Information Technology Policy Manual

Introduction

FAME foundation IT Policy provides the policies and procedures for selection and use of IT within the organization which must be adhered to by all staff. It also provides guidelines that FAME foundation will employ to administer these policies, with the appropriate procedure to follow. FAME foundation will keep all IT policies current and relevant. Therefore, some sections of the policies and procedures will be reviewed and modified frequently. New policies will also be added if necessary.

Any suggestions, recommendations or feedback on the policies contained in this manual are welcome. These policies are binding on all employees.

Technology Hardware Purchasing Policy

Policy Number: {001}

Policy Date: {27-04-2017}

Computer hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and RAM. External hardware devices include monitors, keyboards, mice, printers, and scanners.

Purpose of the Policy

This policy provides guidelines for the purchase of hardware for the business to ensure that all hardware technology for the business is appropriate, value for money and where applicable integrates with other technology for the business. The objective of this policy is to ensure that there is minimum diversity of hardware within the business.

Procedures

Purchase of Hardware

The purchase of all desktops, servers, portable computers, computer peripherals and mobile devices must adhere to this policy.

Purchasing desktop computer systems

The desktop computer systems purchased must run at least a Windows 7 and integrate with existing organizational hardware.

The desktop computer systems must be purchased as standard desktop system bundle and must be HP and Dell.

The desktop computer system bundle must include:

Desktop tower

Desktop screen of 1920*1080

- Keyboard and mouse must be wireless

- Windows 8, and Office 2007
- Speakers, microphone, camera, printers, projectors, etc.}

The minimum capacity of the desktop must be:

- At least 3.5 GHz (gigahertz)
- At least 4 GB RAM}
- At least 3 USB ports }

Any change from the above requirements must be authorised by the IT manager.

All purchases of desktops must be supported by the Executive Directors and be compatible with the organization's server system.

All purchases for desktops must be in line with the purchasing policy in the financial policies manual.

Purchasing portable computer systems

The purchase of portable computer systems includes; notebooks, laptops, tablets and so on.

Portable computer systems purchased must run at least a Windows 7 and integrate with existing hardware of the organization.

The portable computer systems purchased must be HP or Dell.

The minimum capacity of the portable computer system must be:

- At least 3.5 GHz –gigahertz.
- At least 4 GB RAM.
- At least 4 USB ports.

The portable computer system must include the following software provided:

- At least Office 2007, Adobe, Reader, Internet Explorer}

Any change from the above requirements must be authorised by the IT manager. All purchases of all portable computer systems must be supported by the Executive Director and be compatible with the organization's server system.

All purchases for portable computer systems must be in line with the purchasing policy in the financial policies manual.

Purchasing server systems

Server systems can only be purchased by IT manager. Server systems purchased must be compatible with all other computer hardware in the organization. All purchases of server systems must be supported by the Executive Director and be compatible with the organization's server systems. Any change from the above requirements must be authorised by the IT manager. All purchases for server systems must be in line with the purchasing policy in the financial policies manual.

Purchasing computer peripherals

Computer system peripherals include printers, scanners, and external hard drives amongst others. Computer peripherals can only be purchased where they are not included in any hardware purchase or are considered to be an additional requirement to existing peripherals. Computer peripherals purchased must be compatible with all other computer hardware and software in the organization.

The purchase of computer peripherals can only be authorised by the IT manager. All purchases of computer peripherals must be supported by the Executive Director and be compatible with the organization's hardware and software systems. Any change from the above requirements must be authorised by the Executive Director.

Purchasing mobile telephones

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

- The mobile phone must be compatible with the organization's current hardware and software systems. The mobile phone purchased must be Oppo, Tecno, Samsung, etc.
- The request for accessories must be included as part of the initial request for a phone.

- The purchase of a mobile phone must be approved by the Finance office prior to purchase.
- Any change from the above requirements must be authorised by the Executive Director.
- All purchases of all mobile phones must be supported by the Executive Director.
- All purchases for mobile phones must be in line with the purchasing policy in the financial policies manual.

