

**KETU NORTH MUNICIPAL
ASSEMBLY**

**Information
Technology
Policy**



AUGUST, 2021

1. CONTENTS

1.	CONTENTS	1
2.	INTRODUCTION	3
3.	MEMBERS OF THE FIRST IT STEERING COMMITTEE	4
4.	VISION	5
5.	BACKGROUND	6
6.	OBJECTIVES.....	8
7.	CORE VALUES AND GENERAL PRINCIPLES.....	9
7.1	Collaboration:.....	9
7.2	Transparency	9
7.3	Partnership.....	9
7.4	Security and Equal Rights and Equity.....	9
7.5	Openness and Innovation	9
7.6	Supportive Institutional Environment:.....	10
7.7	Accountability and Protection for Assembly Resources:	10
7.8	Personal Use and Privacy:	10
7.9	Relationship with Departmental IT Policies:	11
8.	POLICY PRIORITY/FOCUS AREAS	12
8.1	ENGAGEMENT OF A DEDICATED AND TRAINED IT TEAM.....	12
8.2	ACQUISITION AND ACCESS TO REQUISITE IT GADGETS, AND RELATED MATERIALS.....	12
8.2.1	HARDWARE.....	12
8.2.2	SOFTWARE.....	14
8.3	GUIDELINES FOR CUSTODY, USE AND MAINTENANCE OF IT GADGETS	16
8.3.1	USE OF IT GADGETS.....	16
8.3.2	MAINTENANCE AND SERVICING OF IT GADGET (HARDWARE).....	16

8.4	NETWORK AND INTERNET ACCESS	16
8.4.1	GUIDELINES FOR USE OF INTERNET ACCESS PROVIDED BY THE ASSEMBLY.....	16
8.4.2	GUIDELINES FOR USE OF NETWORK ACCESS PROVIDED BY THE ASSEMBLY	18
8.4.3	THE RIGHTS OF THE ASSEMBLY	20
8.5	CYBER RISK MITIGATION AND SECURITY	21
8.5.1	Confidential Data.....	21
8.5.2	Protect personal and Assembly devices.....	21
8.5.3	Safekeeping and Use of Emails.....	22
8.5.4	Managing passwords.....	23
8.5.5	Data Transfer	23
8.5.6	Firewall	24
8.5.7	Additional Measures	24
8.6	INFORMATION TECHNOLOGY CAPACITY BUILDING FOR ALL STAFF.....	24
8.7	IMPLEMENTATION OF A PROGRESSIVE PAPERLESS SYSTEM.....	25
8.7.1	Take a stand.....	25
8.7.2	Leveraging on Technology (Social Media Platforms)	26
8.7.3	Digitization of Client and Records Department	26
8.7.4	Reducing Printing	26
8.8	PUBLIC INFORMATION MANAGEMENT	27
8.9	CREATING ENABLING ENVIRONMENT AND IT PROMOTION	27
9.	DISCIPLINARY ACTION	29
10.	COMMENTS, QUESTIONS, OR CONCERNS	30
11.	AMENDMENTS	31

2. INTRODUCTION

The management of the Ketu North Municipal Assembly in February 2021 saw the need to harness and harmonize all the ideas the Assembly has generated on Information Technology through a policy framework. It therefore appointed a four (4) member committee to develop and implement an Information Technology Policy for the Assembly. This work brings finality to the first part (IT Policy development) of the mandate of the Steering Committee. Please see the list of the members of the committee, overleaf.

The Ketu North Municipal IT Policy provides the policies for selection and use of IT within the institution which must be followed by all staff. It also provides the guidelines the Assembly will use to administer these policies.

The Assembly will also keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.

Any suggestions, recommendations or feedback on the policies specified in this document are therefore welcome.

These policies and procedures apply to all staff, members and stakeholders.

3. MEMBERS OF THE FIRST IT STEERING COMMITTEE

Stephen Eburam Osei _____ Chairman _____

Lawrence Senya _____ Secretary _____

Augustine Sekyim _____ Member _____

Alfred Seshie _____ Member _____

4. VISION

The vision of the Ketu North Municipal Assembly is to improve the lot of our people through good governance, quality service delivery and to make Ketu North Municipality a model district in Ghana.

