MINISTRY OF GENDER, CHILDREN AND SOCIAL PROTECTION

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

JULY 2025

MINISTRY OF GENDER, CHILDREN AND SOCIAL PROTECTION

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) POLICY

JULY 2025

VERSION 1.0

This Policy was developed by the Ministry of Gender, Children and Social Protection to regulate the usage of Information Communication Technology (ICT) within the Ministry.

For copy, review and comment of the *MoGCSP ICT Policy* please contact
the Research Statistics and Information Management Directorate,
Ministry of Gender, Children and Social Protection
P.O BOX MBO 186, Ministries. Accra, Ghana.
Tel +233 302688181
Website: www.mogcsp.gov.gh

FOREWORD

In an era where technology plays an increasingly pivotal role in enhancing service delivery and fostering communication, the Ministry of Gender, Children, and Social Protection (MoGCSP) recognizes the importance of a robust Information and Communication Technology (ICT) Policy. This policy is designed to guide our staff in the responsible and effective use of technology as we strive to promote gender equality, protect children's rights, and empower vulnerable groups in Ghana.

The MoGCSP's ICT Policy is not just a set of rules; it is a framework that embodies our commitment to transparency, accountability, and innovation. By establishing clear guidelines and standards for the use of ICT resources, we aim to ensure that our technological infrastructure supports our strategic objectives and enhances our ability to serve the public effectively. By implementing this ICT policy, the MoGCSP also aims to streamline processes, improve data management, and facilitate better collaboration among various stakeholders. This initiative not only enhances operational efficiency but also ensures that the ministry's programs are more accessible and impactful for the communities we serve.

This policy reflects our dedication to maintaining a secure digital environment while facilitating collaboration and knowledge sharing among our staff, stakeholders, and the constituents we serve. It emphasizes the importance of compliance with legal frameworks and ethical standards, ensuring that we uphold the rights of individuals and protect sensitive information.

As we implement this ICT Policy, I encourage all employees and stakeholders to embrace the Opportunities that technology offers, while adhering to the guidelines set forth. Together, we can harness the power of ICT to drive positive change and achieve our mission of sustainable national development.

HONOURABLE DR. AGNES NAA MOMO LARTEY
MINISTER
MINISTRY OF GENDER, CHILDREN AND SOCIAL PROTECTION

ACKNOWLEDGEMENT

The Ministry of Gender, Children, and Social Protection (MoGCSP) is pleased to announce the successful formulation of its ICT Policy, a significant milestone made possible through the collaborative efforts of numerous individuals. We extend our heartfelt gratitude to everyone who contributed their knowledge, time, and dedication to this important project.

We would like to specifically acknowledge the Director of the Research, Statistics, and Information Management Directorate (RSIMD) and the entire RSIMD team for their exemplary leadership, guidance, and technical expertise throughout the development of this policy. Their proficiency in statistical methodologies and commitment to ensuring the accuracy and reliability of our data have been instrumental in shaping the ICT Policy.

We also express our sincere appreciation to the Ghana Statistical Service (GSS) Team, whose insights, unique perspectives, and support through the Harmonizing and Improving Statistics in West Africa (HISWA) project have greatly enriched the content of the policy. Their collaborative spirit and commitment to aligning our practices with the best global standards have been vital to the integrity of our ICT Policy.

Furthermore, we value the constructive feedback and contributions from a diverse range of internal and external stakeholders, which have been essential in refining and enhancing the policy. Their insights and perspectives have ensured that the ICT Policy is comprehensive, up-to-date, and reflective of the objectives and values of the MoGCSP.

DR. AFISAH ZAKARIAH

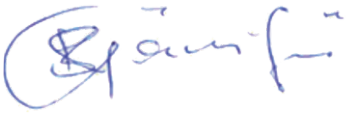
CHIEF DIRECTOR

MINISTRY OF GENDER, CHILDREN, AND SOCIAL PROTECTION

EXECUTIVE SUMMARY

The Ministry of Gender, Children and Social Protection (MoGCSP) has developed this Information and Communications Technology (ICT) Policy to provide a comprehensive framework for the responsible, secure, and effective management of technology resources across the Ministry. Recognizing ICT as a critical enabler for achieving the Ministry's mandate of promoting gender equality, protecting children's rights, and empowering vulnerable populations in Ghana, this policy establishes clear guidelines and standards for ICT governance, asset management, systems administration, communication, data protection, and security. The policy applies to all employees, departments, agencies, and authorized third parties who utilize the Ministry's IT infrastructure and aligns with key national legislation including the Ghana ICT4AD Policy, Cybersecurity Act 2020, Data Protection Act 2012, and NITA standards.

The policy aims to enhance effective budgeting and equitable distribution of IT resources, improve service delivery, protect information assets and IT infrastructure, and build institutional capacity in support of the Government of Ghana's digitalization agenda. It covers eight major areas: IT Governance, IT Asset Management, Systems Administration, IT Communication, Data Protection, Security, and Capacity Building. The policy incorporates gender-sensitive provisions throughout, ensuring equal access to technology, protecting against digital gender-based violence, and promoting inclusive ICT training. Compliance will be monitored through regular audits by the Internal Audit Unit in collaboration with the IT Unit, with violations subject to disciplinary actions. The policy will be reviewed every three years to ensure MoGCSP continues to leverage technology effectively in fulfilling its mission while maintaining security, transparency, and accountability.



DR. SYLVESTER KYEI-GYAMFI

DIRECTOR, RSIM

MINISTRY OF GENDER, CHILDREN, AND SOCIAL PROTECTION

ACRONYMS

Bcc	-	Blind Carbon Copy
Cc	-	Carbon Copy
eGIF	-	Electronic Government Interoperability Framework
HISWA	-	Harmonizing and Improving Statistics in West Africa
HTML	-	Hyper Text Markup Language
HTTP	-	Hyper Text Transmission Protocol
IMAP	-	Internet Message Access Protocol
ISDN	-	Integrated Services Digital Network
IT	-	Information Technology
MoGCSP	-	Ministry of Gender, Children and Social Protection
NITA	-	National Information Technology Agency
PABX	-	Private automatic branch exchange
POP3	-	Post Office Protocol Version 3
PSTN	-	Public Switched Telephone Network
RA	-	Risk Assessment
RSIMD	-	Research Statistics and Information Management Directorate
RTF	-	Rich Text Format
VPN	-	Virtual Private Network

Table of Contents

FOREWORD.....I

ACKNOWLEDGMENT.....II

EXECUTIVE SUMMARY.....III

ACRONYMS.....IV

1.0. INTRODUCTION.....1

2.0. RATIONALE.....1

3.0. MINISTRY PROFILE.....2

3.1. Vision.....2

3.2. Mission.....2

4.0. POLICY OBJECTIVES.....2

5.0. POLICY SCOPE.....3

6.0. POLICY USAGE.....4

7.0. LEGAL FRAMEWORK.....4

8.0. IT/ IS STRATEGY.....6

9.0. INFORMATION TECHNOLOGY (IT) GOVERNANCE.....7

10.0. INFORMATION TECHNOLOGY (IT) ASSET MANAGEMENT.....7

10.1. Management of IT Assets.....7

10.2. Hardware.....8

10.2.1. IT Equipment.....8

10.2.2. Lost or Stolen Equipment.....8

10.2.3. Maintenance of IT Equipment.....8

10.2.4. Procurement of IT Equipment.....9

10.2.5. Removal of IT Equipment.....9

10.2.6. Handling of IT Equipment.....9

10.2.7. Portable Devices.....9

10.2.8. Assignment and Distribution of IT Equipment.....11

10.2.9. Disposal/ Replacement/ Redistribution of IT Equipment.....11

10.3.1. Acceptable use.....11

Table of Contents

10.3.2. Software Standards.....11
10.3.3. Purchasing.....11
10.3.4. Licensing.....12
10.3.5. Installation.....12
10.3.6. Software Documentation.....13
10.3.7. Support.....14
10.3.8. Software Request.....14
10.3.9. Software Usage.....14
11.0. SYSTEMS ADMINISTRATION.....15
11.1. Logical Access Controls.....15
11.1.1. Authorization.....15
11.1.2. Monitoring.....15
11.1.3. Reporting Security Issues.....16
11.1.4. User Registration.....16
11.1.5. User De-registration.....16
11.1.6. Password Management.....17
11.1.7. Remote Access/ Third Party Connections.....17
11.2.2. Guiding Principles-Privileged Accounts.....19
11.2.3. Guiding Principles-Shared User Accounts.....19
11.2.4. Vendor or Default User Account.....20
11.2.5. Test Accounts.....20
11.2.6. Contractors and Vendors.....20
12.0. IT COMMUNICATION.....21
12.1. Internet.....21
12.2. Virtual Private Network (VPN).....21
12.3. Privileged User Accounts.....22
12.4. Electronic Messaging.....22
12.5. Prohibited Actions.....23
12.6. E-mail Disclaimer.....24
12.7. Email Addressing.....24
12.8. Expiration and Deletion of Account.....25
12.9. Reactivation of Designation Email Account.....25
12.10.Attachment to e-mail messages.....25
12.11.Default e-mail messages set up.....25

Table of Contents

12.12.Carbon Copying/ Blind Carbon Copying.....25
12.13.Privacy.....26
12.14.Data Retention/ Deletion.....26
12.15.Data Backup.....26
12.16.Message Monitoring.....26
12.17.Incidental Disclosure.....26
12.18.Voice over IP (VOIP).....26
12.19.Social Media Use.....26
12.19.1. Authorised Users of MoGCSP Official Social Media Accounts.....27
12.20.MoGCSP Website.....28
12.21.Bulk SMS.....28
12.22.Video Conferencing.....28
13.0. DATA PROTECTION.....28
13.1.2. Document Creation/ Authoring/ Collection.....29
13.1.3. Document Review and Approval.....29
13.1.4. Document Release.....29
13.1.5. Document Storage/ Protection/ Organisation.....29
13.1.6. Principles of Data Protection.....29
13.1.7. Document Expiration/ Disposal/ Archival.....30
13.1.8. Cataloguing Policy.....30
13.1.9. Information Sensitivity.....30
13.1.10. Storage.....31
14.0. SECURITY.....31
14.1. Anti-Virus.....31
14.2. Incidents.....31
14.3. Firewall.....31
14.3.1. Intrusion Prevention System.....31
14.3.2. Packet Filtering.....31
14.3.3. Stateful Inspection.....31
14.3.4. Application Filtering.....32
14.4. Software Security.....32

