



Meeting Point International

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

Meeting Point International (MPI)

2026

Approved by the Board members:	Name: AMITO TEDDY BONGOMIN
	Signature:
	Title: TREASURER
	Name: ACHAN AIDA AGNES
	Signature:
	Title: VICE-CHAIRPERSON
	Name: EMMANUEL NSENGA Rutikanga
	Signature:
	Title: Secretary
	Name: BUSINYE ROSE
	Signature:
	Title: person
Approval Date:	22/09/2026
Date of Next Review:	01st September 2028
Version #:	01st

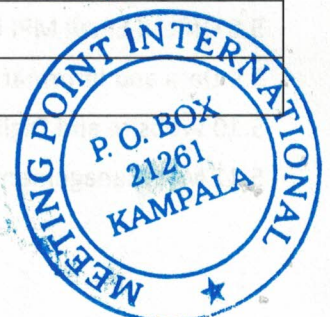


TABLE OF CONTENTS

A. Acronyms and Abbreviations	4
B. Definition of Common Terms	4
FOREWORD.....	5
1. INTRODUCTION	6
1.1 MPI's Vision	6
1.2 Our Mission	6
1.3 MPI's Method	6
2. BACKGROUND	7
2.1 Situational Analysis.....	7
2.2 General Scope.....	8
3. POLICY VISION	9
3.1 Policy Goal.....	9
3.2 Policy Mission	9
4. POLICY OBJECTIVES	9
5. POLICY AREAS AND PROCEDURES.....	9
5.1 ICT Use	9
5.1.1 Prohibited Activities	10
5.2 Technology Hardware and Software Acquisition	11
5.3 MPI Management and Use of Software	11
5.3.1 Software Usage.....	12
5.4 Bring Your Own Device (BYOD)	12
5.4.1 Keeping Mobile Devices Secure	13
5.4.2 Indemnity	14
5.5 Security of Information Technology	14
5.5.1 Information Security.....	14
5.5.2 Network Access	15
5.5.3 Technology Access.....	15
5.6 Business Continuity and Disaster Recovery	15
5.7 ICT Governance	16
5.7.1 MPI Management and Leadership Responsibilities	16
5.7.2 ICT Function Responsibilities.....	16
5.8 Official Email MPI Management and Use.....	17
5.9 Data and Information MPI Management	17
5.10 Website and Digital Platforms - MPI Management.....	18
5.11 MPI Management of ICT Service Agreements	18



5.12 Emergency MPI Management of Information Technology	19
5.13 Use of Social Media	20
6. IMPLEMENTATION STRATEGY	20
7. MONITORING AND EVALUATION	20
INFORMATION AND COMMUNICATION TECHNOLOGY POLICY ACKNOWLEDGMENT AND ACCEPTANCE FORM	22



A. Acronyms and Abbreviations

MPI	Meeting Point International
NGO	Non-Governmental Organization
ICT	Information and Communication Technology
IT	Information Technology
HIV/AIDS	Human Immunodeficiency Virus / Acquired Immunodeficiency Syndrome
LAN	Local Area Network
BYOD	Bring Your Own Device
CIA	Confidentiality, Integrity, and Availability
Wi-Fi	Wireless Fidelity
USB	Universal Serial Bus

B. Definition of Common Terms

Term	Meaning
Staff	Employees and authorized workers of MPI
ICT Personnel	Staff responsible for ICT systems, administration, and user support
Authorized Users	Individuals approved to access MPI systems, devices, or information
Beneficiaries	Individuals receiving care, support, or services from MPI
Donors	Individuals or organizations providing financial or material support to MPI
Vendors	External suppliers providing goods, software, equipment, or services to MPI
Contractors	External persons or firms engaged by MPI to provide services
Personal Device	Any privately-owned laptop, phone, tablet, or other device used for official work
Official Email	An email account issued and authorized by MPI for official communication
Digital Platform	Any online system, application, website, or communication platform used by MPI
Cloud Storage	Online storage used to save, access, and manage digital files and information
Data Protection	Measures and controls used to protect personal and organizational data
Information Security	Protection of information and systems against unauthorized access, misuse, loss, or damage
Business Continuity	The ability of MPI to continue critical operations during or after a disruption
Disaster Recovery	The process of restoring systems, data, and operations after a disruption or disaster
Website Register	A record of MPI website domains, hosting details, renewals, and ownership information
Social Media	Online communication platforms used to share information and engage with the public

FOREWORD

Since its founding in 1992 by Rose Busingye and official registration in 2003, Meeting Point International has remained committed to restoring dignity and hope to people affected and infected by HIV/AIDS and their children in the informal settlements of Kampala, including Naguru, Kireka, Ntinda, and Nsambya. Over the years, MPI has grown in both reach and responsibility, expanding its programs and strengthening the systems that support service delivery to vulnerable communities.

As MPI continues to grow, the role of Information and Communication Technology (ICT) has become increasingly important in supporting efficient operations, communication, record MPI Management, service coordination, and accountability. To strengthen institutional effectiveness and improve service delivery, MPI has invested in technology and digital systems that support both administrative and program functions. It is therefore necessary to establish clear ICT guidelines that ensure these systems are used effectively, responsibly, and securely across the organization.