Policy for Getting Software

Policy Number: {002}

Policy Date: {07/05/2021}

Purpose of the Policy

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

Procedures

Request for Software

All software, including open source, freeware, must be approved by the IT manager prior to the use or download of such software.

Purchase of software

- The purchase of all software must adhere to this policy.
- All purchased software must be purchased by the IT manager.
- All purchased software must be purchased from Adobe, Oracle and Microsoft.
- All purchases of software must be supported by the finance officer and be compatible with the organization's server and/or hardware system.
- Any changes from the above requirements must be authorised by{insert relevant job title here}
- All purchases for software must be in line with the purchasing policy in the Financial policies manual.

Obtaining Open Source or Freeware software

- Open source or freeware software can be obtained without payment and usually downloaded directly from the internet.
- In the event that open source or freeware software is required, approval from the IT manager must be obtained prior to the download or use of such software.
- All open source or freeware must be compatible with the business's hardware and software systems.

Any change from the above requirements must be authorised by the Executive Director.

Policy for Use of Software

Policy Number: 003

Policy Date: 27/06/2021

Purpose of the Policy

This policy provides guidelines for the use of software for all employees within the organization to ensure that all software use is appropriate.

Procedures

Software Licensing

All computer software copyrights and terms of all software licenses will be followed by all employees of the organizations.

Where licensing states limited usage, then it is the responsibility of the IT manager to ensure these terms are followed. The IT manager is also responsible for completing a software audit of all hardware twice a year to ensure that software copyrights and licence agreements are adhered to.

Software Installation

All software must be appropriately registered with Adobe, Oracle or Microsoft when necessary. Only software obtained in accordance with the getting software policy is to be installed on the business's computers. All software installation is to be carried out by the IT manager. A software upgrade shall not be installed on a computer that does not already have a copy of the original version of the software loaded on it.

Software Usage

Only software purchased in accordance with the getting software policy is to be used within the organization. Prior to the use of any software, the employee must receive instructions on any licensing agreements relating to the software, including any restrictions on use of the software.

All employees must receive training for all new software. This includes the training of new employees on the use of existing software appropriately. This will be the responsibility of the IT manager. Employees are prohibited from bringing software from home and loading it onto the organization's computer hardware. Unless express approval from Executive Director is obtained, software cannot be taken home and loaded on a employees' home computer.

Where an employee is required to use software at home, an evaluation of providing the employee with a portable computer should be undertaken in the first instance. Where it is found that software can be used on the employee's home computer, authorisation from the finance officer 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 organization and must be recorded on the software register by the Administrative officer.

Unauthorised software is prohibited from being used in the organization. This includes the use of software owned by an employee and used within the organization. The unauthorised duplicating, acquiring or use of software copies is prohibited. Any employee, who makes, acquires, or uses unauthorised copies of software will be referred to the Executive Director for consequences of his or her action. The illegal duplication of software or other copyrighted works is not condoned within this organization and the Executive Director is authorised to undertake disciplinary action where such event occurs.

Breach of Policy

Where there is a breach of this policy by an employee, that employee will be referred to the Executive Director for reprimand action etc. Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify the Operations Manager immediately. In the event that the breach is not reported and it is determined that an employee failed to report the breach, then that employee will be referred to the Executive Director for reprimand action etc.

Personal Device Policy

Policy Number: 004

Policy Date: 5/07/2021

At FAME foundation, we acknowledge the importance of mobile technologies in improving business communication and productivity. In addition to the increased use of mobile devices, the staffs have requested the option of connecting their own mobile devices to FAME foundation's network and equipment. We encourage you to read this document in full and to act upon the recommendations. This policy should be read and carried out by all staff.

Purpose of the Policy

This policy provides guidelines for the use of personally owned notebooks, smart phones and tablets to promote the organization's objectives. All staff who use or access technology equipment or services are bound by the conditions of this policy.

Procedures

Current mobile devices approved for organization's use

The following personally owned mobile devices are approved to be used for the purpose of achieving the organization's objectives:

- Notebooks, smart phones, tablets, removable media manufactured by Samsung, Apple, Oppo, Tecno and virus-free.