Table of Contents

14.5. Security for Server Room – Environmental Control.....32
14.6. Security for Server Room – Power.....32
14.7. Security for Server Room – Fire.....32
14.8. Close Circuit Television (CCTV).....32
14.9. System Monitoring.....34
14.10.Change Management..... 34
14.11.Database Security.....34
14.11.1. Storage and Retrieval.....34
14.11.2. Vendor Policy.....35
14.12.Network and Internet Security.....35
14.13.Risk Assessment.....35
14.14.Risk Assessment Process.....36
14.15.Backup.....36
14.16.Recovery.....36
14.16.1. Disaster recovery planning goals:.....37
14.16.2. Distribution.....37
14.16.3. Integration.....37
14.16.4. Activation Criteria.....37
14.16.5. Activation Procedures.....38
14.16.6. Disaster Recovery Procedures.....38
14.16.6.1. Communications Procedures.....38
14.16.6.2. Remote Access Procedures.....38
14.16.6.3. Backup and Data Recovery Procedures.....38
14.17.Helpdesk.....38
15.0. CAPACITY BUILDING AND UTILISATION.....39
16.0. COMPLIANCE/ ENFORCEMENT.....39
17.0. VIOLATION.....40
17.1. Penalties.....40
18.0. MONITORING AND EVALUATION.....40
19.0. DISCLAIMER.....41
20.0. AMENDMENT OR REVISION OF POLICY DOCUMENT.....41
21.0. APPENDIX.....43
13.1. Glossary.....43
22.0. REFERENCES.....49

1.0. INTRODUCTION

The Ministry of Gender, Children and Social Protection (MoGCSP) was created by an Executive Instrument 1 (E.I. 1) in January 2013 as a successor to the Ministry of Women and Children's Affairs, currently guided by E.I. 1 2025. The primary objective for its establishment was to have a Ministry responsible for policy formulation, coordination and monitoring and evaluation of Gender, Children and Social Protection issues within the context of the national development agenda.

This will lead to the achievement of gender equality, equity, the empowerment of women and girls, promoting the survival and development of children, thus ensuring their rights. It will also ensure harmonizing social protection interventions to better target the vulnerable, excluded and persons with disability and integrate fulfilment of their rights, empowerment and full participation into national development.

2.0. RATIONALE

Information Communication Technology (ICT) is an essential tool that underpins the effective implementation of programs and interventions at the Ministry of Gender, Children, and Social Protection (MoGCSP). In the context of modern governance, ICT plays a critical role in improving efficiency, transparency, and responsiveness in public administration. For the MoGCSP, which is mandated with promoting gender equality, advancing the welfare of children, and empowering vulnerable groups, ICT facilitates the seamless coordination of its various activities across various sectors, departments, regions, among varied stakeholders. The Ministry also acknowledges the issues of digital gender divide and is committed to ensuring that, ICT deployment and training efforts encourage equal access, use and benefits for all staff, regardless of gender, disability, or other status.

Given the increasing complexity and scope of the Ministry's programs, there has been a substantial rise in the dependency on ICT systems to support day-to-day operations. From case management systems for vulnerable populations to data-driven policy decisions, ICT is central to the success of MoGCSP's mandate. Reliable IT infrastructure ensures that programs such as the Livelihood Empowerment Against Poverty (LEAP), the Ghana National Household Registry (GNHR), and other interventions can be effectively managed, tracked, and evaluated in real time.

Therefore, it is crucial for the Ministry to have a robust, secure, and continuously operational ICT system to ensure the smooth execution of business processes. Without such systems, delays in service delivery, data management inefficiencies, and the risk of cyber vulnerabilities could compromise the Ministry's ability to meet its objectives.

In response to these needs, the Ministry has developed the Information and Communications Technology (ICT) Policy. This policy provides a framework for standardizing and enhancing ICT operations across the Ministry, ensuring that technology is not only aligned with the Ministry's strategic goals but is also resilient, scalable, and capable of supporting long-term growth and sustainability. The ICT Policy is essential for guiding investments in digital infrastructure, ensuring data protection and privacy, improving service delivery, and optimizing resource use in the pursuit of the Ministry's mandate.

3.0. MINISTRY PROFILE

3.1. Vision

The vision of MoGCSP, “A harmonious society in which the survival and development of the sexes, children, the vulnerable, and persons with disability are guaranteed”. The vision of the Ministry is guided by the following values: integrity, Excellence and Social Justice.

3.2. Mission

MoGCSP exists to contribute to the development of the nation by achieving gender equality and equity, facilitate the enforcement of the rights of children, promote the integration and protection of the vulnerable, excluded and persons with disabilities in the development process through appropriate policies and strategies with adequate resources.

4.0. POLICY OBJECTIVES

The broad objective of the policy is to promote a governance framework for a secure ICT enabled social development environment in line with government of Ghana digitalisation agenda

The specific objectives of the IT Policy are to:

a. Enhance effective budgeting and allocation of IT resources.
b. Promote and encourage even distribution of the requisite IT resources among all the Directorates and Departments.
c. Improve internal efficiency and quality service delivery within MoGCSP.

a. Protect the Ministry's information and IT infrastructure.

b. Regulate the development and deployment of IT systems of the Ministry

c. Guide the purchase, usage, maintenance, and disposal of IT hardware and software in line with current trends in enterprise solutions at large.

d. Protect data rights and privacy of employees of the Ministry.

e. Provide effective guidelines to ensure the smooth running of the MoGCSP's IT systems.

f. Provide guidelines for Integrating IT systems of the various departments and agencies of the Ministry.

g. Improve human resource and institutional management capacity in IT.

h. Protect the data integrity of the Ministry.

5.0. POLICY SCOPE

The policy covers the following broad areas.

1. **IT Governance:** This section outlines the governance framework for the management of IT resources within the Ministry. It includes decision-making structures, roles, and responsibilities to ensure that IT operations align with the Ministry's objectives and comply with regulatory requirements.

2. **IT/IS Strategy:** This section defines the strategic direction for the Ministry's IT and Information Systems (IS), ensuring alignment with the Ministry's overall goals and objectives. It includes long-term plans for adopting and integrating technology to improve service delivery, enhance operational efficiency, and support the Ministry's mandate.

3. **IT Asset Management:** This section addresses the life cycle management of IT assets, from user requests for asset acquisition to the final disposal of obsolete or redundant IT equipment. It ensures proper documentation, tracking, and maintenance of all IT assets to optimize their usage and minimize waste.

4. **Systems Administration:** This section covers the technical management of key IT systems such as applications, networks, and internet services. It ensures that the Ministry's IT infrastructure is securely and efficiently managed by the IT Unit of RSIM or through collaborative arrangements with external service providers.

4. **IT Communication:** This area governs the management of communication systems, including email, internet access, and internal messaging platforms. It ensures the proper usage of communication technologies to facilitate collaboration, information sharing, and outreach.

5. **Capacity Building and Utilization:** This section emphasizes the Ministry's commitment to IT capacity building, ensuring that staff have the necessary skills and training to utilize IT systems effectively. It outlines programs and initiatives aimed at building IT literacy and developing specialized expertise among staff.

7. **Data Protection:** This section focuses on safeguarding the confidentiality, integrity, and availability of data managed by the Ministry. It ensures compliance with data protection regulations and establishes protocols for handling, storing, and processing sensitive information.

8. **Security:** This section provides guidelines for securing the Ministry's IT systems, networks, and data against unauthorized access, cyber threats, and other security risks. It outlines the measures to be taken to protect the Ministry's digital assets, including the implementation of firewalls, encryption, and regular security audits.

6.0. POLICY USAGE

The IT Policy applies to all employees of the Ministry of Gender, Children, and Social Protection (MoGCSP) and its associated agencies, directorates, and departments who utilize the Ministry's IT peripherals and resources. Additionally, the principles of this policy extend to non-employees, including consultants, third-party firms, contractors, and visitors who access the Ministry's IT systems.

7.0. LEGAL FRAMEWORK

Ghana ICT for Accelerated Development (ICT4AD) Policy: for the realization of the vision to transform Ghana into an Information-rich knowledge-based society and economy through the development, deployment, and exploitation of ICTs within the economy and society.

Ghana National Cyber Security Policy & Strategy: establishing institutional frameworks, creating awareness, ensuring coordination of cyber security initiatives, and enforcement of cyber standards in Ghana.

Cybersecurity Act 2020 (Act 1038): to establish the Cyber Security Authority; to regulate cybersecurity activities in the country; to promote the development of cybersecurity in the country, and to provide for related matters.

Electronics Transaction Act 2008 (Act 772): Section 56, 60, Identification of Critical Electronic Records and Databases and Restrictions on Disclosure of Information.

Data Protection Act 2012 (Act 843): to establish a Data Protection Commission**,** to protect the privacy of individuals and personal data by regulating the processing of personal information, to provide a process to obtain, hold, use, or disclose personal information.

National Information Technology Agency (NITA) policy documents:

1. **Systems-and-Applications-Standards:** This document "applies to the acquisition, supply, development, operation, maintenance, and disposal (whether performed internally or externally to the MDA) of software systems, products and services, and the software portion of any system. Software includes the software portion of firmware."
2. **Management-of-IT-Infrastructure-MDAs-and-MMDAs**:
   The main objective of this document is to provide best practice guidelines for use in the operation, usage, management, maintenance, and repair of IT equipment in MDAs/ MMDAs."
3. **Local Area Network (LAN) Standards:** This standard provides mandatory requirements, recommended best practices, background information, and guidance to assist with the implementation of the ICT cabling infrastructure across the different Government Institutions.
4. **Electronic-Records-and-Data-Management-Standards:** For effective management of reliable records in digital format, among the critical success factors is the implementation of proper business information systems.