The development of this ICT Policy has taken into consideration MPI's mission, operational needs, and alignment with other existing organizational policies and procedures, as well as internationally recognized ICT best practices. This policy will be reviewed periodically to ensure that it remains relevant, responsive to technological changes, and aligned with MPI's strategic goals and service priorities. From time to time, it may be necessary to revise, expand, or amend sections of this policy and its related procedures.

MPI's ICT Policy provides a structured framework to guide the use, MPI Management, and governance of ICT resources across the organization. It outlines best practices, defines the roles and responsibilities of staff and system users, and provides guidance on the proper implementation, use, and protection of ICT systems and resources in support of MPI's mission.

All users are required to comply with the guidelines set out in this policy, as well as applicable national laws and relevant international standards, and to refrain from any activity that may expose MPI to operational, legal, or reputational risk.

Lastly, I wish to acknowledge the efforts of MPI Management, the ICT personnel, who contributed to the development of this policy and whose continued commitment supports the effective and responsible use of technology at Meeting Point International.

1. INTRODUCTION

Founded by Rose Busingye in 1992, Meeting Point International (MPI) is a Ugandan non-governmental organization working with women, men, youth and children from the slums of Kampala, who are mainly affected and infected by HIV/AIDS.

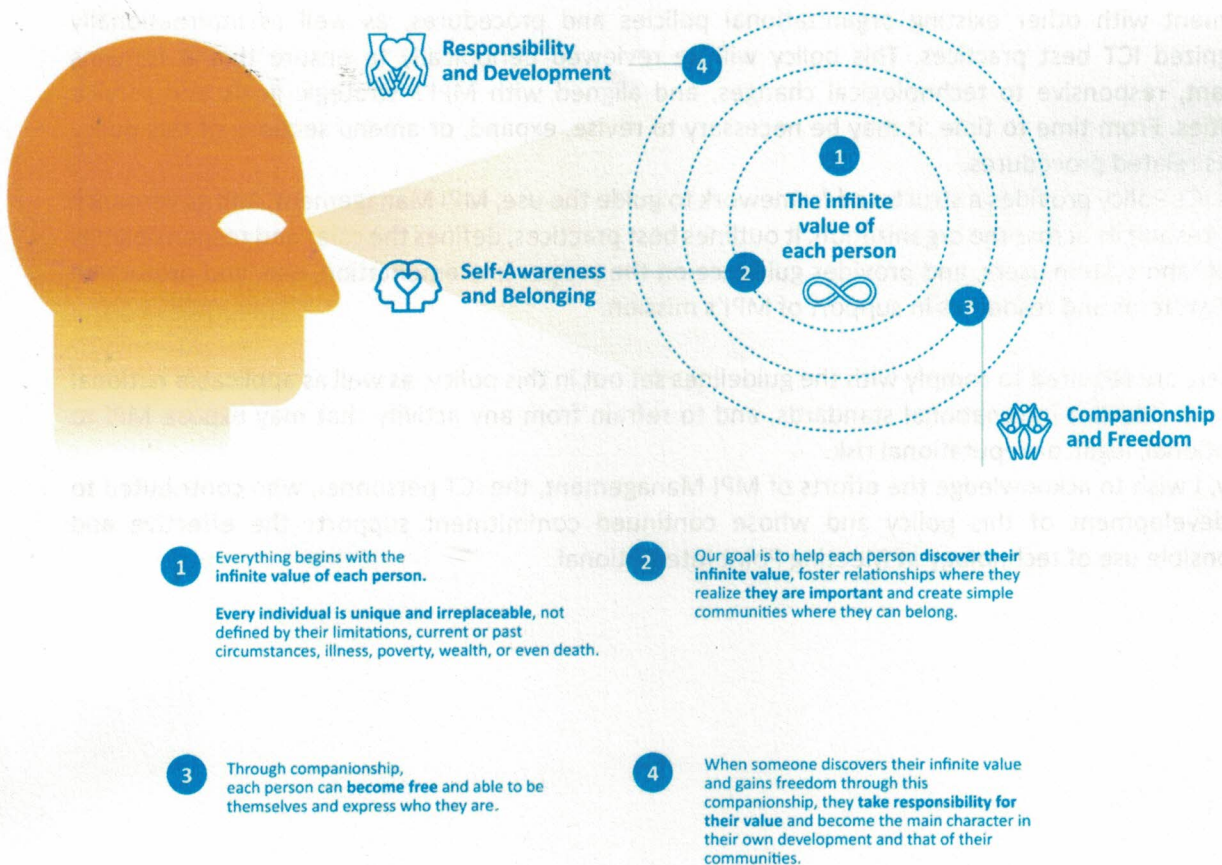
1.1 MPI's Vision

For every person to discover their infinite value and dignity, through a journey towards their own human development and that of their communities.

1.2 Our Mission

MPI aims at continuously accompanying every person and community, prioritizing victims of HIV/AIDS, promoting education at all levels and committing to poverty alleviation.

1.3 MPI's Method



2. BACKGROUND

In its mission to restore dignity and hope to people affected and infected by HIV/AIDS and their children, Meeting Point International recognizes Information and Communication Technology (ICT) as an essential enabler in improving service delivery, strengthening internal operations, and supporting effective communication across the organization. ICT plays a critical role in facilitating access to information, improving coordination of programs, strengthening case MPI Management, and enhancing communication between staff, beneficiaries, partners, and other stakeholders.