The vision of the IT policy is to make the Ketu North Municipality a National Model District in Information and Technology through the creation of an enabling environment for the development, deployment and exploitation of IT tools to augment existing interventions; among staff, members and other stakeholders of the municipality for the improvement of the lot of the citizenry and achievement of other development goals of the Assembly.

5. BACKGROUND

The Ketu North Municipal Assembly exists to improve the living standard of the people in the Municipality through efficient use of both human and material resources for the provision of socio-economic infrastructure and services.

The Ketu North Municipal Assembly recognizes the vital role Information Technology plays in the achievement of its missions and related administrative functions as well as its importance in a forward-looking institution.

The use of Information technology has emerged as a key contributor to social and economic development enhancement efforts. Appropriate use of information technology engenders enhanced public awareness, participation and inclusiveness. This has the tendency to support the decentralization agenda and make relevant information available to the stakeholders in an accessible and secured manner.

The Assembly continues to make giant steps to make relevant technology and machinery more accessible to the general public and improving internal technology adoption and use, to ensure a more convenient, sustainable and futuristic performance of its functions.

This policy is expected to provide and assure a vibrant structure and administration for the increased protection of the Assembly's information, information technology resources; its development, deployment and exploitation drive to ensure appropriate access, custody, use and maintenance to support the transformation of the district into an information-rich, knowledge-based society and economy in Ghana.

To achieve these, the Assembly has thus declared the information technology sector a priority sector, and therefore intends to likewise prioritize its research and capacity development interventions in order to create an atmosphere conducive to attracting direct/indirect investment keeping in view the private sector's role in the development of information technology for the staff and stakeholders.

Additionally, the Assembly shall gradually computerize the functions and services of its relevant offices and support same to ensure improved service delivery, better flow of public information

through the web and social media portals, as well as progressively facilitate the provision of Internet facilities to all its offices and all parts of the municipality. The Assembly is also moving towards the use of information technology to promote e-commerce, e-education, e-health among others, and to transfer technology to rural areas.

Nevertheless, the Assembly has also taken cognizance of the threat Information technology poses in the current rapidly changing cyber environment and therefore sees the need for the enactment of appropriate policy and legislation to govern the use of information technology in the municipality (including the provision of legal sanctions).

6. OBJECTIVES

The objectives of this policy include:

- To promote the use of IT among staff and other stakeholders
- To provide a framework for procurement, adoption, training, custody, use and maintenance of information technology tools among staff of the Assembly
- To support the modernization of the decentralized services, operations and other functions of the Assembly effectively and efficiently
- To provide the institutional framework and support for the development, deployment, and use of information technology.

7. CORE VALUES AND GENERAL PRINCIPLES

The Ketu North Municipal Assembly accents to the following core values and general guiding principles.

7.1 Collaboration:

The Ketu North Municipal Assembly believes in collaborating other state agency and actors, as well as other stakeholders to improve the social and economic welfare of the staff and citizenry especially in the area of Information and Technology

7.2 Transparency

The Assembly believes in operating an open and transparent management of the municipal Assembly to enhance trust and cooperation. Information Technology has been recognized to be one of the surest ways to engender transparency and cooperation.

7.3 Partnership

The Assembly encourages partnership with any business entity, groups and investors especially in the Information Technology sector to enhance the progress of the municipality.

7.4 Security and Equal Rights and Equity

The management of the municipality shall ensure the rights, liberties and security of all inhabitants as well as the equitable distribution and management of all resources

7.5 Openness and Innovation

The Assembly encourages and thus solicits ideas, views and interventions that would enhance innovations and progress of the municipality.

7.6 Supportive Institutional Environment:

The Ketu North Municipal Assembly seeks to provide a supportive working, living, and learning environment. To accomplish this, we actively look for ways to encourage exchange and discourse, to bring together management, staff, and other stakeholders; and to build a community that encourages all of its members to succeed and grow.

