MANEPO IT SERVICES POLICY

Title	MANEPO IT Services Policy
Document type	Policy
SOP point of contact	IT Focal Person, Clement Lefu
Date of issue	12/09/2018

Introduction

MANEPO provides its employees with IT Services for reasons of efficiency and to enable programme related issues update in terms of recent innovations and way of doing things. This document outlines the current policies, procedures and guidelines to assist in using the facilities provided in an effective manner.

A Policy: In the IT Services area, policies point to specific area of focus. For example, an "acceptable use" policy would cover the rules and regulations for appropriate use of the Services provided by IT.

A Procedure: a standard which is usually a collection of system/procedure specific requirements that must be met by everyone. For example, the Service Provision Standard details what must be done when a new person joins MANEPO.

A Guideline: This is a practice. It is typically a collection of system specific or procedural specific suggestions for best practice.

The IT Manager will review the Policies, Procedures and Guidelines annually, or flowing a significant change, in order to take advantage of the current best practice. The benefits to be gained from implementation of best practice in service management include:

Employees and IT

The HR and Administration Manager has the responsibility to keep the IT department updated in regard to new staff, leaving staff or changes in staff roles that will have an impact on the level of access they may be given.

Staff - Leavers and New Starters

When new staff join MANEPO, it is the responsibility of the HR and Administration Manager to inform IT department in good time to ensure that they are set up in time for their first day of working. Whilst urgent requests will be facilitated where possible, short term notice may mean access to systems or equipment is not ready for new starters.

It is **ESSENTIAL** that it is completed and sent to the IT help desk two weeks before the employee is due to start.

Should the role require them to have access to two accounts such as IT help desk and personal email, the two accounts can be linked so that all the same permissions and files are available. IT department must be notified of this when account is requested to avoid any delays in access.

When a staff is to leave MANEPO, it is the responsibility of the HR and Administration Manager to ensure that IT department is made aware of any arrangements that are put in place around IT requirements. Due to data protection, accounts will be closed on departure unless previously agreed with the IT department. The IT department can change passwords and add account onto a manager, or their delegated staff member, for monitoring. If this is not requested the account will be closed. It is **ESSENTIAL** that MANEPO's IT service providers are informed of leavers at least two weeks in advance before they leave.

It is a serious data protection and potential security issue if non-staff members are able to access MANEPO systems after they have left the organization.

IT Induction and Training

All new staff must have a brief IT induction on joining MANEPO carried out by a member of the IT department. Line managers should contact the IT Department to arrange an induction.

The induction will provide a brief overview of the IT systems available and ensure that all access has been set up and is functioning as requested. Due to the constant evolving environment and developments within IT systems, staff can request additional training at any stage. This can be arranged via ITdepartment@manepo.org/info@manepo.org

Provision of IT Equipment

To support staff in to carry out their duties, it is possible to have equipment including mobile phones and laptops loaned on fixed term basis or, if the role requires it and there is the budget in the staff member's department, purchased for the position.

Whether staff are loaned or allocated equipment they are expected to take reasonable care of the equipment. Loss or damage of equipment must be reported to the IT department/HR and Administration Manager straight away. IT equipment remains the property of MANEPO at all times and must be relinquished on request and / or at the termination of contract. This

equipment is to be used solely by MANEPO employees and must only be used in the daily execution of MANEPO business, unless otherwise approved by the **Executive Director** in writing

Under no circumstances must employees allow non-employees to use systems, access data on the systems, or make copies of this data for external use. Employees who have been issued MANEPO equipment, such as laptops, temporarily or permanently, should take every reasonable precaution to maintain the safety and functionality of the equipment while it is in their care. The equipment should be kept in a protective case or bag where these are provided, it should be kept dry and clean and not stored in places where extremes of temperature or humidity occur

When the equipment is taken away from the office, reasonable care must be taken to minimize the risks of theft and loss or accidental damage. Under no circumstances must laptops or laptop bags be left in open view on a car seat- they must always be locked away in the boot. The equipment supplied by MANEPO is solely for use by MANEPO staff and the system and its contents are the employee's responsibility should inappropriate content be found.

When left in the office, it is an insurance requirement that laptops must be locked away at night.