Over the years, Meeting Point International has invested in ICT infrastructure and digital tools to improve administrative efficiency, program implementation, data MPI Management, financial accountability, and communication within the organization. As MPI continues to grow and expand its reach in serving vulnerable communities across Kampala, the need for reliable, secure, and efficient ICT systems has become increasingly important.

MPI recognizes that technology continues to evolve rapidly, creating both opportunities and risks. While digital systems improve efficiency and support service delivery, they also expose the organization to risks such as cyber threats, data loss, unauthorized access, and misuse of information systems. As MPI handles sensitive information relating to beneficiaries, staff, partners, and organizational operations, it is essential that such information remains secure, confidential, and accessible only to authorized users.

It is therefore necessary for MPI to establish clear guidelines to govern the acquisition, use, MPI Management, and protection of ICT infrastructure and digital information systems. These guidelines are intended to safeguard organizational information, ensure responsible use of ICT resources, and protect the integrity of systems used in daily operations.

All users of MPI's ICT resources, including employees, interns, volunteers, consultants, contractors, and service providers, must be guided on the appropriate and responsible use of ICT in order to maximize its benefits while minimizing risks to the organization.

Despite continued investment in ICT resources, the opportunities and risks associated with technology require a clear framework for managing and protecting these assets. This policy therefore provides the guiding principles for the acquisition, use, maintenance, and protection of ICT equipment, systems, and information resources at Meeting Point International.

The policy is important in protecting the integrity, confidentiality, and availability of MPI's ICT systems and information resources, safeguarding users against misuse and unauthorized access, and providing a framework for addressing any improper use of ICT resources in violation of organizational policies and procedures.

2.1 Situational Analysis

Information and Communication Technology (ICT) has become one of the most important tools for improving efficiency, accountability, communication, and service delivery in organizations. For Meeting Point International, ICT is an essential enabler in supporting program implementation, beneficiary MPI Management, internal coordination, financial accountability, and communication with staff, partners, donors, and the communities it serves.

Recognizing the importance of ICT, MPI has adopted and continues to use a number of digital tools and systems to support its operations. These include organizational email systems, internet services, staff communication platforms such as WhatsApp, digital data collection tools, financial systems, cloud-

based storage, and social media platforms used for communication and visibility. MPI also relies on a Local Area Network (LAN), shared digital resources, and internet-based systems to support both administrative and program functions. These initiatives can deliver greater value when supported by clear policies and guidelines.

Despite this progress, MPI continues to face several challenges in the use of ICT resources. These challenges affect operational efficiency, data security, and the effective use of digital tools across the organization.

- Unrestricted or poorly controlled access to ICT resources may also expose MPI to security threats such as unauthorized access, malware, misuse of systems, and possible data breaches. These risks can compromise organizational operations and the confidentiality of sensitive information.
- Power instability and unreliable internet connectivity also affect MPI's day-to-day operations. Since many organizational functions depend on digital systems and internet access, disruptions in electricity and connectivity can negatively affect productivity and service delivery.
- Another challenge is the limited availability of specialized ICT personnel to fully manage, secure, and maintain ICT infrastructure and support users across the organization. This can affect system performance, user support, and timely response to ICT-related issues.

An ICT Policy is therefore necessary to provide clear guidance on how these challenges can be addressed and managed effectively.

Despite these challenges, MPI has significant opportunities to strengthen its use of ICT and improve institutional performance. These opportunities include:

- The increasing availability of affordable digital technologies and cloud-based systems that can improve communication, collaboration, data storage, and service delivery.
- The existence of national laws and regulations related to data protection, privacy, cybersecurity, and digital communications that provide a framework for responsible ICT use.
- Expanding internet and telecommunications infrastructure in Uganda, which has improved access to digital tools and reduced the cost of connectivity.
- Increased opportunities for digital learning, innovation, and system automation that can improve operational efficiency and reporting.

At the same time, MPI faces several ICT-related threats, including physical damage to equipment, cyber threats such as malware and phishing attacks, unauthorized access to systems, data loss, and misuse of digital resources. These threats require deliberate safeguards and controls.

This policy is therefore intended to help MPI maximize its ICT strengths, address existing weaknesses, leverage available opportunities, and protect the organization against internal and external ICT-related risks.

2.2 General Scope

This policy applies to all users of ICT resources at Meeting Point International, including employees, interns, volunteers, consultants, contractors, and service providers who access or use MPI's ICT systems, infrastructure, devices, or data in the course of their work.

This policy covers the following areas:

- ICT Use
- Technology Hardware and Software Acquisition
- MPI Management and Use of Software
- Bring Your Own Device (BYOD) for Official Use

- Information Security
- Business Continuity and Disaster Recovery
- Information Technology Administration
- Official Email MPI Management and Use
- Website and Digital Platform MPI Management
- MPI Management of ICT Service Agreements
- Emergency ICT Incident MPI Management
- Use of Social Media

3. POLICY VISION

An organization where ICT is effectively used as a strategic tool to support efficient operations, quality service delivery, and organizational growth.

3.1 Policy Goal

To enhance institutional efficiency, accountability, and effectiveness through the proper MPI Management, regulation, and use of ICT resources in support of MPI's mission and operations.