5. **Data-Centre-Standards:** A large group of networked computer servers typically used by organisations for the remote storage, processing, or distribution of large amounts of data.

The MoGCSP IT facilities provide tools for the effective and efficient execution of work. Users of MoGCSP 's IT facilities are required to comply with the tenets of the policy to protect the integrity and use of the infrastructure.

Users consent to abide by all applicable Ghanaian laws and to abstain from any actions that could expose the MoGCSP to legal risk.

To protect the integrity of MoGCSP 's IT facilities and its users against unauthorized or improper use:

a. MoGCSP has the right to investigate use of the facilities in violation of the MoGCSP 's rules and policy.
b. MoGCSP reserves the right, without notice, to limit or restrict any individual's use, and to inspect, copy, remove, or otherwise alter any data, file, or system resource which may undermine authorised use, or which violates the MoGCSP 's rules or policy.
c. IT Unit also reserves the right to periodically examine any system and usage as well as authorisation history as a necessary step to protect the infrastructure.

MoGCSP reserves the right to amend this policy to bring it into compliance with the applicable laws of Ghana.

8.0. IT/ IS STRATEGY

The IT/IS strategy ensures that there a linkage between the use of IT/IS to enhance internal processes and also deliver effectively on MoGCSP annual action plan, Medium- and Long-Term Development goals and Policy Documents and International Obligations.

The Directorate, Departments, Agencies planning or implementing a project, policy, strategy documents should contact IT Unit to align the planning or implementation with technology (required hardware or devices) and information systems.

IT Unit must develop and maintain the technology and information systems required for the implementation of all projects, policy, and strategy documents.

IT Unit must maintain a database, analyse data and submit report that supports the progressive implementation of MoGCSP annual action plan, Medium- and Long-Term Development goals and Policy Documents and International Obligations.

9.0. INFORMATION TECHNOLOGY (IT) GOVERNANCE

The Ministry of Gender, Children, and Social Protection (MoGCSP) shall establish a clear IT governance framework to ensure ICT initiatives align with its strategic objectives.

1. ICT Reporting: The ICT function will report directly to the Director of Research, Statistics, and Information Management Directorate (RSIM/D), aligning IT with data and information management.
2. IT Steering Committee: Tasked with defining IT missions and overseeing the development of ICT services, ensuring they support the Ministry's objectives.
3. ICT Organizational Structure: An appropriate structure, based on the Ministry's Organizational Manual and approved by the Office of the Head of Civil Service (OHCS), will ensure the ICT function is adequately staffed and aligned with business goals.

10. INFORMATION TECHNOLOGY (IT) ASSET MANAGEMENT

The Research Statistics and Information Management (RSIM)/IT Unit shall lead the Ministry to align Information Technology and Information Systems to the Ministry Sector medium-term goals, policies, international obligations and others.

An IT asset is anything, tangible or intangible, that can be used by the Ministry to create, produce and/or offer its services. IT asset includes information system infrastructure, network infrastructure, data repositories, IT equipment.

10.1 Management of IT Assets

The IT Unit is responsible for the proper management of MoGCSP IT Assets: Information Systems, Data Repositories, etc.

- Where the IT Assets is managed by consultant(s) IT Unit would work together with the consultant(s) to manage asset.
- The IT Unit would have Administrator access to all Information Systems and its Infrastructure, IT equipment etc.
- All staff - permanent or temporary (consultants, service persons, and relevant stakeholders) who register an account on behalf of the Ministry or for the Ministry shall not use their personal emails or phone numbers.

10.2. Hardware

10.2.1. IT Equipment

- Only authorised persons shall be allowed to use MoGCSP IT equipment, both on and off MoGCSP premises.
- All users of MoGCSP IT equipment shall ensure the protection of equipment in their possession or under their control against accidental, negligent or deliberate damage or theft.
- The RSIM shall develop and disseminate standard procedures on usage of IT equipment to all users.
- The IT Unit along with the Estate and Internal Audit Unit shall regularly maintain an updated inventory of all IT equipment detailing among others their location, allocation, re-allocation, cost, expected lifespan.

10.2.2. Lost or Stolen Equipment

- Users shall report the details of all lost or stolen equipment in an Incident Report Form and submit to his/her Head of Directorate which would be forwarded to the Head of RSIM and/or Head of General Administration.
- The Head of RSIM and/or Head of General Administration will forward an official complaint to the Chief Director for further action.

10.2.3. Maintenance of IT Equipment

- The General Administration Directorate / Estate Unit in collaboration with IT Unit shall be responsible for the maintenance of all MoGCSP IT Equipment.

- It is prohibited for MoGCSP I.T equipment to be taken by the user to a third party for repairs or maintenance.
- It is prohibited for MoGCSP equipment to be maintained or repaired by a third party who is not a licensed service provider.
- IT Unit and users shall not place IT equipment in areas susceptible to water seepage, dust, sunlight, high humidity and temperature, and salinity.

10.2.4. Procurement of IT Equipment

All Units undertaking procurement are to liaise with the RSIM/IT and act on advice for the procurement of all MoGCSP IT Equipment.

10.2.5. Removal of IT Equipment

- Removal of any IT equipment other than portable devices from its normal place of use must be authorised by the IT Unit and logged in the Equipment Movement Logbook prior to removal by IT Unit.
- Details should include equipment specifications, name of user or where the equipment is being moved from and to, why it is being moved and the date of removal and replacement.

10.2.6. Handling of IT Equipment

- Users shall always exercise good judgement and safeguard the equipment.
- Users shall report damage to IT equipment in an incident report form and submit to his/ her Head of Directorate which would be forwarded to the Head of RSIM and or the Head of General Administration.
- The Head of RSIM and or Head of General Administration will forward an official complaint to the Chief Director for further action.

10.2.7. Portable Devices

- The IT Unit shall regulate the use of Portable Digital Devices within MoGCSP network.
- The ministry defines acceptable business use as activities that directly or indirectly support the mission, vision and core mandate of MoGCSP.

- The use of personal devices during working hours should be limited and must not affect the discharge of official duties.
- The following defines the boundaries for the acceptable use of personal devices connected to MoGCSP's network.
    .1. Employees are blocked from accessing certain websites during work hours while connected to the corporate network. The websites blocked is at the discretion of the Ministry.
    .2. Devices may not be used to store or transmit illegal unethical materials.
- Personal devices must not be the sole repositories of any of MoGCSP's information. All business information stored on personal devices should be backed up on Ministry approved official devices and online repositories.
- The following are guidelines to ensure that the uses of personally owned devices are compliant with the Ministry's security standards:
    .1. To prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the Ministry network.
    .2. Passwords must be according to the Ministry's password policy.
    .3. Rooted (Android), jailbroken (iOS) or cracked devices are strictly forbidden from accessing the network.
- The following are guidelines to ensure that the use of personally owned devices is compliant with the Ministry's security standards
    .1. The Ministry reserves the right to disconnect devices or disable services without notification.
    .2. The employee is expected to always use his or her device in an ethical manner and adhere to the Ministry's policies.
    .3. The employee assumes full liability for risks including, but not limited to, the partial or complete loss of Ministry and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
    .4. The Ministry reserves the right to take appropriate disciplinary action for noncompliance with this policy.

10.2.8. Assignment and Distribution of IT Equipment

- The General Administration Directorate shall be solely responsible for the assignment/ distribution of IT facilities considering gender balance/ equity to ensure the specific needs of both female and male officers. All IT equipment is to be embossed before assigned to officers.
- The RSIM/IT Unit shall provide, advise, setup, and support for the distribution of IT facilities.

10.2.9. Disposal/ Replacement/ Redistribution of IT Equipment

- IT Unit will recommend or advise for renewal/replacement of IT facilities when the need arises.
- IT Unit shall ensure the security processing of equipment prior to it being disposed by the Stores Unit.
- IT Unit shall ensure that data files are backed up and deleted prior to redistribution when applicable.

10.3. Software

10.3.1. Acceptable use

The parameters for what constitute "acceptable use" of MoGCSP's software resources are set forth here. Only documents related to the Ministry may be created, researched, and processed using software that MoGCSP has acquired and distributed. You accept personal responsibility for their appropriate usage and this policy by using the MoGCSP's software systems.

10.3.2. Software Standards

- MoGCSP's IT section of the Ministry must ensure that software's procured and deployed meet the standards highlighted in NITA's Regulatory Documents for Application and e-Government Interoperability Framework.
- The software to be procured must have the appropriate hardware in place before it is purchased.

10.3.3. Purchasing

- Purchasing of MoGCSP software shall be done by the Procurement Directorate with specification provided by the IT Unit, to ensure that all applications conform to corporate software standards and are purchased at the best possible price.

- A member of the NITA procurement team may sit on the MoGCSP's Entity Tender Committee for enterprise solutions or software purchase. Note: The best price possible may not necessarily be the cheapest.
- All purchases for software must be in line with the MoGCSP's purchasing procedure and policy.

10.3.4. Licensing

- Each employee is individually responsible for reading, understanding, and following all applicable licenses, notices, contracts, and agreements for software that he or she uses or seeks to use on MoGCSP's devices.
- Unless otherwise provided in the applicable license, notice, contract, or agreement, any duplication of copyrighted software, except for backup and archival purposes, is a violation of state law. In addition to violating such laws, unauthorised duplication of software is a violation of the MoGCSP's Software Policy.
- The IT Unit along with the Audit Unit, is responsible for undertaking audit of all software at least once a year to ensure that all copyright and license agreements are adhered to.
- Most of the standard software titles listed on NITA's e-Government Interoperability Framework which are being used within the Ministry, are not freeware; therefore, the cost of software is a consideration for most titles and their deployment.
- It is the goal of the RSIM to keep licensing accurate and up to date. To address this, the Ministry is responsible for purchasing software licenses.

10.3.5. Installation

Only original software with the proper license is to be installed on MoGCSP's IT devices. All software installation is to be carried out by the IT Unit.