7.7 Accountability and Protection for Assembly Resources:

All Members and Staff of the Assembly have responsibility to protect the resources for which they have access and/or custodianship. All Members and Staff of the Assembly are accountable for their access to and use of its resources.

7.8 Personal Use and Privacy:

The Assembly recognizes that members and staff have reasonable expectations of privacy in their uses of Information Technology Resources. However, rights to privacy are reserved for and by the Assembly due to the following reasons

- The Assembly owns and supplies these Information Technology Resources to its management, members and staff fundamentally for the purpose of accomplishing its functions, missions and vision.
- The Information Technology Resources may contain many closely shared environments and resources and the rights of other users must be considered and protected.
- Legal and ethical restrictions apply.

Individuals may have access to unreserved use through private or commercial systems located at their residence or elsewhere. Resources or systems owned and maintained by the Assembly are primarily intended for use for the Assembly, not personal or any other business.

7.9 Relationship with Departmental IT Policies:

Departments and Units within the Assembly may adopt additional information technology policies that are specific to their operations, provided that such requirements are consistent with this Policy and the unit provides a copy of more specific unit policies to management and the IT Steering Committee. In the event of inconsistency, the provisions of this Policy will prevail, unless the more specific policies are necessary to meet legal requirements governing certain types of information, in which case the more specific legal requirements and related policy will take precedence.

8. POLICY PRIORITY/FOCUS AREAS

8.1 ENGAGEMENT OF A DEDICATED AND TRAINED IT TEAM

This policy seeks to ensure a balanced team of officers with the requisite practical and professional knowledge to support the administration and information and technology advancement drive in the municipality. There shall be an IT Steering Committee in the Assembly, that shall be responsible for the planning and consultation on IT related activities and development in the best interest of Assembly, taking into consideration the current and the future needs of the Assembly.

Thus:

- a. Management shall engage a Steering Committee by appointment.
- b. Members to be appointment shall include;
 - i. The MIS Officer or the head of IT
 - ii. Other officers with the requisite IT knowledge
- c. Management shall facilitate at least an annual training for team members.
- d. Provide periodic motivation for the Steering Committee.

8.2 ACQUISITION AND ACCESS TO REQUISITE IT GADGETS, AND RELATED MATERIALS

This policy seeks to address the harmonization of task/function specific IT gadgets in terms of acquisition to one unique brand that is Durable, Efficient and Cost Effective with availability of its accessories for maintenance and servicing.

The MIS Officer or the Head of IT shall ensure that all work-related data are appropriately backed up to allow access to information or records when there is breakages or damages in an office.

8.2.1 HARDWARE

This policy provides guidelines for the purchase of hardware for the Assembly to ensure that all hardware technology for the Assembly is appropriate, provides value for money and where

applicable integrates with other technology for the Assembly. The objective of this policy is to ensure that there is minimum diversity of hardware within the Assembly.

- a. There shall be acquisition of Desktop Computers, Laptops, Printers, Networking Materials and other Internet Providing Gadget from a Credible and an authorized supplier.
- b. All IT gadgets and Related resources shall be procured or done in consultation with the IT department and the IT Steering Committee
- c. The IT department or an approved officer shall be responsible for setting up all IT related gadgets in every Office when assigned.
- d. The IT department shall see to it that all IT and related gadget are kept in the appropriate environment according to standards and best practice.
- e. The IT department shall take stock of all IT related gadgets and report on their state of condition every half year to the IT Steering Committee.
- f. The IT department will take inventory of all IT related gadget for all the offices and make a procurement plan for the acquisition of IT gadget needed for the future.

8.2.1.1 Purchasing Server Systems

- a. Server systems shall be purchased on the recommendation of the IT department
- b. Server systems purchased must be compatible with all other computer hardware in the Assembly.
- c. Any change from the above requirements must be authorized by IT departments and the IT Steering Committee

8.2.1.2 Purchasing Computer Peripherals

Computer system peripherals include printers, scanners, external hard drives etc.

- a. Computer peripherals shall only be purchased when they are not included in any hardware purchase or are considered to be an additional requirement to existing peripherals.
- b. Computer peripherals purchased must be compatible with all other computer hardware and software in the Assembly.