3.2 Policy Mission

To promote the effective, secure, and responsible use of affordable ICT systems and services by all users in supporting MPI's programs, operations, and service delivery.

4. POLICY OBJECTIVES

1. To provide guidelines for the acquisition and use of ICT hardware and software across the organization.
2. To provide guidelines for the protection and security of organizational information and digital systems.
3. To regulate and control access to MPI's ICT infrastructure, systems, and resources.
4. To provide guidance on the administration and MPI Management of ICT infrastructure and related resources.
5. To establish procedures for responding to ICT emergencies, incidents, and loss of information.
6. To provide guidelines on the use of official email, digital communication platforms, websites, and social media.

5. POLICY AREAS AND PROCEDURES

5.1 ICT Use

Overview

This section provides guidelines for the appropriate, secure, and responsible use of ICT resources at Meeting Point International. It covers the acceptable use of email, internet, software, digital devices, and organizational systems. It also outlines expectations regarding personal use, data handling, software installation, copyright compliance, and prohibited activities.

This policy applies to all users of MPI ICT resources, including employees, interns, volunteers, consultants, contractors, and other authorized third parties. It also applies to all ICT equipment, systems, and digital resources owned, leased, or managed by MPI.

Procedures

All information stored on electronic or computing devices owned, leased, or managed by MPI remains the property of Meeting Point International and must be protected in accordance with organizational data protection and information security requirements.

All computers, mobile devices, and other equipment connected to MPI systems or networks must comply with applicable ICT access and security requirements.

All users must maintain secure passwords for systems and devices. Sharing passwords or allowing unauthorized access to systems is strictly prohibited.

All computing devices must be protected with password-enabled screen locks. Users must lock or log off devices when left unattended.

Users must exercise caution when opening emails, attachments, links, or files from unknown or suspicious sources, as these may contain malware, phishing attempts, or other security threats.

5.5.1 Prohibited Activities

The following activities are strictly prohibited when using Meeting Point International ICT resources:

1. No user is permitted to engage in any activity that is illegal under applicable national or international law while using MPI's ICT systems or resources.
2. Users must not violate intellectual property rights, including copyright, trademarks, patents, trade secrets, or software licensing agreements. This includes the installation, copying, distribution, or use of unauthorized, pirated, or unlicensed software.
3. Accessing data, systems, servers, applications, or user accounts without authorization, or for purposes unrelated to official work, is strictly prohibited.
4. Introducing malicious software or harmful code into MPI systems or networks, including viruses, worms, Trojan horses, ransomware, spyware, or other disruptive software, is prohibited.
5. Users must not share passwords, disclose login credentials, or allow another person to use their account or system access.
6. Users must not attempt to compromise, disrupt, or interfere with ICT systems, network communications, or organizational services.
7. Unauthorized network monitoring, vulnerability scanning, port scanning, or security testing is prohibited unless expressly approved by authorized ICT personnel.
8. Circumventing authentication controls, access restrictions, or security mechanisms on any device, account, application, or network is prohibited.
9. Users must not run unauthorized scripts, programs, commands, or send disruptive messages intended to interfere with, disable, or disrupt systems, devices, services, or another user's access.
10. Sharing confidential organizational, staff, beneficiary, donor, or partner information with unauthorized persons outside MPI is strictly prohibited without formal authorization.
11. Sending unsolicited bulk messages, spam, chain emails, or unauthorized promotional content using MPI systems is prohibited.
12. Personal blogging, publishing, or posting using MPI systems, devices, or internet resources in a manner that may expose the organization to risk, misrepresentation, or reputational harm is prohibited unless expressly authorized. Limited and appropriate use may only be permitted with prior approval from MPI Management.

5.2 Technology Hardware and Software Acquisition

Overview

From time to time, Meeting Point International acquires ICT hardware and software to support its operations, service delivery, communication, and administrative functions. These acquisitions may include computers, laptops, printers, servers, networking equipment, communication tools, software applications, operating systems, cloud services, and other digital solutions.

Such investments often involve significant financial resources and are necessary to support operational efficiency, organizational growth, and changing technological needs. To ensure compatibility, scalability, security, and value for money, it is important to establish clear guidelines governing the acquisition of ICT hardware and software.

This section provides guidance for the acquisition of ICT hardware and software to ensure that all technology procured by MPI is appropriate, cost-effective, secure, and aligned with organizational needs. These guidelines also apply to donated ICT equipment, bundled software, pre-installed software, subscriptions, and digital tools acquired for operational use.

Procedures

1. All ICT procurement shall follow MPI's approved procurement policies and procedures.
2. All ICT vendors, suppliers, and service providers must meet MPI's procurement, technical, and compliance requirements.
3. The ICT function shall provide technical specifications and guidance for the acquisition of all ICT hardware and software.
4. No ICT equipment, whether procured or donated, shall be deployed or used before verification, inspection, and approval by the responsible ICT personnel.
5. All acquired ICT hardware and software must meet organizational standards for compatibility, security, maintainability, and operational suitability.
6. Procurement of ICT equipment and software must consider total cost of ownership, including maintenance, licensing, support, upgrades, and replacement costs.