10.3.5.1. Approved Methods of Installation

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

- Original Equipment Manufacturer (OEM) installation on the hardware
- An IT Unit installation procedure that provides for the following:

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

- Custom Built IT Solution
- An automated installation through an IT-developed solution that may be used in a rapid-deployment scenario or silent-install situation

10.3.5.2. Non-Approved Methods of Installation

Software cannot be installed on MOGCSP's systems in the following scenarios:

- An installation not administered by the IT Unit.
- Software not purchased by MoGCSP and not approved by IT Unit.
- A pirated copy of any software downloaded from the Internet.
- Any means not covered by the ways that software can exist on MOGCSP computers.

10.3.6. Software Documentation

All bespoke softwares developed under the MoGCSP must have the following documents submitted to the Ministry through RSIM/IT Unit.

- Source Code
- System or Functional Requirements Document
- System Designs
- User acceptance Documentation
- Training manuals (End User and Technical Manuals)
- Hosting Accounts, and any other account related to the system.
- Database account
- Maintenance Agreement.

For subscription-based software, the following documents must be submitted to the Ministry through RSIM.

- License indicating the validity period.
- Support Documentation
- Training manuals (End User and Technical Manuals)
- All accounts related to the Software

10.3.7. Support

MOGCSP's IT Unit is responsible for installing and supporting all software on MOGCSP Infrastructure. MOGCSP's IT Unit relies on installation and support to provide software in a good operating condition to MOGCSP employees so that they can best accomplish their tasks

10.3.8. Software Request

- If a user requires a special software other than those provided by RSIM/IT Unit, the request must be sent to the RSIM/IT Unit to ascertain if the software meets required standards and is appropriate. The IT Unit will forward the request to the Procurement Unit for processing.

10.3.9. Software Usage

- Prior to the use of any software, the employee must receive training and instructions on usage and licensing agreements relating to the software, including any restrictions on use of the software.
- This will be the responsibility of IT Unit in collaboration with Human Resource and relevant stakeholders.
- Employees are prohibited from bringing software from home and loading it onto their assigned computer hardware.
- Unless express approval from the Chief Director, is obtained, software cannot be taken home and loaded on an employees' personal computer.
- Where an employee is required to use software at home, the option of providing the employee with a portable computer should be considered in the first instance.
- Where the employee cannot be provided with a portable computer, authorization from the Chief Director is required to purchase separate software, if licensing or copyright restrictions apply. Where software is purchased in this circumstance, it remains the property of the Ministry.
- All software acquired for or on behalf of the Ministry or developed by MoGCSP employees or contract personnel on behalf of MoGCSP shall be deemed MoGCSP property. All such software must be used in compliance with applicable licenses, notices, contracts, and agreements.

11.0. SYSTEMS ADMINISTRATION

11.1. Logical Access Controls

11.1.1. Authorization

- MoGCSP shall have a comprehensive control system for granting Network, Systems, Data, and Application access to both staff and authorised non-staff. Access to the use of IT facilities may be granted by the IT Unit.
- System Managers are to ensure that each computer system has a unique electronic identifier ID.
- System and data managers, as applicable shall conduct and document a risk analysis for each system and based on the analysis, implement any mechanisms that are warranted.
- Access to IT facilities shall be granted only upon approval by the RSIM/IT Unit.

11.1.2. Monitoring

To ensure that IT facilities are secure and efficient:

- RSIM / IT Unit shall periodically monitor the facilities and user rights.
- RSIM / IT Unit shall take emergency action to safeguard the integrity and security of the facilities, including termination of a program, job, or online session, or temporarily alter user account names and passwords.
- All security-related events on critical or sensitive systems shall be logged and audit trails saved.
- The RSIM/IT Unit may suspend any person from using the facilities if found to be:
    - responsible for deliberate or grossly negligent damage to any IT facilities.
    - in possession of confidential information obtained improperly through IT usage.
    - responsible for deliberate destruction of information through IT usage.
    - responsible for deliberate interruption of normal services provided by the MoGCSP.
    - responsible for the infringement of any Intellectual Property rights.
    - gaining or attempting to gain unauthorised access to accounts and passwords.

- gaining or attempting to gain access to restricted areas without the permission of the IT Unit.
- responsible for inappropriate use of the facilities.

- Restoration of a suspended person to further use of IT facilities will be dependent on approval by the Chief Director in consultation with the IT Unit.
- Anyone with knowledge of a security issue shall only discuss the issue with the IT Unit.
- Users shall not attempt to probe computer security mechanisms. Any person in possession of files containing hacking tools or other suspicious material without the prior written authority of the IT Unit would be subject to disciplinary procedures.

11.1.3. Reporting Security Issues

Anyone who identifies security issues in the IT system shall immediately notify the IT Unit where:

- Sensitive information is in danger of being lost, suspected of being lost, or disclosed to unauthorised persons.
- Unauthorised use of information on the system has taken place or is suspected to have taken place.
- Passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed or in danger of being lost or disclosed.
- There is any unusual systems behaviour, such as missing files, frequent system crashes, misrouted messages.

11.1.4. User Registration

- Only authorised persons will be registered on the MoGCSP IT facilities.
- All MoGCSP users shall be assigned access rights based on role.

11.1.5. User Deregistration

- Persons shall be de-registered when found to be ineligible
- Users who have been interdicted, dismissed, transferred, have vacated their posts, are indisposed for at least four (4) months, are on leave of absence, retired, resigned, or dead shall be deregistered.
- In the implementation of the above, the Director of HR shall immediately inform the IT Unit to de-register the said user.

11.1.6. Password Management

All systems will be protected by passwords

· Full rights to all MoGCSP-owned servers shall be given to no more than three (3) persons approved by the IT Unit to ensure continuity of operations. A copy of the passwords shall be kept in a secure environment for their access. Data owners or custodians may employ another layer of protection to protect end-user access to their data. The IT Unit shall not be prevented access to any data on the System.

· Decryption of passwords is not permitted, except by authorised staff performing security reviews or investigations.

· Access to the network, servers, and systems shall require unique logins and authentication.

· Accounts of terminated users shall be immediately disabled.

11.1.7. Remote Access/ Third Party Connections

· All remote access/third party connections need authorisation, after risk analysis by MoGCSP's IT Unit. Third-party connection to MoGCSP network shall not be allowed unless authorised by the IT Unit. Authorisation shall be documented by the IT Unit.

· All third-party connections are owned by MoGCSP and shall be reviewed and approved in advance as part of the authorisation process.

· It is the responsibility of MoGCSP employees, contractors, vendors, and agents with remote access privileges to MoGCSP 's network to ensure that their remote access connection shall be in line with the provisions of the Guidelines to Policy Document Governing IT.

· The following, under Password and Internet/Virtual Private Network Security Policy provides further details of protecting information when accessing the MoGCSP network via remote access methods, and acceptable use of MoGCSP 's network:

· Acceptable Encryption Policy

· Virtual Private Network (VPN) Policy

· Acceptable Use Policy

· Unacceptable Use Policy

11.2. Access Control and User Management

11.2.1. Guiding Principles- General Requirements

The IT Unit will provide access privileges to MoGCSP's technology (including networks, systems, applications, computers, and mobile devices) based on the following principles:

- Need to know – users or resources will be granted access to systems that are necessary to fulfil their roles and responsibilities.
- Least privilege – users or resources will be provided with the minimum privileges necessary to fulfil their roles and responsibilities.
- Requests for users' accounts and access privileges must be formally documented and appropriately approved.
- Requests for special accounts and privileges (such as vendor accounts, application and service accounts, system administration accounts, shared / generic accounts, test accounts, and remote access) must be formally documented and approved by MoGCSP.
- Application and service accounts must only be used by application components requiring authentication; access to the passwords must be restricted to authorised IT administrators or application developers only.
- Where possible, the Institution will set user accounts to automatically expire at a pre-set date.
- More specifically, when temporary access is required, such access will be removed immediately after the user has completed the task for which the access was granted.
- User accounts assigned to contractors will be set to expire according to the contract's expiry date.
- User accounts will be disabled after 3 months of inactivity. This does not apply to accounts assigned to staff.
- Access rights will be immediately disabled or removed when the user is terminated or ceases to have a legitimate reason to access MoGCSP's systems.
- A verification of the user's identity must be performed by the IT Unit before granting a new password.

- Existing user accounts and access rights will be reviewed at least annually to detect dormant accounts and accounts with excessive privileges. Examples of accounts with excessive privileges include:
- An active account assigned to external contractors, vendors, or employees that no longer work for the Institution.
- An active account with access rights for which the user's role and responsibilities do not require access. For example, users who do not have authority or responsibility to approve expenses should not have access with approval permissions within a financial system.
- System administrative rights or permissions (including permissions to change the security settings or performance settings of a system) granted to a user who is not an administrator.
- Unknown active accounts.
- All access requests for system and application accounts and permissions will be documented.

11.2.2. Guiding Principles-Privileged Accounts

- A nominative and individual privileged user account must be created for administrator accounts (such as “first_name.last_name.admin”), instead of generic administrator account names.
- Privileged user accounts can only be requested by Directors and must be appropriately approved by the Chief Director.

11.2.3. Guiding Principles-Shared User Accounts

- Where possible, the use of specific network domain “security groups” should be used to share common access permissions across many users, instead of shared accounts.
- Shared user accounts are only to be used on an exception basis with the appropriate approval. This includes general user accounts such as “guest” and “functional” accounts.
- When shared accounts are required:

o Passwords will be stored and handled in accordance with the Password Policy.

- The use of shared accounts will be monitored where possible, including the recording of the time of access, the reason for accessing the shared user account, and the individual accessing his account. When the shared user account has administrative privileges, such a procedure is mandatory, and access to the monitoring logs must be protected and restricted.

11.2.4. Vendor or Default User Account

- Where possible, all default user accounts will be disabled or changed. These accounts include “guest”, “temp”, “admin”, “Administrator”, and any other commonly known or used default accounts, as well as related default passwords used by vendors on “commercial off-the-shelf” systems and applications.

11.2.5. Test Accounts

- Test accounts can only be created if they are justified by the relevant business area or project team and approved by MoGCSP, through a formal request to the Chief Director or the IT Unit.
- Test accounts must have an expiry date (maximum of 6 months). Maintaining test accounts beyond this date must be re-evaluated every 90 days and approved appropriately.
- Test accounts will be disabled / deleted when they are no longer necessary.