Registration of personal mobile devices for organization's use

Employees when using personal devices for organization's use will register the device with the Administrative Officer. The Administrative Officer will record the device and all applications used by the device. Personal mobile devices can only be used for the following purposes in the organization:

- Email access, business internet access, business telephone calls etc.}

Each employee who utilises personal mobile devices agrees:

- Not to download or transfer the organization or personal sensitive information to the device.
- Not to use the registered mobile device as the sole repository for FAME foundation's information. All business information stored on mobile devices should be backed up.
- To make every reasonable effort to ensure that FAME foundation's information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorised persons and all registered devices should be password protected
- Not to share the device with other individuals to protect the business data access through the device
- To abide by FAME foundation's internet policy for appropriate use and access of internet sites etc.
- To notify FAME foundation immediately in the event of loss or theft of the registered device
- Not to connect USB memory sticks from an unverified or unknown source to FAME foundation's equipment.

All employees who have a registered personal mobile device for the use of the organization acknowledge that the business:

- Owns all intellectual property created on the device
- Can access all data held on the device, including personal data
- Will regularly back-up data held on the device
- Will delete all data held on the device in the event of loss or theft of the device

- Has the first right to buy the device where the employee wants to sell the device
- Will delete all data held on the device upon termination of the employee. The terminated employee can request personal data be reinstated from back up data
- Has the right to deregister the device for the use of the organization at any time.

Keeping mobile devices secure

The following must be observed when handling mobile computing devices (such as notebooks and tablets):

- Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away
- Cable locking devices should also be considered for use with laptop computers in public places, e.g. in a seminar or conference, even when the laptop is attended
- Mobile devices should be carried as hand luggage when travelling by aircraft.

Exemptions

This policy is mandatory unless the Operations manager/Executive Director grants an exemption. Any requests for exemptions from any of these directives should be referred to the Admin Officer.

Breach of this policy

Any breach of this policy will be referred to the Operations manager who will review the breach and determine adequate consequences, which can include the confiscation of the device or termination of employment.

Indemnity

FAME foundation bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of staff in accessing or using these resources or facilities. All staff indemnifies FAME foundation against any and all damages, costs and expenses suffered by the organization arising out of any unlawful or improper conduct and activity, and in respect of any

action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by the organization.

Information Technology Security Policy

Policy Number: 005

Policy Date: 26/08/2021

Purpose of the Policy

This policy provides guidelines for the protection and use of information technology assets and resources within the business to ensure integrity, confidentiality and availability of data and assets.

Procedures

Physical Security

For all servers, mainframes and other network assets, the area must be secured with adequate ventilation and appropriate access through secured lock.

It will be the responsibility of the Administrative Officer to ensure that this requirement is followed at all times. Any employee becoming aware of a breach to this security requirement is obliged to notify the Chief Security Officer immediately.

All security and safety of all portable technology, such as laptop, notepads, and tablets will be the responsibility of the employee who has been issued with the devices. Each employee is required to use passwords to protect the information on the device and to ensure the asset is kept safely at all times to protect the security of the asset issued to them.

In the event of loss or damage, the Operations Manager will assess the security measures undertaken to determine if the employee will be required to reimburse the business for the loss or damage.

All laptops, notepads, and tablets, when kept at the office desk are to be secured by passwords provided by the Operations Manager.

Information Security

All sensitive and valuable data belonging to the organization must be backed up. It is the responsibility of the Operations manager to ensure that data back-ups are conducted twice daily and the backed up data is kept in the bank.

All technology that has internet access must have anti-virus software installed on them. It is the responsibility of the IT manager to install all anti-virus software and ensure that this software remains up to date on all technology used by the business.

All information used within the business is to adhere to the privacy laws and the business's confidentiality requirements. Any employee breaching this will be reprimanded adequately.

Technology Access

Every employee will be issued with a unique identification code to access the organization's technology and will be required to set a password for access every 24 hrs.

Each password is to be at least 12 characters with a combination of alphanumeric characters and not to be shared with any employee within the organization.

The Administration Officer is responsible for the issuing of the identification code and initial password for all employees.