Permanent allocation

MANEPO IT department is able to purchase equipment for staff subject to line manager /budget holder approval; any equipment purchased for departments will be cross charged back to the department

When requesting IT equipment, a minimum of 2 weeks' notice is required, it may take longer to purchase laptops and ensure they are configured. If equipment is required for a specific date, please inform IT department at the time of the request. Should it not be possible to provide equipment by date required temporary equipment will be provided.

Temporary allocation

The IT department does hold a small supply of IT equipment, including laptops. IT equipment is loaded on a first come first served basis. All requests for temporary loan must provide the following information:

- Who the equipment is for?
- Length of time required for (based on return time the next loan may be agreed so please ensure equipment is returned on time)
- Reason for loan (e.g. travel aboard, meeting)

On return of the equipment to the IT department, to support future users experience, any issues or damage to equipment must be reported. Any information stored on the equipment loaned will be deleted on return to the IT department for data protection requirements. Staff members should ensure that they have copies of all information required before equipment is returned.

Bring your own device to work (BYOD)

"Bring Your Own Device" (BYOD) refers to organizations permitting staff/device owners to bring personally owned mobile devices (e.g. tablets and smart phones) to their workplace and use those devices to access organizational information and applications.

BYOD usage principals at MANEPO

MANEPO allows employees to use their own equipment including, smartphones, tablets and laptops for their convenience to facilitate remote working or in the office environment. It is important with BYOD that the security and integrity of MANEPO data and technology infrastructure is maintained, a separate policy will provide more detail on BYOD. Limited exceptions to the policy may occur due to variations in devices and platforms.

To access MANEPO IT services on your own devices you must ensure you have an anti-virus product of a suitable quality that is up to date and that your device has sufficient security installed and setup (i.e., screen saver lock or equivalent).

Inadequate security puts MANEPO data at risk, as such staff members are responsible for ensuring that their devices have the appropriate security levels on it. Any member of staff who is unsure if their equipment has the appropriate security level must confirm with IT department before downloading or using organizational systems.

BYOD and staff responsibilities

All relevant polices still apply when staff are working in a BYOD way, in addition to this, individuals must take responsibility for their own device and they use it. They must:

- Familiarise themselves with their own device and its security features so that they can ensure the safety of MANEPO information
- Ensure all relevant and required security features are in place to maintain the integrity of data
- Prevent theft of equipment and loss of date
- Take responsibility for any software they download to their device
- Maintain the device to ensure it is regularly patched and upgraded
- Ensure that the device that is not used for any purpose that would be at odds with any of MANEPO data protection policies
- Set up passwords or equivalent and a sufficient length and complexity for the particular type of device
- Not hold any information that is sensitive on personally owned devices, all information should be saved in the Citrix environment
- Where it is essential, due to access issues etc, that information is stored temporarily on a personal device this should be deleted as soon as it no longer required, or it is possible to save within the Citrix environment
- Report the loss of any device containing MANEPO data to the IT department
- Beware of any data protection issues and ensure personal data is handled appropriately
- Report any security break immediately to the IT department

Whilst IT department will always endeavor to assist staff whereever possible, MANEPO cannot take any responsibility for supporting devices it does not provide.

A breach of any clause in this policy may result in being found in breach of the Code of Conduct and punishable through summary dismissal and prosecution, where the issue is serious.

IT Applications

MANEPO provides employees who need IT Services with a common set of applications.

Microsoft

Office 365 is the brand name used by Microsoft for a group of software plus services subscriptions that provides productivity software and related services to its subscribers. For consumers, the service allows the use of Microsoft Office apps on Windows and OS X, provides storage space on Microsoft's cloud storage service OneDrive.

Working area	**Shared Drives**
Human Resources	HR (HR Only)
Finance	Finance (Finance only)

Working area	**Applications**
All Staff	Email (Outlook)

General IT Policies

Security

Data protection and IT security is essential for MANEPO. All staff accessing the IT systems are required to ensure they are supporting the safety and compliance of the systems they are using. Staff members who are not using the systems appropriately may become subject to HR investigation and have their access limited or revoked.