11.2.6. Contractors and Vendors

- In line with the Data Protection Act, contracts with contractors/vendors will include specific requirements for the protection of data. In addition, contractor/vendor representatives will be required to sign a Non-disclosure Agreement (“NDA”) prior to obtaining approval to access MoGCSP systems and applications.
- Before granting access rights to a contractor/vendor, the RSIM Directorate must verify that the requirements agreed upon have been complied with.
- The name of the contractor/vendor representative must be communicated to the IT Unit at least 2 business days before the person needs access.

- The need to terminate the access privileges of the contractor/vendor must be communicated to the IT Unit at least 1 business day before the contractor / vendor representative's need for such access ends.

12.0. IT COMMUNICATION

This chapter addresses the Ministry's IT Communication Systems and discusses the means of communication in place.

The following have been adopted as official means of communication.

1. Internet
2. E-mailing
3. Social media
4. PABX telephone system (VoIP)
5. Portal and Electronic Workflow Applications
6. MoGCSP Website
7. Fax
8. Bulk-SMS
9. Video Conferencing
10. Mobile Phones

12.1. Internet

- All connections to the Internet shall go through a secure connection point to ensure that the network is protected.
- RSIM Directorate should contact NITA for the availability of internet service provisioning at specified locations of the Ministry
- All Internet sites that may interfere with the smooth flow of Internet traffic shall be blocked.

12.2. Virtual Private Network (VPN)

- VPN shall be controlled among other things to prevent multiple unauthorised connections from one point.
- Users shall not connect to IT networks through VPN without first ensuring that all the technology is protected by up-to-date anti-virus software.

12.3. Privileged User Accounts

- Privileged access shall be given to selected authorized users
- Privileged usage access shall be always used prudently and appropriately
- Prohibited actions include but are not limited to:
- Casual browsing of other users' email, directories, and the contents of these directories
- Performing activities that would lead to an unauthorised level of access.

12.4. Electronic Messaging

The Ministry's email service can be used on any device, no matter whether owned by MoGCSP or an employee. The use of the Ministry's Emails does not matter where those E-mailing take place, whether on MoGCSP premises while traveling for business while working from home or any other location employees find themselves.

The provision in this section seeks to:

- Reduce the security and business risks faced by the Ministry
- Ensure the use of corporate email by staff for the Ministry's day-to-day business process
- Ensure employees follow good email etiquette
- Helps the Ministry satisfy its legal obligations regarding email use

All staff shall be issued official MoGCSP email addresses. It is mandatory for all employees to use their official email addresses for communicating official messages and correspondence related to their roles within the Ministry.

In the event of downtime or technical issues affecting the email system, the IT Unit will promptly communicate necessary guidelines and alternative communication methods to ensure continuity in official communications.

The e-mail system is MoGCSP's property, and all copies of messages created, sent, received or stored on the system are the property of MoGCSP. MoGCSP maintains its e-mail system solely for official purposes.

12.5. Prohibited Actions

IT Unit shall ensure that prohibited actions are periodically updated and disseminated.

The following actions and uses of the e-mail system are explicitly forbidden:

a. Sharing of email passwords is prohibited.

b. Personal use that creates a direct cost for the MoGCSP.

c. Usage of the system for personal monetary gain or for commercial purposes that is not related to work.

d. Sending unsolicited bulk mail messages of a personal nature.

e. Propagation of chain letters.

f. Advertising of personal items.

g. The use of private email accounts for official communication is strictly prohibited, except in instances of system downtime or as otherwise communicated by the IT Unit

h. Capturing and "opening" of electronic mail, except by authorised users to diagnose and correct delivery problems.

i. Use of electronic mail to harass or intimidate others

j. Sending copies of documents in violation of Intellectual Property laws and regulations.

k. Inclusion of the work of others into electronic mail communications in violation of Intellectual Property laws and regulations.

l. To interfere with others to conduct government business.

m. Use of electronic messaging systems for any purpose restricted or prohibited by Intellectual Property laws or regulations.

n. "Spoofing" i.e., constructing an electronic mail communication so it appears to be from someone else.

o. "Snooping" i.e., obtaining access to the files or electronic mail of others to satisfy idle curiosity, with no substantial government business purpose.

p. Subscribing to mailing lists, discussion groups, a list-server, or other such bulk mailing services, for private purposes.

q. Attempting unauthorised access to electronic mail attempting to breach any security measures on any electronic mail system or attempting to intercept any electronic mail transmissions without proper authorisation.

r. Using a password or code to access a file, or retrieve stored information, unless authorised to do so.

s. Frivolous usage of the e-mail system.

t. Subscribing to third-party mail systems and use of such mail systems from the premises of the MoGCSP, unless directly related to an official need or objective.

u. Except where authorised, retrieving and reading of any e-mail messages that are not addressed to the user.

12.6. E-mail Disclaimer

Users may not transmit personal opinions as those of MoGCSP, nor make any statement that may be construed to be a statement from MoGCSP. The IT Unit shall ensure that a disclaimer is suffixed to all email messages.

12.7. Email Addressing

The acceptable email address format is firstname.lastname@mogcsp.gov.gh. In the event where two names appear the same, then the middle name is added to the last name with a hyphen in between.

Sub Agencies under the Ministry may create a subdomain e.g. mda.mogcsp.gov.gh with approval from the Chief Director.

12.8. Expiration and Deletion of Account

An account shall be expired, deactivated or deleted under the following conditions:

a. The officer resigns/posted out from the service.

b. The officer retires from the service.

c. Any account that is inactive for ninety (90) days shall be deactivated if no information is given to the IT Unit. The account shall be deleted from the MoGCSP messaging system after one (1) year if no request is received during this duration. Subsequently, all formalities will need to be completed all over again for the reopening of the said account with the same ID subject to availability.

d. The officer is no longer able to perform his/her duties (missing, death, dismissal etc.)

The Director Human Resource shall inform the IT Unit when either of the above conditions is triggered.

12.9. Reactivation of Designation Email Account

The Director of Human Resource shall inform the IT Unit of the successor to a deactivated account to allow for activation for the new designated staff.

12.10. Attachment to e-mail messages

- The size of attachments to electronic messaging shall be controlled to avoid clogging the system. The accepted limit for document attachment is 25mb.
- Larger files must be shared over Microsoft SharePoint or FTP server.
- Approval should be sought to share MoGCSP owned document (must be categorised).

12.11. Default e-mail messages set up

Email Account shall be created by the IT Unit upon request by the Head of Human Resource of the Ministry/ Department/ Agency for new staff.

12.12. Carbon Copying/ Blind Carbon Copying

- Carbon Copying (CC) should only be done for individuals who need to have access or knowledge of the content of the message being sent but are not required to respond or action the message.
- Forwarded e-mails shall only be sent to authorised persons.

12.13. Privacy

Users shall not intercept, disclose or take part in intercepting or disclosing electronic messages. MoGCSP reserves the right to investigate the interception or disclosure of electronic messages.

12.14. Data Retention/ Deletion

- Email messages shall be retained on the server.
- No User shall delete official correspondence from his/ her emails.

12.15. Data Backup

- A backup schedule for the messaging system shall be implemented and tested periodically.
- Backup copies shall be stored securely at a location away from the system for our use.

12.16. Message Monitoring

The use of the e-mail system shall be subject to monitoring for security and/or network management reasons to support operational, maintenance, auditing, security and investigative activities. Users may also be subject to limitations on their use of such resources.

12.17. Incidental Disclosure

The content of an individual user's communications may be reviewed during incident response/ problem resolution.

12.18. Voice over IP (VOIP)

This system is the Ministry's private telephone network. It enables staff to communicate within the Ministry by using Voice over IP (VoIP) enabled phones. With this system, all internal telephony is routed through MoGCSP's Local Area Network (LAN), rather than via the Public **Switched Telephone Network (PSTN).**

12.9. Social Media Use

- MoGCSP's social media accounts should be used to post updates, messages etc. by authorised officers that are clearly in line with the Ministry's overall objectives.
- MoGCSP's social media handles must be verified by an authorised officer.
- MoGCSP editorial committee must review content before it is published online.
- MoGCSP should provide communication devices to authorised staff for official work.

12.9.1. Authorised Users of MoGCSP Official Social Media Accounts

Authorisation will be provided by the RSIM/D or PR Unit considering but not limited to assigned duties such as social media-related tasks that form a core part of an employee's job.

Authorised officers may use MoGCSP social media accounts to

a. Respond to enquiries and requests for help
b. Share blog posts, articles, and other content created by the Ministry
c. Share insightful articles, videos, media, and other content relevant to the Ministry, but created by others
d. Provide followers with an insight into what goes on at the Ministry
e. Promote publicity for Ministry events

Authorised users of the Ministry's social media account:

a. Must not use personal social media accounts for work-related purposes
b. Must not use official social media accounts for non-work purposes.
c. Must not use it to share or spread inappropriate content, or to take part in any activities that could bring the Ministry into disrepute.
d. Must not create or transmit material that might be defamatory or incur liability for the Ministry.
e. Must not post messages, status updates or links to material or content that is inappropriate.
f. Must not use social media for any illegal or criminal activities
g. Must not send offensive or harassing material to others via social media
h. Must not broadcast unsolicited views on social, political, religious issues, etc
i. Must not send or post messages or material that could damage MoGCSP's image or reputation
j. Must not post, upload, forward, or link to spam, junk email, or chain emails and messages
k. When sharing an interesting blog post, article or piece of content, employees should always review the content thoroughly and should not post a link based solely on a headline.

l. Must share content that promote gender equality and avoid reinforcing gender stereotypes. These platforms must not be used to harass or intimidate individuals based on gender, age, disability, or other status.

12.20. MoGCSP Website

The MoGCSP's website seeks to provide information to the public on the activities of the Ministry. It will also serve as a medium where complaints and reports can be filed for action to be taken. The Ministry's website address is www.mogcsp.gov.gh.

The Ministry's website at a glance, should give an overview of MoGCSP including all its Departments, Agencies, and Units.