5.3 MPI Management and Use of Software

Overview

This section provides guidelines for the MPI Management and use of software within Meeting Point International to ensure that all software used is appropriate, secure, licensed, and aligned with organizational needs. These guidelines apply to commercial software, subscription-based software, cloud applications, open-source software, freeware, and any other software used on MPI systems.

Procedures

1. All software used within MPI must comply with applicable copyright laws, licensing agreements, and software usage terms.
2. ICT personnel shall ensure that software licensing requirements are monitored and complied with.
3. Software audits shall be conducted periodically to ensure compliance with software licensing, registration, and usage requirements.
4. All software installed on MPI systems must be appropriately licensed, registered, and documented where required.
5. MPI shall remain the registered owner or authorized user of all software installed on its systems, where applicable.

6. Only software acquired, approved, and documented in accordance with this policy may be installed or used on MPI systems.
7. All software installations, upgrades, updates, and removals shall be carried out or approved by authorized ICT personnel.
8. Software upgrades may only be installed where the original licensed software version exists and upgrade requirements are met.

5.3.1 Software Usage

Only software acquired and approved in accordance with this policy may be used within MPI.

Users must receive guidance on software licensing conditions, permitted use, and applicable restrictions before using software.

Users shall receive appropriate training for newly introduced software and systems to ensure proper and secure use.

Software may not be installed on personal devices for official work unless expressly approved by authorized ICT personnel and MPI Management.

Where official work requires software on a personal device, prior approval must be obtained and licensing, security, and ownership conditions must be documented and approved.

Any software purchased for authorized use on personal devices for official work remains the property of MPI and must be recorded in the software register.

5.3.2 Breach of Software Guidelines

Unauthorized software is strictly prohibited on MPI systems and devices. This includes privately owned, unlicensed, unapproved, or unsupported software used on MPI ICT infrastructure.

Unauthorized copying, duplication, installation, distribution, or use of software is prohibited and may result in disciplinary action.

Any user found installing, distributing, or using unauthorized software may be subject to disciplinary action in accordance with organizational policy.

Any user who becomes aware of unauthorized software use or a breach of this policy must report it immediately to the responsible ICT personnel or MPI Management.

Failure to report known software misuse or policy violations may result in disciplinary action.

5.4 Bring Your Own Device (BYOD)

Overview

Meeting Point International recognizes the growing importance of mobile technologies in improving communication, flexibility, and productivity in the workplace. Staff may, where authorized by the MPI Management, use personally owned devices such as laptops, tablets, and mobile phones to access organizational systems, data, and communication platforms for official work purposes.

This section provides guidelines for the secure and responsible use of personally owned devices for official business. These guidelines apply to all employees, interns, volunteers, consultants, contractors, suppliers, and other authorized users who use personal devices to access MPI systems, networks, or information.

Procedures

Each user who uses a personal device for official work must agree to the following conditions:

1. All personal devices used for official work must be registered and approved before use, including any applications used to access MPI systems or data.

2. Users must not store, download, or transfer sensitive organizational information to personal devices unless expressly authorized and protected by approved security controls. Sensitive information includes beneficiary records, financial information, donor data, internal reports, contracts, and confidential organizational documents.
3. Users must take all reasonable precautions to ensure that organizational information is not exposed, compromised, or viewed by unauthorized persons, especially when using devices in public or shared spaces.
4. All registered personal devices must be protected with passwords, screen locks, and other approved security controls.
5. Personal devices used for official work must be maintained with current operating system updates, updated applications, anti-malware protection, and appropriate security settings.
6. Users must not share personal devices used for official work with unauthorized persons in a way that may expose organizational systems or data.
7. All users must comply with MPI's internet, acceptable use, and information security requirements when accessing organizational resources through personal devices.
8. Users must immediately report loss, theft, compromise, or unauthorized access involving a registered personal device used for official work.
9. Users must not connect untrusted USB drives, storage devices, or external accessories from unknown sources to MPI systems or networks.
10. All users who register personal devices for official business acknowledge that MPI:
 - Retains ownership of all official work, records, and organizational information created, stored, transmitted, or accessed on the device in the course of official duties.
 - May require access to official organizational data stored on the device where necessary for operational, legal, compliance, or security purposes.
 - May require official work data on such devices to be backed up in accordance with organizational data MPI Management requirements.
 - May remove, restrict, or delete organizational data from the device in the event of loss, theft, compromise, misuse, or security risk.
 - May revoke authorization for use of a personal device for official work at any time where security, compliance, or operational concerns arise.
 - May require the removal of all official organizational data from the device upon termination of employment, contract, or authorization.

5.4.1 Keeping Mobile Devices Secure

The following security measures must be observed when using mobile devices for official work:

1. Mobile devices must not be left unattended in public places, unsecured homes, shared workspaces, or motor vehicles. Wherever possible, devices should remain in the possession of the user or be securely locked away.
2. Additional physical protection measures, such as laptop locks or secure carrying cases, should be used where appropriate, especially in public or shared environments.
3. Mobile devices should be carried securely during travel and, where possible, kept as hand luggage when traveling.
4. Users must avoid accessing or displaying sensitive organizational information in public spaces where unauthorized persons may view it.
5. Devices used for official work must be protected against theft, physical damage, and unauthorized access at all times.
6. Once work activity is completed, mobile devices must be returned to the office and stored in a secure location as agreed with the respective supervisors.

