

c. However, it remains the responsibility of the user to make sure that their antivirus/malware/Windows/store packages are up to date and if not, to contact the ICT section immediately for assistance.

d. If a virus/malware is detected, it must be dealt with as soon as possible.

17 INTERNET USAGE

Users granted internet access via the Municipality computer system are required to apply for it by obtaining the approval of their relevant Director/CIO and forward it to the ICT section 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 Municipality and may result in the personal liability and disciplinary steps against the User:

a. Users may not use Municipality Internet/dongle access to conduct any other business than that of the Municipality except as otherwise authorised by the relevant Director/CIO. The determination of the prior if unclear resides with the CIO.

b. Users may not use Municipality 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 investigate and 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 shall 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 Municipality business read in the context of a. above.

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 and CIO.

i. Unless specifically authorised/delegated/approved otherwise, Users may not transact on behalf of the Municipality 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 for which the ICT section can be contacted for assistance.

k. Users are strictly prohibited from posting sensitive information such as usernames, passwords, security codes or server/network-specific information which could assist third parties wishing to gain unauthorised access to the Municipality computer system.

l. Users are prohibited from publishing or transmitting confidential information on or via the Internet. If a situation exists where prohibited/confidential information must be transmitted, approval will be required from the relevant Director/CIO prior to the transmission or publication of such information on or via the Internet.

m. Users may not knowingly introduce viruses/malware or any risky items into the Municipality computer system and networks.

n. Subscriptions to online services are limited only to services that will enhance and promote the business of the Municipality and subject to the relevant Director in conjunction with the CIO for approval.

o. Electronic Banking and other such reasonable personal services are permitted to all users within reason, 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 or Municipality in any way, form, or cost.

q. Anyone seen abusing the internet, must be reported to the Director and CIO.

18 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/correct manner.

b. The Municipality 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/spam 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 Municipality 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 in conjunction with the CIO 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 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. Approvals and electronic/digital signatures via email carry the same weight as a physical documented approval or signature.

i. No users may send e-mail messages using another person’s e-mail account unless specifically authorised or requested to do so with valid cause and reason.

j. All users are expected to read their e-mail and process/update their Collaborator document management system and performance management system 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 Municipality's computer system. Your e-mails/documents/files can be monitored without prior notification. 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 and emails created/maintained on the Municipality's e-mail system remain the 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 regular housekeeping of their e-mail systems and device on a regular basis. This involves deleting or archiving (as appropriate) messages/files that are no longer required. All attachments which need to be kept should be saved to disk, archived, and the e-mails/files deleted where practical. Users are also required to empty the "Deleted items" folder on a regular basis.

p. The e-mail system is ideally 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 or files.

q. No spamming is allowed.

r. Users may not to disguise their identity while using Municipality systems.

s. Users may not alter or manipulate 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 manual and must not contain personal slogans or sayings. The Municipality corporate identity and branding guidelines held by the Communications department always retain preference in this regard.

18.1 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. The forwarding of chain letters, junk mail, jokes and executables is strictly forbidden.

d. No mass or chain mailings, i.e. messages containing instructions to forward the message to others.

e. All messages distributed via the Municipality's e-mail system, even personal e-mails, are George Municipality's property.

18.2 Legal risks of e-mail

a. If you send or forward e-mails with any libelous, 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 email/attachment that contains a virus/malware, you and George Municipality can be held liable.

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

19.1 Monitoring

The Municipality computer system is provided to employees, at Municipality expense, for the employees' use for Municipality business. To protect its rights and interests, the Municipality can procure software monitoring applications, which may assist with routinely monitoring all Internet/device/hardware/software usage and e-mail/file traffic on the Municipality e-mail and related system. Thus, whilst all e-mail/work will not be routinely read/checked, any e-mails/files identified as potentially infringing any policy may be accessed, reviewed, and read by the CIO or his/her alternate. The Municipality reserves the right to access and read the contents of e-mail messages/files/documents and track/assess 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 Municipality,

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 or disciplinary policy.