12.21. Bulk SMS

Bulk messaging is the dissemination of large numbers of SMS messages for delivery to mobile phone terminals. It is used by media companies, enterprises, banks (for marketing and fraud control), and consumer brands for a variety of purposes including entertainment, enterprise, and mobile marketing. The Ministry shall use this media for alerts, reminders, information sharing, and communication between both staff and the public.

12.22. Video Conferencing

A video conference is a live, visual connection between two or more people residing in separate locations for communication. At its simplest, video conferencing provides transmission of static images and text between two locations. At its most sophisticated, it provides transmission of full-motion video images and high-quality audio between multiple locations.

13.0. DATA PROTECTION

13.1. Electronic Document Management

13.1.1. Document Workflow

- The Records Unit under the General Administration Directorate shall register all documents and electronically capture them.
- Document Workflow shall follow the accepted channel of correspondence being implemented in the Ministry.

13.1.2. Document Creation/ Authoring/ Collection

- MoGCSP shall establish policies to authenticate users and determine the integrity of each type of electronic record.
- All official documents/records shall be created; copied, scanned, or generated using the standard approved by PRAAD/ NITA and are compatible with the Document Management System.

13.1.3. Document Review and Approval

All official documents/records shall be approved in accordance with MoGCSP 's current approval hierarchy.

13.1.4. Document Release

MoGCSP depending on approval hierarchy shall restrict the distribution of documents, records, data and resources generated on or reposed on IT facilities where national security or MoGCSP resources may be placed at risk or where there are issues of sedition, Intellectual Property rights infringements.

13.1.5. Document Storage/ Protection/ Organisation

- Users shall be obliged to always preserve the integrity of electronic information.
- All official documents must be uniquely identified by at least a document number, revision number, publication date, and title before storage.
- MoGCSP shall ensure that all official documents are appropriately reviewed and approved to certify new documents, ensure accuracy, and update the documents as necessary.

13.1.6. Principles of Data Protection

MoGCSP will ensure that users processing personal data shall abide by the following principles of good data protection practice. The data must be:

a. Fairly and lawfully processed.

b. Processed for limited purposes.

c. The data should be updated accordingly

d. Adequate, relevant, and not excessive.

   i. Accurate

   ii. Kept according to law but not kept longer than necessary.

e. Processed in accordance with the data subject's rights.

f. secured from unauthorised access.

g. Data shall not be shared/ transferred without adequate protection as provided in the data protection laws of Ghana.

h. MoGCSP should ensure that all data controllers under the Ministry are registered with the National Data Protection Commission.

i. Special attention shall be given to protecting sensitive gender-related data, including information about survivors of gender-based violence and vulnerable populations. Access to this data must be strictly controlled.

j. Staff who handle gender-sensitive data shall be trained in confidentiality and trauma-informed approaches to data security.

13.1.7. Document Expiration/ Disposal/ Archival

· MoGCSP will ensure that all documents created or reproduced in any manner shall be categorised to conform to the classifications system of the Public Records Administration and Archives Department (PRAAD).

· MoGCSP shall ensure that all official documents that must be archived are subject to the archival process set forth by the PRAAD and any appropriate establishment.

· MoGCSP shall put in place a robust mechanism to dispose of electronic data in conformity with the standards of retention and disposition schedule laid down by PRAAD.

13.1.8. Cataloguing Policy

For proper cataloguing, all information shall be hosted in soft copy formats to ensure quick retrieval to supplement the hard copy version of the information when required.

13.1.9. Information Sensitivity

MoGCSP's management is responsible for determining the sensitivity levels.

RSIM shall implement mechanisms for protecting information at varying sensitivity levels:

a. Low Sensitivity

b. Medium sensitivity

c. High Sensitivity

13.1.10. Storage

Users shall protect the storage of official information, IT systems from unauthorised persons.

The Ministry must have full control over and access to all its data.

14.0. SECURITY

14.1. Anti-Virus

Only up-to-date IT Unit approved Anti-virus software shall be always installed on IT Systems including end users' computers.

14.2. Incidents

Immediately if a virus incident is detected, the user shall alert the IT Unit by the fastest direct means available and shall immediately thereafter fill out an Incident Report Form and submit it to the IT Unit. IT Unit shall promptly initiate resolution of the virus incident.

14.3. Firewall

A robust approved firewall shall be always implemented on IT facilities.

14.3.1. Intrusion Prevention System

The IT Unit shall configure an Intrusion Prevention System (IPS) which would provide network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits which come in the form of malicious inputs to target applications or services that attackers use to interrupt and gain control of an application or machine.

14.3.2. Packet Filtering

The IT Unit shall configure access control lists to regulate authorized source and destination networks

IT Officer shall configure firewall to filter inbound and outbound authorized traffic only

14.3.3. Stateful Inspection

The IT Unit shall deploy a firewall that has stateful inspection feature to keep track of each connection in a state table and blocking packets that deviate from the expected state.

14.3.4. Application Filtering

The IT Unit shall configure firewall to allow or deny access based on authorized applications running on domain. Unsecured http (port 80) will be blocked and only https (443) will be allowed on the MoGCSP network.

14.4. Software Security

MoGCSP's IT Section will test for flaws to uncover vulnerabilities the system and determine that its data and resources are protected from possible intruders.

14.5. Security for Server Room – Environmental Control

Install a temperature monitoring device to report changes in temperature levels.

14.6. Security for Server Room – Power

There shall always be an adequate and clean power supply to the server room.

All servers and PCs shall have Uninterruptible Power Supply (UPS) and appropriate power rating outlets capable of supporting the system.

A power generator shall be provided as a backup to the national power grid.

14.7. Security for Server Room – Fire

There shall be installed in the server room, a fire-detection/early warning mechanism, consisting of smoke or heat detectors integrated into the building's fire alarm system, which on activation, shall raise an audible alarm and possibly cut the power supply to the various rooms. There will also be availability of appropriate fire extinguishers

14.8. Close Circuit Television (CCTV)

A critical component of a comprehensive security plan is closed-circuit television (CCTV) — a technology that can remotely monitor and record activities within MoGCSP. The objective of this is to ensure the Institution has adequate security controls to restrict access to systems and data and to monitor activities.

The purpose of this policy is to provide guidelines for the use of CCTV and Access Control on MoGCSP 's property in a way that enhances security but also respects the expectation of reasonable privacy among members of the Ministry. This policy applies to all departments, and agencies under the ministry.

- CCTV monitoring and Access control is to deter crime and to protect the safety and property of the Ministry. Safety and security purposes include, but are not limited to:
  - Protection of all individuals.
  - Protection of MoGCSP-owned and/or operated property and buildings, including building perimeters, entrances and exits, lobbies and corridors, special storage areas, server rooms, and cashier locations.
  - Verification of alarms and access control systems.
  - Investigation of criminal activity and serious disciplinary activity, such as unauthorised access to some storage areas, in accordance with this policy.
- CCTV monitoring will be conducted in a professional, ethical, and legal manner. The IT Unit involved in monitoring will be appropriately trained and supervised in the responsible use of this technology. Violations of the code of procedures set forth under the scope below may result in disciplinary action consistent with the rules and regulations governing MoGCSP.
- Information obtained through monitoring will only be released when approved by the Minister or Chief Director of MoGCSP.
- Monitoring will be conducted in a manner consistent with all existing ministry policies, including the non-discrimination policy, the sexual harassment policy, and other relevant policies. Monitoring based on the characteristics and classifications contained in the non-discrimination policy (e.g., race, gender, sexual orientation, national origin, disability, etc.) is strictly prohibited.
- The existence of this policy does not imply or guarantee that cameras will be constantly monitored in real-time by the IT Unit.

· Access controls are necessary to ensure that only authorised users can obtain access to an Institution's information and systems

This applies to:

MOGCSP HQ, Departments, Agencies, Secretariats, and Council of MoGCSP.

All staff, consultants, contractors, agents, and authorised users accessing MoGCSP's IT systems and applications.

All IT systems or applications managed by MoGCSP's IT Unit that store, process or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

Any diversion of security technologies for purposes other than the safety and security purposes contemplated by this policy is prohibited.

14.9. System Monitoring

All security-related events on critical or sensitive systems shall be logged and audit trails saved at intervals.

14.10. Change Management

RSIM shall have a change management plan to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes associated with the Ministry's IT infrastructure and services, to minimize the number and impact of any related incidents.

14.11. Database Security

14.11.1. Storage and Retrieval

· The IT Unit shall ensure that all Databases are secured. Storage and retrieval of information shall only be by authentication and authorization.

· To maintain the security of databases, access to tables, fields and records shall be granted after authentication of issued credentials.

14.11.2. Vendor Policy

There shall be a service level agreement with Service Providers who intend to provide services to MoGCSP in accordance with the Information Security guidelines.

14.12. Network and Internet Security

- There shall be established De-militarized Zone (DMZ) standards; all equipment owned and/or operated by MoGCSP located outside IT Internet firewalls.
- These standards apply to any host device outsourced or hosted at external/third-party service providers, if that equipment resides in the domain or appears to be owned by MoGCSP
- IT Unit shall collaborate with the Internal Audit Unit to periodically audit DMZ equipment in accordance with the Internal Audit Policy.
- MoGCSP network and computing systems shall be secured against unauthorised access and/or abuse.
- IT Unit shall ensure that the use of network sniffers is restricted to resolving network problems. Auditors or security officers in the performance of their duties may be authorised to use the utility.

14.13. Risk Assessment

A Risk Assessment/Remediation program shall be developed and implemented by the RSIM.

- The execution of the remediation programs shall be the joint responsibility of the RSIM /IT Unit, designated Information Security teams, and the entity (department/ directorate/ division/ Unit) responsible for the system's areas being assessed.
- Users shall fully cooperate with the Risk assessment/ remediation program being conducted on systems for which they are held accountable.

14.14. Risk Assessment Process

Risk Assessment Processes shall be defined by the MoGCSP Information Security or MoGCSP Cyber Security team in collaboration with the RSIM /AUDIT and the entity under consideration.