- c. Any change from the above requirements must be consented by the IT department or the Steering Committee

8.2.1.3 Purchasing Mobile Devices (Phones/Tablets)

A mobile phone may be purchased once the eligibility criteria is met.

- a. The purchase of a mobile devices must be from a Credible authorised supplier to ensure the Assembly takes advantage of volume pricing-based discounts provided by the Supplier.
- b. The mobile devices must be compatible with the Assembly current hardware and software systems.
- c. The mobile devices purchased must be from a CREDIBLE brand.
- d. The request for accessories (a hands-free kit etc.) must be included as part of the initial request for a mobile device.
- e. The purchase of a mobile device must be approved by the IT department or the Steering Committee prior to purchase.
- f. Any change from the above requirements must be consented by the IT department or the Steering Committee

8.2.2 SOFTWARE

This policy provides guidelines for the purchase of software for the Assembly to ensure that all software used by the Assembly is appropriate, provides value for money and where applicable integrates with other technology for the Assembly. This policy applies to software obtained as part of hardware bundle or pre-loaded software.

8.2.2.1 Acquisition of Software

All software, including commercial and non-commercial software such as open source, freeware, etc. must be approved by the IT department prior to the use or download of such software.

8.2.2.2 Commercial software

The purchase of all software must adhere to this policy.

- a. All purchasable software must be purchased in consultation with the Head of IT or the Steering Committee
- b. All purchasable software must be purchased from 'reputable software seller(s)'
- c. All purchasable of software must be compatible with the Assembly's server and/or hardware system.
- g. Any change from the above requirements must be consented by the IT department or the Steering Committee

8.2.2.3 Non-commercial or open source or freeware software

Open source or freeware software can be obtained without payment and usually downloaded directly from the internet.

- a. In the event that open source or freeware software is required, approval from {insert relevant job title here} must be obtained prior to the download or use of such software on the Assembly system(s)
- b. All open source or freeware must be compatible with the institution's hardware and software systems.
- c. Any change from the above requirements must be consented by the IT department or the Steering Committee

NB: All procured Hardware and Software must have a minimum of 2 to 3 years guarantee and warranty.

8.3 GUIDELINES FOR CUSTODY, USE AND MAINTENANCE OF IT GADGETS

8.3.1 USE OF IT GADGETS

- a. Golden rule, all IT and related gadgets must be used for the purpose of which it was given.
- b. Avoid putting persona password on IT gadgets under your care or seek for approval from the IT department for proper documentation of the password
- c. Avoid visiting unauthorized sites
- d. Avoid using all IT and related gadgets for personal gains that is not Assembly activities related
- e. Report on all lost, fault and damages of all IT and related gadgets under your care to the appropriate office (IT Department) for redress.
- f. Avoid given access or leaving any of the Assembly IT and related gadget in the hands of a third party.

8.3.2 MAINTENANCE AND SERVICING OF IT GADGET (HARDWARE)

- a. Management in consultation with the IT department shall procure the services of a qualified Technician to service and the maintain IT and related gadgets of the Assembly on regular basis.
- b. All IT and related Gadgets that are faulty or damaged must be reported to the IT department for redress.

8.4 NETWORK AND INTERNET ACCESS

8.4.1 GUIDELINES FOR USE OF INTERNET ACCESS PROVIDED BY THE ASSEMBLY

The internet use policy is intended to provide guidelines for the acceptable use of the internet, computers, and other forms of technology use, from the Assembly. The guidelines set in this policy are intended to provide examples of inappropriate behaviors that are prohibited in the Assembly. The acts outlined in this document are also intended to serve as a precedent for addressing related unacceptable behaviors concerning the use of the internet and other technology provided by Assembly.

8.4.1.1 Bullying, harassment, discrimination, and other hostile behavior

Staff of the Assembly are trusted to use Assembly property in a way that is respectful and appropriate. Assembly has zero tolerance for comments and actions that would be considered racist, sexist, derogatory, vulgar, threatening, harassing, or otherwise discriminatory. This includes but is not limited to actions and comments partaken when using the internet and other technology provided by the Assembly.