5.4.2 Indemnity

Meeting Point International shall not be held responsible for personal loss, damage, or liability arising from the personal use of privately-owned devices used for official work.

Users remain personally responsible for unlawful, unauthorized, or improper use of their personal devices while accessing organizational systems or information.

Users shall be held accountable for any loss, damage, liability, or legal consequences arising from misuse, negligence, or non-compliance with this policy while using personal devices for official work.

Any legal or disciplinary action resulting from misuse of personal devices in connection with MPI business may proceed independently under applicable organizational policies and laws.

5.5 Security of Information Technology

Overview

Confidentiality, Integrity, and Availability (CIA) are the core principles of effective information security MPI Management. Meeting Point International recognizes that protecting information systems, digital infrastructure, and organizational data is essential to ensuring continuity, trust, accountability, and secure service delivery.

This section provides guidelines for protecting ICT assets, systems, and information resources to ensure that organizational data remains secure, accurate, available, and protected against unauthorized access, misuse, damage, loss, or disruption.

These requirements apply to all employees, interns, volunteers, consultants, contractors, and other authorized users who access or use MPI ICT systems, infrastructure, or information resources.

Procedures

Physical Security

1. All ICT infrastructure, including servers, routers, switches, network devices, and related equipment, must be physically secured against unauthorized access, theft, damage, and misuse.
2. ICT equipment must be kept in secure environments with appropriate physical safeguards, including controlled access and environmental protection.
3. Adequate ventilation, cooling, and protection from environmental hazards must be provided for ICT infrastructure and equipment.
4. Access to critical ICT infrastructure and equipment shall be restricted to authorized personnel only.
5. Users issued with portable ICT equipment, including laptops, tablets, and mobile devices, are responsible for the physical safety and security of those devices.
6. Portable ICT equipment kept in offices must be secured using available organizational security measures when not in use.

5.5.1 Information Security

Critical organizational data must be regularly backed up and securely stored in accordance with MPI data protection and backup requirements.

All devices connected to MPI systems or the internet must have approved and up-to-date anti-malware or endpoint protection installed where applicable.

Authorized ICT personnel are responsible for ensuring that security software is installed, maintained, monitored, and updated on organizational systems.

All information created, accessed, stored, or transmitted through MPI systems must comply with applicable privacy, confidentiality, and data protection requirements.

Unauthorized disclosure, misuse, alteration, or destruction of organizational information is prohibited and may result in disciplinary action.

5.5.2 Network Access

Access to MPI network infrastructure, systems, and services must be authorized by designated ICT personnel.

Access to network resources shall be restricted to official and authorized purposes only.

All Wi-Fi enabled devices accessing MPI systems must be secured with passwords and appropriate authentication controls.

All computers and connected devices must be secured physically and logically when unattended.

Devices connected to MPI networks must run up-to-date software, supported applications, and appropriate security protections, including firewall controls where applicable.

All network resources remain the property of Meeting Point International and may be monitored, restricted, or access-controlled for security, compliance, and operational purposes.

5.5.3 Technology Access

Every authorized user shall be assigned a unique user account or identification credential to access MPI systems and services, including network services, email, and other digital platforms.

Users shall be required to create and maintain secure passwords for access to organizational systems and services, and passwords must be changed periodically in accordance with ICT security requirements.

Passwords must meet minimum security standards, including appropriate length, complexity, and confidentiality, and must not be shared with any other person.

Authorized ICT personnel shall be responsible for issuing user credentials, granting system access, and managing account activation for all authorized users.

Where a user forgets a password, is locked out of an account, or experiences access issues, only authorized ICT personnel may reset credentials or restore access. Any temporary password issued must be changed immediately upon first login.

The following access levels shall apply unless otherwise authorized:

Technology / Service	Authorized Users
Desktop computers and laptops	Authorized MPI staff and approved users
Internet services (wired and wireless)	Authorized MPI staff and approved users
Servers, routers, switches, and network devices	Authorized ICT personnel only
Official email services	Authorized MPI staff and approved users
Shared systems and digital platforms	Authorized MPI users and external users based on assigned roles and permissions

Authorized ICT personnel shall be responsible for maintaining and periodically reviewing access procedures, permissions, and controls under this policy.

5.6 Business Continuity and Disaster Recovery

Overview

The Business Continuity and Disaster Recovery Policy provides a framework to ensure that critical organizational functions can continue or be restored in the event of disruption, disaster, or system failure. This includes identifying critical systems and data, establishing backup and recovery procedures, defining responsibilities, and ensuring that essential operations can continue during and after an incident.

This policy serves as an important safeguard against data loss, operational disruption, and service interruption arising from hardware failure, software failure, cyber incidents, human error, natural disasters, or other emergencies affecting ICT systems.

Procedures

Meeting Point International shall classify data and systems to identify critical information and services requiring backup, continuity, and recovery measures.

Backup schedules, retention periods, and offsite or alternative storage arrangements shall be implemented in accordance with approved data backup and records MPI Management requirements.

Backup storage locations and media shall be securely protected from unauthorized access, theft, damage, and environmental hazards such as heat, moisture, fire, and dust.

Critical organizational data shall be stored and backed up using approved technologies and secure storage methods appropriate to current operational and security requirements.