14.15. Backup

- Full backups of all Ministry data shall be performed weekly.
- Incremental backups of all Ministry data shall be performed daily.
- Where possible backups are run overnight and are completed before 8 AM on working days.
- Upon completion of backups, media copies shall be moved automatically to a secure remote site for disaster recovery purposes.
- Backups are stored in secure locations. A limited number of authorised personnel have access to the backup application and media copies.
- The IT Backup systems have been designed to ensure that routine backup operations require no manual intervention.
- The IT Unit monitors backup operations and the status for backup jobs is checked daily during the working week.
- Any failed backups are re-run immediately the next working day.
- The copies of the backup shall be stored on premises in a different facility from the data centre.

The purpose of this is as follows

- To provide secure storage for data assets critical to the workflow of official Ministry business
- To prevent loss of data in the case of accidental deletion/corruption of data, system failure, or disaster
- To permit timely restoration of archived data in the event of a disaster or system failure
- The scope of this applies to all official computers and other devices that contain Ministry data.

14.16. Recovery

RSIM shall have a disaster recovery plan to ensure business continuity in case of any disaster. The purpose of this disaster recovery (DR) plan is to prepare MoGCSP in the event of disruptions affecting corporate local area networks (LAN), Internet access, communication systems, and workflow services due to factors beyond our control

(e.g., natural disasters or man-made events). This plan will also guide the restoration of said services and normalize operations to the widest extent possible in a minimum time frame.

All MoGSCP departments and agencies that are connected to the WAN are expected to implement preventive measures whenever possible to minimize operational disruptions and to recover as rapidly as possible when an incident occurs.

This plan identifies vulnerabilities and recommends necessary measures to prevent extended network outages. It is a plan that encompasses all MoGSCP department and agency network operations in all locations

14.16.1. Disaster recovery planning goals:

- To provide operational continuity and quick recovery for all critical systems impacted by a technology-related disaster event.
- To ensure that the disaster recovery program is properly communicated to all staff, clearly identifying all essential roles and responsibilities.
- To ensure adherence to established safety procedures, exit plans, and related emergency requirements.
- To maintain an orderly process for business resumption and systems recovery.
- To ensure that disaster recovery activities and strategies are continually tested and revised as needed.

14.16.2. Distribution

RSIM would initiate protocols for activation of DR when all conditions to trigger it have been met. All communication channels as defined in the document would be followed to start the recovery process.

14.16.3. Integration

All other staff may work from remote locations and access local resources via an internet connection.

16.16.4. Activation Criteria

Activation Criteria (Trigger Events)

- Outage of power systems for periods beyond 6 hrs.
- Internet disruption from primary ISP beyond 3 hrs.

14.16.5. Activation Procedures

IT UNIT in charge will evaluate the severity of a disaster. The findings would be shared with the IT steering committee for the appropriate DR plan to be endorsed and recommended to the Chief Director to activate protocols to initiate the DR plan.

14.16.6. Disaster Recovery Procedures

14.16.6.1. Communications Procedures

- The Chief Director would announce the occurrence of disaster, and the IT steering committee would initiate protocols to switch over to a warm site.
- Staff would be briefed daily via their private emails about the status of the Disaster remedial plan to be able to allow staff to plan their daily operations.
- IT Support team would be available on standby to guide MoGCSP staff to access the warm site
- Users should resort to personal phone lines, private emails, Modem Dongles provided by MIS, and Tether personal phones for internet access, the website is hosted in the cloud.

14.16.6.2. Remote Access Procedures

Secure remote access would be provided via VPN access. IT Support staff would communicate by Mail and Phone to all MoGCSP staff to switch access to redundant sites.

14.16.6.3. Backup and Data Recovery Procedures

Backups are stored on External USB Storage and are readily accessible in the event of the need to restore a failing system.

USB Storage backups would be readily available and easily connected to the target failover system for direct backup restoration thereby preventing overhead costs

14.17. Helpdesk

There shall be an established Help Desk to provide users with a single point of contact to receive help on various computer issues and also when DR plans are activated. The Helpdesk shall be trained to provide gender-sensitive and respectful ICT support services and must ensure that females and other vulnerable staff can safely report any IT-related issues.

15.0. CAPACITY BUILDING AND UTILISATION

The Ministry is fully aware that human resource development in IT is a crucial element in the achievement of IT objectives. Consequently, MoGCSP shall implement a vigorous IT Training program that is aimed at producing an IT-literate workforce.

- Every member of staff shall have training at least in but not limited to basic computer literacy and be able to produce results using IT products. Training programs in the use of productivity software (i.e. MS Word, MS Excel, MS PowerPoint, etc) shall be organized periodically to raise the competence of all staff.
- Specialized training shall be organized for staff according to their sectional and/or professional groupings in specific software products best suited for their job functions.
- The MoGCSP IT systems, services, and facilities are provided to enable employees and other authorized individuals to perform their duties effectively and efficiently. All normal use of these systems in pursuit of MoGCSP business within an employee's authority to act is allowed. Illegal activity is not allowed.
- ICT training programs shall be gender-responsive and inclusive. Deliberate efforts shall be made to encourage the participation of female staff and those with special needs, as well as other marginalized groups.
- Training shall include content on digital safety and cyber hygiene, especially for female staff and vulnerable users who may face increased cyber risks.
- Directorates, Departments and Agencies within the Ministry of Gender, Children, and Social Protection (MoGCSP) are encouraged to actively seek training from the IT Unit to enhance their operational effectiveness and improve their ability to leverage technology in their day-to-day tasks. They may request training by submitting a formal request with identified training needs.

16.0. COMPLIANCE/ ENFORCEMENT

To ensure compliance with the ICT Policy, the following enforcement measures will be implemented:

1. The Internal Audit Unit of MoGCSP in collaboration with the IT Unit shall conduct regular periodic audits of the IT systems and usage policies. Findings from these audits will be presented to the Research, Statistics, and

Information Management Directorate (RSIM) for necessary remediation.

2. Any user found to have violated this policy shall be subject to disciplinary action as per the guidelines established in the Civil Service Code of Conduct.

3. All users must avoid any form of digital gender-based violence, such as cyberstalking, non-consensual image sharing, and online harassment. Such actions will be subject to sanctions under the Civil Service Code of Conduct and Ghana's cybersecurity laws.

17.0. VIOLATION

Users who violate the ICT Policy of the Ministry of Gender, Children, and Social Protection (MoGCSP) may face disciplinary actions as outlined in the Civil Service Code of Conduct. The Ministry is committed to maintaining a secure and efficient IT environment, and adherence to this policy is essential for achieving that goal.

17.1. Penalties

Penalties for violating the ICT Policy will vary based on the nature and severity of the specific violation. Employees found to be in violation of this policy will be subject to appropriate disciplinary actions, which may include:

1. Written Warning: For minor infractions, a formal warning may be issued, outlining the nature of the violation and the expected corrective actions.
2. Suspension: For more serious violations, employees may face temporary suspension from their duties, pending further investigation.
3. Termination: In cases of severe or repeated violations, disciplinary actions may escalate to the OHCS for the termination of employment.

18.0. MONITORING AND EVALUATION

The Monitoring and Evaluation (M&E) framework of this ICT Policy is established to ensure its successful implementation and continuous improvement.

The framework aims to:

· Track the overall progress of the ICT Policy, identifying gaps or areas for enhancement to align with the Ministry's goals and objectives.

- Monitor key performance indicators such as system uptime, compliance with security protocols, user engagement, and effectiveness of IT infrastructure in supporting program delivery.
- Measure specific indicators, including the rate of adoption of ICT systems, user satisfaction levels, incidences of security breaches, and the functionality of digital services provided by the Ministry.
- Collect relevant data through various channels, such as system performance logs, audit trails, user feedback, and quality assessments to ensure data-driven decision-making.
- Carry out regular monitoring and evaluation exercises, including the generation of quarterly and annual reports to track progress against set benchmarks.
- Assign clear responsibilities for the M&E process to key stakeholders, including the IT Department, policy makers, data owners, and end-users to ensure accountability and shared ownership.
- Evaluate the Policy's performance against criteria such as effectiveness, efficiency, quality of service delivery, security of systems, and overall user satisfaction, enabling informed adjustments when necessary.

19.0. DISCLAIMER

The Ministry of Gender, Children, and Social Protection (MoGCSP) shall not be liable for any loss, damage, or inconvenience, whether direct, indirect, or consequential, arising from the use, misuse, or unavailability of its IT systems, services, or data. The Ministry does not guarantee the accuracy, reliability, or completeness of any information obtained through its systems. Users of the Ministry's IT systems undertake to indemnify, defend, and hold harmless the MoGCSP from any claims, liabilities, or damages resulting from their use of the Ministry's IT resources, including but not limited to errors, omissions, or system failures

20.0. AMENDMENT OR REVISION OF POLICY DOCUMENT

The ICT Policy shall be reviewed and amended every three (3) years to reflect the evolving needs of the Ministry and the dynamic nature of technology. However, interim revisions may be authorized by the Chief Director when deemed necessary.

Triggers for revision may include:

- Significant advancements in technology that impact the Ministry's operations.
- Changes in legal or regulatory frameworks that require adjustments to ICT practices.
- Feedback from user satisfaction surveys or security audits that highlight areas for improvement.
- Any other factors that require modifications to ensure the policy remains relevant, efficient, and aligned with best practices in ICT management.

20.0. APPENDIX

13.1. Glossary

1. **Access control** is a system that enables an authority to control access to areas and resources in a given physical facility or computer-based information system. An access control system, within the field of physical security, is generally seen as the second layer in the security of a physical structure. Access control (AC) is the selective restriction of access to a place or other resource. The act of accessing may mean consuming, entering, or using. Permission to access a resource is called authorization.

   Access to the IT system must be restricted to only authorised users or processes, based on the principle of strict need-to-know and least privilege.

2. "**Users**" are departments, agencies, council staff, consultants, contractors, agents, and authorised users accessing MoGCSP IT systems and applications.

3. "**System or Application Accounts**" are user IDs created on IT systems or applications, which are associated with specific access privileges on such systems and applications.

4. "**Privileged Accounts**" are system or application accounts that have advanced permissions (as compared to regular user account permissions) on such systems or applications. Examples of user accounts with privileges include administrative and super user accounts.