8.4.1.2 Personal use of the internet during work hours

Staffs are expected to use Assembly-provided internet and other devices as a resource for completing their assigned duties and supporting the objectives of Assembly. Excessive personal use of Assembly internet (“cyberloafing”) during work hours is not permitted, however occasional and reasonable personal use is acceptable, so long as:

- This use of the internet does not interfere with staff productivity, including the quality of work produced and other indicators of performance.
- The staff’s personal use of the internet does not violate any other guidelines contained within this document.
- Personal use does not cause undue effects to the Assembly network by consuming an excessive amount of the limited available bandwidth. Examples include but are not limited to downloading/uploading unreasonably large files and streaming videos.
- Staffs do not use Assembly property to perform commercial services outside of tasks and projects assigned by Assembly.

8.4.1.3 Piracy, data theft, hacking, and other illicit or unsafe activity

The following activities are strictly forbidden on Assembly equipment:

- Illegally downloading music, films, software, and other digital goods (“Piracy”)
- Installing software on Assembly computers without the authorization of a Assembly information technology (IT) representative
- Sharing confidential material, trade secrets, or other proprietary information outside of authorized parties of Assembly
- Gaining unauthorized access to programs, systems, websites, etc (“Hacking”)
- Introducing malicious software (“Malware”) onto the Assembly network or performing other actions that put the security of the organization at risk
- Attempting to bypass the Assembly web filter to access blocked material
- Accessing content that would reasonably be considered not safe for work such as pornography, violent imagery, and other adult-oriented content.
- Sharing or leaking passwords or other credentials that are used to provide access to Assembly equipment, services, accounts, and other Assembly assets.

8.4.2 GUIDELINES FOR USE OF NETWORK ACCESS PROVIDED BY THE ASSEMBLY

The Assembly depends upon its IT Network for administrative activities. It is essential that the stability, integrity and security of the IT network be safeguarded for use by all members of the Assembly.

The IT Network is the infrastructure which connects devices allowing the exchange of data to support the Assembly’s business and operations.

The management and oversight of the IT Network is the remit of IT Services under the management of the Head of IT in collaboration with the IT Steering Committee. The Assembly reserves the right to refuse connection for any non-standard device.

8.4.2.1 Scope

The scope of the policy covers all users and all equipment irrespective of ownership that is attached to network data points on the Assembly network or uses the Assembly operated wireless network.

For the purposes of clarification, this includes, but is not limited to desktop computers, laptops, servers, printers, tablets, Chromebooks, smart phones, reprographic and audio-visual devices, irrespective of ownership.

8.4.2.2 Operational Guidelines for use of Assembly Provided Physical Network

To maintain the integrity and protection of the Assembly's IT Network all equipment connected to the IT Network must comply with a set of minimum standards. Poorly configured, managed or operated equipment may lead to serious degradation of network operation or a breach in network and systems integrity resulting in: Disruption to business as usual processes, Disclosure of Assembly information, System or network compromise, etc.

Thus:

- a. Permission must be obtained from IT office before any non-standard device is connected to the network. This process is handled through the IT Service Desk.
- b. The Assembly may use an installed agent to control network access and ensure appropriate service packs and anti-virus programs are installed, up-to-date and running.
- c. The IT office in collaboration with the IT Steering Committee may employ measures to ensure compliance with this policy, e.g. remote audit and security penetration testing.
- d. For security and network maintenance purposes, authorised individuals within IT Office may monitor equipment, systems and network traffic at any time.
- e. All devices must use DHCP for IP configuration, with the exception of essential IT Infrastructure devices.
- f. New physical connections of equipment to a data port of the Assembly's network may only be made by the approved IT Officer. Under no circumstance should a user attach any device to a data port without a prior approval.

- g. Connected equipment must be maintained in accordance with manufacturers' recommendations. In particular, operating system and application software should be kept up-to-date to ensure that security vulnerabilities are not created. Systems must run up-to-date anti-malware software where available.
- h. Equipment must not be, or remain, connected to the network after a manufacturer ceases to provide security patches, without the prior approval of the Head of IT Services.
- i. Users must not attempt to circumvent any firewall or software designed to protect systems against harm.
- j. Unauthorised use of IP addresses or changing of a System MAC address is prohibited.