Data retention and archival practices shall comply with MPI records MPI Management and data retention requirements.

Critical systems and data shall be restored in accordance with documented disaster recovery and restoration procedures.

Disaster recovery procedures and related documentation shall be reviewed periodically and updated to reflect operational, technological, and organizational changes.

Backup data and restoration processes shall be tested regularly to ensure reliability, integrity, and readiness for recovery.

5.7 ICT Governance

Overview

Effective ICT governance provides the structure required to ensure that ICT investments, systems, and services are aligned with organizational priorities and managed in a way that delivers value, reduces risk, and supports operational effectiveness. Strong ICT governance helps ensure accountability, efficient resource use, sound decision-making, and effective oversight of ICT systems and investments across Meeting Point International.

ICT Oversight and Governance

MPI shall establish appropriate governance structures to guide ICT planning, oversight, implementation, and accountability.

5.7.1 MPI Management and Leadership Responsibilities

MPI Management shall provide oversight and strategic direction for ICT governance, including:

- Ensuring that ICT strategy aligns with organizational goals and operational priorities.
- Monitoring the quality, performance, and value of ICT initiatives and investments.
- Providing oversight and decision-making support on significant ICT changes, risks, and priorities.
- Supporting ICT planning, governance, and operational accountability across the organization.

5.7.2 ICT Function Responsibilities

The ICT function shall be responsible for the day-to-day coordination and MPI Management of ICT activities, including:

- Coordinating ICT planning and implementation in support of organizational needs and priorities.
- Supporting users to ensure effective and responsible use of ICT resources through user support and technical assistance.
- Developing and maintaining ICT systems, software and networks to support communication, collaboration, and operational efficiency.

- Protecting ICT infrastructure, systems, and organizational data from cyber threats, misuse, and operational risks.
- Supporting systems for the secure collection, storage, MPI Management, protection, and use of organizational data.
- Conducting periodic ICT reviews or audits to ensure compliance with ICT policies, standards, and controls.
- Managing ICT-related vendor relationships, service agreements, and technology support arrangements.

5.8 Official Email MPI Management and Use

Overview

Email is an essential tool for official communication and day-to-day operations at Meeting Point International. However, improper use of email may expose the organization to operational, legal, and security risks. This section provides guidance on the secure, appropriate, and responsible use of official email systems. This policy applies to all employees, interns, volunteers, consultants, contractors, and other authorized users who access or use MPI official email services.

Procedures

All authorized users shall be provided with official email accounts for official communication where required by their role.

Personal email accounts shall not be used for official organizational communication unless expressly authorized.

Email account credentials must not be shared.

All official email accounts must be protected using secure passwords and appropriate authentication controls.

Official emails, records, and communications created or transmitted through MPI email systems remain organizational property and may be monitored in accordance with applicable policies and legal requirements.

Users must not open suspicious attachments, links, or messages received from unknown, unverified, or untrusted senders.

Misuse of official email systems may result in restriction of access, disciplinary action, or other appropriate measures.

5.9 Data and Information MPI Management

Overview

This section provides guidance on the generation, collection, storage, protection, access, use, retention, and sharing of data and information created, received, processed, or held by Meeting Point International.

All organizational data and information, regardless of format or storage medium, are organizational assets and must be managed responsibly to ensure security, accessibility, integrity, confidentiality, and compliance.

Procedures

All data and information generated, received, processed, or stored in the course of organizational work remain the property of Meeting Point International.

Departments, units, and designated custodians responsible for processing or managing data shall ensure that information is properly organized, stored, maintained, and made accessible for authorized

use. Data and information shall only be accessed, used, shared, or disclosed by authorized persons for legitimate organizational purposes.

Authorized personnel responsible for ICT and data MPI Management shall ensure proper administration, protection, storage, and control of electronic information systems and records.

All data handling must comply with applicable privacy, confidentiality, records MPI Management, and data protection requirements.

5.10 Website and Digital Platforms - MPI Management

Overview

Meeting Point International uses its website and digital platforms as important public communication channels for sharing information, organizational visibility, stakeholder engagement, and access to public-facing content.

This section provides guidelines for the hosting, administration, maintenance, security, and updating of MPI websites and digital platforms.

Procedures

MPI shall maintain a website register managed by designated responsible personnel, which shall include:

- A list of all domain names registered to MPI.
- Domain registration and renewal dates.
- A list of hosting service providers.
- Hosting subscription and renewal dates.
- Security certificate and digital security information.
- Administrative and technical ownership records for all websites and digital platforms.

Website Content

All content published on Meeting Point International websites and digital platforms must be accurate, relevant, appropriate, and up to date.

Responsibility for content quality, relevance, and accuracy shall rest with the designated communications function or authorized content owners.

All website content must be reviewed and approved by authorized personnel before publication.

Website content shall be reviewed regularly to ensure continued accuracy, relevance, and alignment with organizational priorities.

All website content must comply with MPI branding, communication, and visual identity standards to ensure a consistent and professional organizational image.

Technical changes, updates, and administrative modifications to the website shall be managed by authorized ICT or designated digital administrators in a secure and controlled manner.