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

Employees must ensure that all business-related e-mail messages/files/documents that should be available to other employees of the Municipality remain available. The employee consents to access by the Municipality to protect system security or The Municipality's proprietary rights.

19.2 Unauthorised use to be reported.

Users shall not knowingly permit/allow the unauthorised use of the Municipality's e-mail and related network/system. Any unauthorised use of the Municipality's e-mail/related systems must be reported without delay to the relevant Director/Municipal Manager in which the unauthorised use occurred, and to the CIO without delay.

19.3 Consequences and Violation

a. The terms and conditions of this policy have the force and effect of The Municipality's 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 Municipality's Standard Conditions of Service or any other relevant policy as amended from time to time.
c. Management reserves the right to discipline offenders in terms of this Policy or any other related applicable policy.
d. A user who contravenes the terms and conditions of this policy or any other related and relevant 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 Municipality.

20 3G/4G/5G/LTE – DATA USAGE

a. The purpose of providing an internet device is to enable the following functions:

i. Accessing the internet and web-based e-mail/files system/documents/applications/ services while not connected to the municipal network (off-site) usually due to being out of town or working from home; and
ii. Remote network/server support (for ICT personnel).

b. Connectivity is provided to all Municipal Councillors, Directors, Deputy-Directors, Managers, MM, and ICT officials. Connectivity to other officials is approved by the relevant Director if sufficient funds are available in the budget of the relevant Directorate/ICT as relevant.

c. The device and sim card must be returned to the ICT section upon leaving the employment of George Municipality, or if the Director and CIO considers that an official no longer requires the use of such a device.

d. By receiving a 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 section must be notified immediately. If there is a cost incurred for a new sim card or device, this may be for the user's/directorate or Municipality account depending on the situation/merits.

e. Since the usage of certain devices give access to Internet and E-mail/file/document functionality, the user must abide by the policies and procedures already described in those sections in the ICT policy.

f. Connectivity may be 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 section's control.

g. Connectivity contracts are managed by the ICT section and the costs associated with the contracts may be for the relevant department's cost. Any costs associated with exceeding the package procured may be for the user's own personal account or for the relevant Directorate.

h. All user accounts may be capped, if a user reaches their cap before the month end, the user will need to provide valid reasons to the ICT section for their consideration before potentially adding additional data for the rest of the month or making an alternative arrangement.

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) POLICY

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

Signed at GEORGE on the ……. day of June 2026.

_____
MR BR ELLMAN
MUNICIPAL MANAGER

ANNEXURE 1– SYSTEMS AND NETWORK ACCESS APPLICATION FORM

(Please note that this form may still exist in its physical or paper form in some sections but may/will/can be replaced by any equivalent electronic/digital/ automated form or system to ease its use. The form then only exists as an example of the fields which may be relevant and info required to apply for access to above mentioned resources, not all fields are compulsory)

MUNISIPALITEIT GEORGE MUNICIPALITY
ICT Systems & Network Access

First Name: _____Surname: _____

Cell phone Number: _____

Employee number / I.D Number:

Directorate	
Department	
Section	
Job Title	
Immediate Supervisor	

I require access to the following systems of Municipality 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 Municipality's 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, files, documents, 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 Municipality Standard Conditions of Service and that disciplinary action may be taken against me for violation of the terms and conditions of this Policy or any other related relevant policy.

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

THIS DOCUMENT WILL BE KEPT ON RECORD.

ANNEXURE 2 – IMPLEMENTATION ROADMAP

OVERVIEW

This document contains the management practices that the municipality is not currently geared to implement. These are, however, seen as important, therefore the roadmap indicated that timeframe in which the municipality will implement each management practice. The Municipality reserves the right to add new items to the roadmap as we follow the phase in approach. All the items, however, will be implemented within the five-year strategy.

IMPLEMENTATION ROADMAP OF ICT GOVERNANCE FRAMEWORK

	Targeted Implementation Year			
Item - Policies	**Y2**	**Y3**	**Y4**	**Y5**
Management of ICT Framework with Domains			X	
Municipal Governance of ICT Charter			X	
Municipal Governance of ICT Policy			X	