8.4.2.3 Operational Guidelines for use of Assembly Provided Wireless Network

- a. All wireless connections to the Assembly network must be individually authenticated, logged, and be trackable back to the user.
- b. All wireless access points which connect to the Assembly network must be owned by the Assembly and operated by the approved IT Officer. Users must not turn their device into an access point or an ad hoc network unless all devices on the ad-hoc network are isolated from the Assembly's network.
- c. Rogue wireless access points will be located, removed and disposed of by the approved IT Officer
- d. Personally owned Mobile Devices including any device not owned by the Assembly is only authorised to connect to the WLC_Open-Access wireless profile for Internet access only.

8.4.3 THE RIGHTS OF THE ASSEMBLY

8.4.3.1 Staff monitoring

The equipment used to access the internet is the property of the Assembly. IT Officer in collaboration with the IT Steering Committee may use an approved "user" monitoring software to ensure the acceptable use of information technology by staff, maintain the security of Assembly data and property, and assist with staff productivity tracking. This activity tracking

software may be used to monitor staff computer activity, including monitoring internet activity such as the websites visited by staffs.

8.4.3.2 Copyrights

All data created on Assembly computer systems is considered to be owned by the Assembly. Unauthorized disclosure of this data is not permitted and the Assembly reserves the right to disclose this data to authorized parties at its discretion.

8.5 CYBER RISK MITIGATION AND SECURITY

The Cyber Security Policy includes guidelines and provisions for security measures to help mitigate cyber risk. It applies to all staff, contractors, volunteers and anyone who has a permanent or temporal access to the Assembly systems and hardware. The ultimate goal is to help the Assembly to better manage IT-related cyber risks.

8.5.1 Confidential Data

Confidential data is valuable and is to be kept away from unauthorized persons. Assembly confidential data include

- Unpublished financial information
- Data of clients
- Patents or copyrights

All staff are obliged to keep this data safe

8.5.2 Protect personal and Assembly devices

When staff use their digital device to access Assembly emails or accounts, they introduce security risk to Assembly data.

Staff are to

- Keep all devices password protected
- Ensure all Assembly computers are installed with approved antivirus and regularly updated
- Do not leave device exposed or unattended to
- Install security updates of browsers and systems regularly or as soon as updates are available
- Log in to all Assembly Management System accounts through secure and/or private networks

To ensure an ongoing cyber risk mitigation, the MIS Officer shall

- Conduct Disk encryption setup for all Assembly computers
- Install approved Password management tool on all Assembly computers and
- Install an approved antivirus and malware software and regularly assess authentication systems on all Assembly machines
- The IT/MIS officer shall install a password management tool, which generates and stores password as may be required.
- Inform staff regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches in collaboration with the IT Steering Committee
- In collaboration with the IT Steering Committee issue relevant notices of alert

It is important that the MIS/IT officer is informed about scam or fraudulent attempts, breaches and malware, to ensure a proactive protection of the Assembly IT infrastructure.

All staff are thus, expected to promptly report perceived attacks, suspicious emails or phishing attempts MIS/IT officer who must investigate promptly, resolve the issue and issue a relevant notice to concerned users.

8.5.3 Safekeeping and Use of Emails

Emails can hosts scams and malicious software. To avoid virus infection or data theft, staff must

- Avoid opening attachments and clicking on links when the content is not adequately trusted
- Be suspicious of click baits and avoid them
- Check if email you receive are legitimate

- Look for inconsistencies or giveaways (eg. Grammar mistakes, capital letters, excessive exclamation marks)

If a staff is not sure about an email received is safe, they may refer to an IT Steering Committee member or the MIS Officer

8.5.4 Managing passwords

Password leaks can compromise the Assembly entire infrastructure. Passwords should always be secured and remain secret.

- Choose passwords with at least eight characters (including capital and lower-cases letters, numbers and symbols) and avoid individual information which can easily be guessed (e.g birthdays)
- Remember passwords instead of writing them down
- Exchange credentials only when necessary.
- Change passwords every two months.