5.11 MPI Management of ICT Service Agreements

Overview

For the purpose of this policy, an ICT Service Agreement refers to any formal arrangement between Meeting Point International and a service provider for the delivery, support, maintenance, or MPI Management of ICT-related products or services. Such agreements define service expectations, responsibilities, quality standards, support arrangements, and accountability obligations between MPI and the service provider.

This section provides guidance for the MPI Management of all ICT service agreements entered into on behalf of MPI.

ICT service agreements may include, but are not limited to:

- Provision of ICT equipment and related services
- Supply and support of network hardware and software
- Repair and maintenance of ICT equipment
- Provision of software, subscriptions, and digital systems
- Website design, hosting, maintenance, and support
- Cloud services, communication tools, and managed ICT services

Procedures

All ICT service agreements shall be reviewed first of all by the ICT responsible and then by the appropriate authorized personnel, including procurement, MPI Management, and where necessary legal review, before approval or execution.

All ICT service agreements must be approved in accordance with MPI's procurement and authorization procedures.

All ICT service agreements, obligations, service terms, support conditions, and renewal dates shall be documented and maintained in accordance with MPI records MPI Management requirements.

ICT service agreements shall clearly define service scope, responsibilities, performance expectations, security obligations, support arrangements, and escalation procedures.

ICT vendors and service providers must comply with MPI's applicable ICT, confidentiality, data protection, and security requirements.

5.12 Emergency MPI Management of Information Technology

Overview

For the purpose of this policy, ICT emergencies include incidents or disruptions that affect the availability, integrity, confidentiality, or functionality of ICT systems and services. These may include:

- Internet service failure
- Email service failure
- ICT hardware failure
- Malware infection or other security breach
- Website disruption or service outage
- Loss of critical data
- Network failure or system unavailability

This section provides guidelines for the MPI Management of ICT-related emergencies to ensure timely response, minimize disruption, and restore critical operations as quickly as possible.

Procedures

All ICT failures, incidents, disruptions, and security events must be reported immediately to the designated ICT responsible for prompt assessment and response.

Authorized ICT responsible shall take immediate action to assess, contain, resolve, and recover from ICT incidents in order to minimize operational disruption.

ICT emergency response procedures shall be documented, maintained, and periodically tested to ensure effectiveness and readiness.

Significant ICT incidents shall be documented, reviewed, and escalated to MPI Management where necessary.

Appropriate corrective and preventive actions shall be taken following ICT incidents to reduce recurrence and improve resilience.

5.13 Use of Social Media

Overview

Social media includes digital platforms and online communication tools used to share information, engage audiences, and communicate with the public. For Meeting Point International, social media is an important communication channel for public engagement, visibility, awareness, stakeholder communication, and organizational representation.

This section provides guidance on the responsible, appropriate, and secure use of social media in support of MPI's communication objectives.

Procedures

Information shared through official social media channels must be accurate, credible, appropriate, and aligned with MPI's communication standards.

Content published on official social media platforms must be professional, respectful, factual, and consistent with organizational values, policies, and communication objectives.

Only authorized MPI personnel may access or manage official MPI social media accounts as part of their assigned responsibilities.

Staff must not publish personal opinions, unauthorized statements, or unofficial views on official organizational social media accounts.

Confidential, sensitive, misleading, offensive, or inappropriate content must not be published through official social media channels.

Official social media use must comply with applicable legal, privacy, safeguarding, and organizational communication requirements.

6. IMPLEMENTATION STRATEGY

This policy shall be implemented through the development, approval, and use of supporting procedures, standards, manuals, and operational guidelines in the relevant policy areas.

The designated ICT personnel, supported by MP Management, shall be responsible for coordinating implementation, monitoring compliance, and supporting the effective application of this policy across the organization.

The ICT function shall ensure organization-wide awareness, communication, training, and sensitization on this policy and its requirements.

Compliance with this policy shall be monitored regularly, and appropriate corrective or disciplinary action shall be taken where violations occur.

All users of MPI ICT resources are responsible for complying with this policy and supporting its effective implementation.

7. MONITORING AND EVALUATION

Achievement of the objectives of this policy shall require regular monitoring, review, and evaluation of implementation, compliance, performance, and outcomes.

The ICT responsible, supported by MPI Management, shall provide oversight for monitoring and evaluating the implementation of this policy and related ICT initiatives.

Periodic reviews shall be conducted to assess ICT performance, policy compliance, operational effectiveness, and emerging risks.

A monitoring and evaluation framework shall be developed to guide implementation tracking, compliance monitoring, and policy performance assessment.

This policy shall be reviewed periodically to ensure continued relevance, effectiveness, and alignment with technological developments, organizational priorities, and operational needs.

A formal policy review shall be conducted at least every three (3) years, or earlier where necessary, to reflect significant changes in technology, risk, legal requirements, or organizational operations.

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY ACKNOWLEDGMENT AND ACCEPTANCE FORM

I, (Full Name)
..... (Position/Role/Organization if applicable),
acknowledge receipt of the Meeting Point International (MPI)'s Information and Communication
Technology Policy.

I confirm that I have read, understood, and accepted the Child Protection Policy as part of my
employment, collaboration, volunteer service, consultancy, partnership, or engagement with Meeting
Point International (MPI).

Name : _____
Signature : _____
Date : _____

A copy of the signed Information and Communication Technology Policy should be returned to the
Administration office or to this email: admin@meetingpoint-int.org