Un-authorized Use

MANEPO will not tolerate the use of email, Internet or any other IT systems for any of the following:

- Sending messages from somebody else's mailbox and purporting to be that person.
- Sending abusive or personally insulting messages (unacceptable via any medium).
- Accessing or attempting to access somebody else's messages or data without their consent.
- Downloading of inappropriate material from the Web.
- Publishing offensive, defamatory, racist, or abusive material on the Intranet, MANEPO's website and social networks groups, such as: Facebook, Myspace, Instagram.

Software

The systems come with specific applications loaded on them. Employees must not replace existing or load additional applications onto the machines without approval from IT department.

Any third-party data loaded onto the systems must be undertaken by the IT department. Application owners are responsible for purchasing and maintaining licence agreements for specialist applications and keeping the IT department informed.

Anti-virus

A good anti-virus product should be chosen for the organization which can protect against all types of computer and network attacks. A centralized server- based antivirus system is suggested for an organization with a computer network. This is important as new and more potent viruses are discovered every day

Procurement and Licensing Policy

Introduction

In normal circumstances, all IT purchases including equipment, software and consumables must be through the procurement team.

Hardware

All Hardware purchases must conform to the current purchasing criteria. By minimising the variations on equipment, we can maximise both our purchasing discounts and provide a quality level of support. The IT Manager is responsible for deciding the most appropriate suppliers and product specifications.

Software

MANEPO's policy is to use Microsoft software wherever practical.

Email and Internet Policy

The Email and Internet Policy applies to all employees of MANEPO who have access to computers and the Internet to be used in the performance of their work. Use of the Internet by employees is permitted and encouraged where such use supports the goals and objectives of MANEPO. However, access to the Internet is a privilege and all employees must adhere to the policies concerning Computer, Email and Internet usage.

Violation of these policies could result in disciplinary and/or legal action leading up to and including termination of employment. Reasonable personal use is acceptable in the employee's own time; this includes lunch hours. Consideration should be given on the bandwidth of internet usage and the impact on organizational activity.

Monitoring of Web Usage

Every employee should be aware that the use of Internet/Intranet and e-mail maybe be monitored by MANEPO IT department for security and network related reasons. All data entering or leaving MANEPO is scanned for objectionable content and where found is blocked. Limitations may be placed where excessive usage is determined or where usage which otherwise affects the wider MANEPO network is determined.

The following uses of e-mail or access to the Internet are deemed unacceptable:

- The unreasonable use of e-mail or the Internet for a purpose not directly related to your job.
- Viewing, storing or distributing any material which can be construed as pornographic, offensive, abusive or likely to cause offence, including jokes.
- Viewing, storing or distributing any form of illegal material, or any material or data that could be linked to illegal practices.
- Storing, copying, running or playing computer games.
- Transferring any MANEPO data or information to third parties without the explicit permission of a line manager and then only for legitimate business needs.
- Misuse of the Internet or email may result in disciplinary action.

Messages

Normal standards of confidentiality, etiquette and privacy should be observed by all users (as per telephones and post).

This is business email and MANEPO Managers may access at any time e.g. during absence. Email for staff who have left can be automatically forwarded to their line manager for work continuity purposes for a short period.

Security of email

Your password is your own “key” to security and as such you should not disclose it to anyone. If you suspect that your password is known to another member of staff (unless you specifically requested them to check your mailbox), you should change your password.

If you forget your password, contact IT department who will allocate a new password. You are advised to change this to one of your own choice as soon as possible.
It must be noted that if you print electronic mail messages, there is a risk that other staff that use the printer may pick up the message and read it.

Email Sent or Received

Care must be taken when making statements about other people or companies. Copyright laws also apply. You must, therefore, not use articles, logos or other materials without permission of the person or company who sent it to you.

Personal Use of MANEPO IT Equipment

The Policy

MANEPO recognizes that employees may wish to use the IT facilities for their own purposes out of work hours. Reasonable personal use is deemed acceptable and does not result in a cost to the Organization. Reasonable use must not result in any changes to the IT equipment or software.

Examples of unreasonable use may include:

- Installing additional software on the computer, including downloaded applications from the Internet.

DISCIPLINARY ACTION

All employees, volunteers, interns and trustees should abide by the IT Policy and its guide.

The IT Department is allowed to monitor employees' computer, emails and access to the Internet without pre-authorization. Violations of this policy should be reported to the HR and Administration Manager for further action.