8.5.5 Data Transfer

Transferring data from one source to another may introduce security risk.

Staff must:

- Avoid transferring sensitive data (e.g customer information, staff records) to other devices or accounts unless it is so approved. When mass transfer of such data is needed, staff are to request for approval from the designated team/officer
- Avoid sharing confidential data over unsecured network/system
- Ensure that the receivers of a shared data are authorized entities which have adequate security policy
- Reports scams, privacy breaches and hacking attempts as soon as suspected

8.5.6 Firewall

All parts of the Assembly network (i.e. all of the IP address space allocated) shall be protected by a centrally managed Assembly Firewall.

8.5.7 Additional Measures

To reduce the likelihood of security breaches, staff are instructed to:

- Turn off their screens and lock their devices when leaving the desks.
- Report stolen or damaged equipment as soon as possible to [IT Officer]
- Report to MIS to change all account passwords at once when a device is stolen
- Report a perceived threats or possible security weakness in Assembly system
- Avoid accessing suspicious websites
- Refrain from downloading suspicious, unauthorized or illegal software on the Assembly equipment

8.6 INFORMATION TECHNOLOGY CAPACITY BUILDING FOR ALL STAFF

To ensure sustainable use of information technology in the Assembly, it is crucial that all levels of staff are trained to handle, secure, operate, and store all tools and gadgets appropriately.

Broad training and development initiatives shall include:

- Specific Content - Competency Development training for head of units/departments as well as officers of direct responsibility on relevant software packages Eg. Microsoft (Office, Excel, Powerpoint), ArcGIS, CAD, SPSS, KoboCollect, etc.
- Developing a pool of Certified Information Technology Trainers of the Assembly who may facilitate the training of other staff
- General handling, storage, installation and maintenance trainings for relevant staff on available IT tools and gadgets with special attention for cleaners and other office support workers
- Training of all staff on cyber security

- Training of all staff on the IT policy of the Assembly

These shall be achieved through:

- Development of online/virtual smart training portals on web and/or social media for relevant IT equipment or required competency for all staff by the Assembly
- Conduct and/or sponsorship of staff for relevant IT programmes/courses workshops, seminars or summits by the Assembly
- Promotion of IT Training opportunities/avenues for all staff by the Assembly
- Facilitating inter-organizational or cross-district Information Technology Learning Platforms for relevant staff by the Assembly

8.7 IMPLEMENTATION OF A PROGRESSIVE PAPERLESS SYSTEM

The main reason ICTs are used in the workplace is that they allow humans to do their work faster, more efficiently and with fewer wasted resources. This policy seeks to address the Assembly overt dependence on paper, which has a serious negative environmental impact. Not only is the dependence on paper bad for the environment, this reliance also makes it hard to track down specific documents when you need to access them most. In addition, the Assembly security and compliance efforts are challenged by the need to store information in a safe, organized, and legally responsible way.

By this policy, the Assembly is leveraging on technology to make paperless office possible, and the use of technologies for visitor records management, e-signatures, digitized registry system, virtual official internal communication systems (digitized memo management softwares), team collaboration, and external communications to make it a reality.

8.7.1 Take a stand

Management is to make paperless office policy official and practical by providing by communicating key benchmarks and maximum/minimum goals.

These may include:

- a. A ceiling on the volume of paper used monthly for each department/unit.
- b. Progressive limitations for paper printing and other paper issuance.
- c. Use of central or networked printing pools for applicable departments and units.
- d. Institution of awards for paperless champion(s) in the Assembly to create momentum and boost results.

NB: The stores officer or the officer responsible for the issuing papers may document the progress being made and add a personal element to the paperless course.

8.7.2 Leveraging on Technology (Social Media Platforms)

The Assembly should leverage on social media and create platforms for committees and sub committees of the Assembly to distribute common letters meant for the committee members to avoid printing of individual letters. Further, individual letter should also be shared using the person individual social media platform or mails.

8.7.3 Digitization of Client and Records Department

The Assembly shall either procure an electronic filing software or train officers to use other conventional available software to digitize and improve the filling process of the Records and the Client Service Unit.