5. "**Access Privileges**" are systems permissions associated with an account, including permissions to access or change data, process transactions, create or change settings, etc.

6. "**Administrator Account**" is a user account with privileges that have advanced permissions on an IT system that are necessary for the administration of this system. For example, an administrator account can create new users, change account permissions, modify security settings such as password settings, modify system logs, etc.

7. "**Application and Service Accounts"** are user accounts that are not associated with a person

8. "**Nominative User Accounts**" are user accounts that are named after a person.
9. **Antivirus** or **anti-virus software** is used to prevent, detect, and remove malware, including but not limited to computer viruses, computer worms, Trojan horses, spyware, and adware.
10. **Backup** In Information Technology, a **backup** or the process of **backing up** refers to making copies of data so that these additional copies may be used to restore the original after a data loss event.
11. **Calendaring** is a computer software process or application that captures, plans, and organizes events and provides the user with an electronic version of the normal hard copy calendar.
12. **Carbon copying**, abbreviated **cc** or **c.c.**, is the technique of using carbon paper to produce one or more copies simultaneously during the creation of paper documents. With the advent of email, the term has also come to refer to simultaneously sending copies of an electronic message to secondary recipients.
13. **A computer network** often simply referred to as a network, is a collection of computers and devices interconnected by communications channels that facilitate communications and allow sharing of resources and information among interconnected devices.
14. **Contact List** is a list of all staff with corresponding Email Addresses and Details **(**Dept., Rank, Room No., Postal Address, Phone/Fax No. etc.)
15. **Contact Sharing** refers to email Addresses availed for official use. **CVS** Concurrent Versions System is a process of sharing, saving, and recovering version information for people using code.
16. **A database** is an organized collection of data for one or more purposes, usually in digital form. The data are typically organized to model relevant aspects of reality (for example, the availability of rooms in hotels), in a way that supports processes requiring this information (for example, finding a hotel with vacancies).
17. **Digital Asset Management** consists of management tasks and decisions surrounding the ingestion, annotation, cataloguing, storage, retrieval, and distribution of digital assets. Digital photographs, animations, videos, and music are samples of media asset management.

18. **Document** is a broadly used term that refers to word-processing files, e-mail messages, spreadsheets, database tables, faxes, business forms, images, or any other collection of organized data. Documents are also referred to as 'records.'

19. **Document Imaging** is a system for converting paper documents into an electronic or digital format. Techniques such as scanning and Optical Character Recognition etc. are some of the methods that are typically used.

20. **Document Lifecycle** refers to the period between when a document is created and when it is destroyed or archived

21. **Document Management** is the process of managing documents and other means of information such as images from creation, review, and storage to its dissemination. It also involves the indexing, storage, and retrieval of documents in an organized method.

22. **Document Management Systems** enable you to store documents electronically. This facilitates the process of retrieving, sharing, tracking, revising, and distributing documents and the information they contain. A complete Electronic Document Management System (EDMS) provides you with all the software and hardware required to ensure that you maintain control over all your documents, both scanned images and files that were created on a computer—like spreadsheets, word processing documents, and graphics. A complete EDMS includes document imaging, OCR, text retrieval, workflow, and Computer Output to Laser Disk capabilities.

23. **Document Retrieval** Document retrieval is the process by which you can search and 'retrieve' an archived document from a database. This is done by entering information in a database query screen to locate the file you are after. The Document Management System will then retrieve the document and let you work on it, whilst preventing other people from making changes.

24. **Electronic Mail** A method of exchanging digital messages by telecommunication.

25. **Electronic Messaging** is communication on a computer network

26. **Forwarding** Resending of an Email message to another Email Address

27. **A Help desk** is an information and assistance resource that troubleshoots problems with computers or similar products. Corporations often provide help desk support to their customers via a toll-free number, website, and/or e-mail. There are also in-house help desks geared toward providing the same kind of help for employees only. Some schools offer classes in which they perform similar tasks as a help desk.

In the Information Technology Infrastructure Library, within companies adhering to ISO/IEC 20000 or seeking to implement IT Service Management best practices, a help desk may offer a wider range of user-centric services and be part of a larger Service Desk.

28. **Information System (IS)** can be defined as a set of procedures that collects or retrieves, processes, stores, manages and disseminates information to support organizational decision making and control.

29. **Information Technology** provides capabilities that enable these applications to run.

30. **Intellectual property** (**IP**) is a term referring to several distinct types of creations of the mind for which a set of exclusive rights are recognized—and the corresponding fields of law. Under intellectual property law, owners are granted certain exclusive rights to a variety of intangible assets, such as musical, literary, and artistic works; discoveries and inventions; and words, phrases, symbols, and designs. Common types of intellectual property include copyrights, trademarks, patents, industrial design rights, and trade secrets in some jurisdictions.

31. **A mailbox** is a repository in computer memory where emails are stored for a single user.

32. **Meeting Scheduling** is the activity of finding a suitable time for an event such as meeting, conference, trip, etc. electronically.

33. **Metadata** is data about data or information known about the image to provide access to the image. Usually includes information about the intellectual content of the image, digital representation data, and security or rights management information.

34. **Paperless Office is** a workplace in which as much communication and as many procedures as possible have been computerised. The paperless office was predicted in the 1960s. The recent widespread availability of e-mail, the Internet, and word processing, file transfer, and intranet systems means that it is beginning to become achievable for those organisations that wish to pursue it. In a truly paperless office, document storage is on a computer rather than in filing cabinets, and written communication is not circulated in hard copy but e-mailed. This is largely unattainable, as most people still prefer paper to electronic copy, especially when faced with reading more than one page. Encouraging employees to cut down on paper usage can help achieve environmental management targets, and storing information electronically can lead to greater communication efficiency, which may result in a competitive advantage.

35. **Protocol (communications)** is a formal description of digital message formats and the rules for exchanging those messages in or between computing systems and telecommunications.

36. **Recordkeeping**: can be described as a systematic compilation of similar information in an office setting and stored in files/folders for office administration.

37. **Scanning** Using a scanner or other device to create a digital representation or electronic photograph of an image. The scanning process is often labour-intensive and costly, requiring a substantial investment in handling and processing original materials and their surrogate images. The current strategy is to capture an image at the highest resolution appropriate to the original and store it offline as an archival image on CD-ROM or magnetic tape. Techniques such as glossy compression and sub-sampling can then be used to create derivative images for use online. In the future, as the ability to deliver high-quality archival scans develops, it will be possible to place the archival scan online without the cost of recapture. Scanning can be done in-house or contracted out to a vendor. Whether scanning is done in-house or outsourced, the quality of the images can vary widely. Image specifications should be stated clearly in the contract with the vendor and sample images (at varying resolutions) of the materials to be scanned should be requested from the vendor prior to the start of the project.

38. **Snooping** is the unauthorised access to another person's computer or data.

39. **Software license** (or **software license** in commonwealth usage) is a legal instrument (usually by way of contract law) governing the usage or redistribution of software. All software is copyright protected, except material in the public domain.

40. **Spoofing** is an Email message whose sender address appears as though it is coming from a different person/source.

41. **Workflow** Speaks for the flow of work between people or individuals in an organisation, allowing it to be defined and monitored. In document management terms, workflow is usually used in the context of monitoring the creation, distribution, and retrieval of documents.

42. **Workflow Software** allows businesses to move electronic documents along a user-defined 'routing' path, from one workstation to the next, around a local or wide-area network. Once the document arrives at any given workstation, the receiver can add notations to, or modify, the document as they see fit. An insurance company might use workflow software to route claim forms through their organisation. A user at one step might wish to review the forms and add a new document to the electronic 'package' before sending it to the next workstation. The next user might wish to add several notations to the forms before sending them on to the final workstation for approval. The route can be as simple or as complex as a business process requires.

43. **XML (extensible mark-up language)** A key digital technology that focuses on data formatting and document processing, enabling active content delivery.

44. **Digital Gender Divide:** the gap between men and women regarding access to, use of, and skills in ICT.

45. **Gender-sensitive ICT:** technologies and digital environments that are inclusive, accessible, and responsive to the needs of women, men, and other genders.

46. **Digital gender-based violence:** targeted harassment and discrimination through technology against individuals, disproportionately affecting women, based on their gender.

22.0. REFERENCES

Legal And Regulatory Frameworks

1. Cybersecurity Act 2020 (Act 1038), Government of Ghana.
2. Data Protection Act 2012 (Act 843), Government of Ghana
3. Electronic Transactions Act 2008 (Act 772), Government of Ghana.
4. Executive Instrument 1 (E.I. 1), January 2013, Establishment of the Ministry of Gender, Children and Social Protection, Government of Ghana.

National Policies and Strategies

5. Ghana ICT for Accelerated Development (ICT4AD) Policy, Ministry of Communications, Government of Ghana.
6. Ghana National Cyber Security Policy and Strategy, Ministry of Communications and Digitalisation, Government of Ghana.

NITA Regulatory Documents

7. National Information Technology Agency (NITA) Data Centre Standards (Draft), NITA, Ghana.
8. National Information Technology Agency (NITA) Electronic Records and Data Management Standards, NITA, Ghana.
9. National Information Technology Agency (NITA) Local Area Network (LAN) Standards, NITA, Ghana.
10. National Information Technology Agency (NITA) Management of IT Infrastructure for MDAs and MMDAs, NITA, Ghana.
11. National Information Technology Agency (NITA) Systems and Applications Standards, NITA, Ghana.
12. NITA e-Government Interoperability Framework (eGIF), National Information Technology Agency, Ghana.

International Standards and Best Practices

13. Information Technology Infrastructure Library (ITIL), Global Best Practice.
14. ISO/IEC 20000 - Information Technology Service Management, International Organization for Standardization.

Institutional Frameworks

15. Civil Service Code of Conduct, Office of the Head of Civil Service (OHCS), Government of Ghana.

16. MoGCSP Organizational Manual, Ministry of Gender, Children and Social Protection, Ghana.

17. Public Records and Archives Administration Department (PRAAD) Records Retention and Disposition Schedule, PRAAD, Ghana

MINISTRY OF GENDER,CHILDREN AND
SOCIAL PROTECTION

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

JULY 2025