The IT department shall engage or support other departments to come up with proper and applicable formats using available software to operationalize the digitization of the department's activities.

8.7.4 Reducing Printing

The Assembly should place less emphasis on office printers and promote the use of easily shareable file formats like Portable Document Formats (PDFs), digital signature software, internal communication technology tools, and electronic record filing all of which make it easier to rely less on paper.

8.8 PUBLIC INFORMATION MANAGEMENT

The Public Information Management Policy provides the strategic direction and route for creating, capturing and managing information assets (records, information and data) that is channeled through Information technological means to satisfy business, legal and stakeholder requirements. This is to ensure that information channeled through information technological means comply with relevant cyber security, confidentiality/privacy and other regulations.

- a. The IT Steering Committee shall be responsible for Public Information channeled through IT systems for the Assembly.
- b. Each department or decentralized department/unit shall volunteer an officer who shall liaise with the committee for giving and picking of public information.
- c. The Steering Committee shall record and authenticate all information and seek approval from management before publishing the relevant public information.
- d. The Steering Committee shall disseminate information to various stakeholders as soon as possible and needed/required.

8.9 CREATING ENABLING ENVIRONMENT AND IT PROMOTION

In order to assure the achievement of the promise of economic and social development through information technology, it is critical that the Assembly adopt enabling legal and regulatory environments that support e-development.

“Enabling environment” means policy, legal, market, and social considerations that interact both at domestic and global levels to create fertile conditions for IT-led growth.

Ghana’s physical, information technology infrastructure is currently under-underdeveloped and limited in coverage. It is acknowledged that special policy measures and initiatives will need to be aimed at developing the communications infrastructure to improve universal access and service. This policy measures is directed at facilitating the necessary legal, regulatory and institutional enabling environment for the development of the telecommunications and

communications infrastructure to improve the coverage of the network and its services to support the activities of various sectors, and in particular the information technology economy.

The Assembly shall:

- a. Promote and facilitate initiatives targeted at the development of a reliable, fast adaptive and robust infrastructure for Information technology development that will improve access and quality of service
- b. To promote competition in the communications industry to increase customer choice and promote the provision of affordable services
- c. Promote the development, and deployment of basic and broadband and multi-platform communications infrastructure to facilitate public access to information and services
- d. Provide support for the development of human resources through various forms of capacity development at all levels with emphasis on the youth
- e. Support the IT Unit of the Assembly to undertake outreach programmes to promote career paths in Information technology.

9. DISCIPLINARY ACTION

This policy document and its principles shall be binding on all members, staff and stakeholders of the Assembly. Violation of this policy could result in various forms of disciplinary action. Staffs may also be held liable for damages caused by any violations of this policy. The Assembly reserves the right to audit compliance with the policy from time to time.

All staff are to always follow this policy, and those who cause security breaches may face disciplinary action.

Where a user is aware of a breach of the use of software in accordance with this policy, they are obliged to notify IT Steering Committee immediately. In the event that the breach is not reported and it is determined that a user failed to report the breach, then that user shall be deemed as aiding and abetting the breach.

The Steering Committee may recommend to management for actions to be taken on persons who breach this policy.

- First time, unintentional, small scale security breach: the Assembly may issue a verbal warning and train the staff on security
- Intentional, repeated or large-scale breaches (which cause severe financial or other damage); the Assembly will invoke more severe disciplinary action.
- Each incident shall be examined on a case by case study
- Staff who are observed to disregard the Assembly IT policy will face progressive discipline even if their behavior has not resulted in a security breach

10.COMMENTS, QUESTIONS, OR CONCERNS

If a staff, member or stakeholder is uncertain about what is considered acceptable or unacceptable use of the any related information technology or they have any other questions and concerns, they shall contact the IT Steering Committee through the Coordinating Director of the Assembly for further clarification.

11.AMENDMENTS

The terms of this policy are subject to change at the discretion of Assembly. Staffs will be notified of amendments. Staffs will be required to provide a signed acknowledgement of their receipt and acceptance of the revised policy.