Where an employee forgets the password or is 'locked out' after three attempts, then the Operations Manager is authorised to reissue a new initial password that will be required to be changed when the employee logs in using the new initial password.

It is the responsibility of the Operations manager to keep all procedures for this policy up to date.

Information Technology Administration Policy

Policy Number: 006

Policy Date: 5/07/2021

Purpose of the Policy

This policy provides guidelines for the administration of information technology assets and resources within the organization.

Procedures

All software installed and the license information must be registered on the IT excel sheet. It is the responsibility of the Administrative Officer to ensure that this registered information is managed appropriately. The register must record the following information:

- What software is installed on every technology.
- What license agreements are in place for each software packages.
- Renewal dates if applicable.

The IT manager is responsible for the maintenance and management of all service agreements for the business technology. Any service requirements must first be approved by the Operations manager.

The Administrative Officer is responsible for maintaining adequate technology spare parts and other requirements including toners and printing paper etc.

A technology audit is to be conducted annually by the IT Manager to ensure that all information technology policies are being adhered to. Any unspecified technology administration requirements should be directed to the IT manager.

Website Policy

Policy Number: 006

Policy Date: 07/08/2021

Purpose of the Policy

This policy provides guidelines for the maintenance of all relevant technology issues related to the website of the organization.

Procedures

Website Register

The website register must record the following details:

- List of domain names registered to the organization.
- Dates of renewal for domain names.
- List of hosting service providers.
- Expiry dates of hosting.

The reviewing of the register as well as the renewal of items listed in the register will be the responsibility of the Administrative Officer.

Website Content

All content on the website of the organization is to be accurate, appropriate and current. This will be the responsibility of the IT officer. All content on the website must follow the content guide.

The content of the website is to be reviewed monthly. The following persons are authorised to make changes to the organization's website:

- Programme Manager
- Operations Manager

- IT Officer

Basic branding guidelines must be followed on websites to ensure a consistent and cohesive image for the organization.

Electronic Transactions Policy

Policy Number: 007

Policy Date: 13/06/2021

Purpose of the Policy

This policy provides guidelines for all electronic transactions undertaken on behalf of the organization. The objective of this policy is to ensure that the use of electronic funds transfers and receipts are started, carried out, and approved in a secure manner.

Procedures

Electronic Funds Transfer (EFT)

It is the policy FAME foundation that all payments and receipts should be made by EFT where appropriate.

All EFT payments and receipts must adhere to all finance policies in the financial policies manual. All EFT arrangements, including receipts and payments must be submitted to the Administrative Officer of the organization. EFT payments must have the appropriate authorisation for payment in line with the financial transactions policy in the financial policies manual.

EFT payments can only be released for payment once authorised by the Executive Director for good control over EFT payments. The Finance Officer then proceeds to make the payments.

It is the responsibility of the Executive Director to annually review EFT authorisations for initial entry, alterations, or deletion of EFT records.

Electronic Purchases

All electronic purchases by any authorised employee must adhere to the purchasing policy in the financial policies manual.

Where an electronic purchase is being considered, the person authorising this transaction must ensure that the internet sales site is secure and safe and be able to demonstrate that this has been reviewed.

All electronic purchases must be undertaken using the organization’s credit cards only.

IT Service Agreements Policy

Policy Number: 008

Policy Date: 12/09/2021

Purpose of the Policy

This policy provides guidelines for all IT service agreements entered into on behalf of the business.

Procedures

The following IT service agreements can be entered into on behalf of the organization:

- Provision of general IT services
- Provision of network hardware and software
- Repairs and maintenance of IT equipment
- Provision of organization's software
- Provision of mobile phones and relevant plans
- Website design, maintenance etc.

All IT service agreements must be reviewed by the IT Manager before the agreement is entered into. Once the agreement has been reviewed and recommendation for execution from the Operations Manager has been received, then the agreement must be approved by the Executive Director.

All IT service agreements, obligations and renewals must be recorded in the IT excel sheet. Where an IT service agreement renewal is required, in the event that the agreement is substantially unchanged from the previous agreement, then this agreement renewal can be authorised by the Operations Manager.

Where an IT service agreement renewal is required, in the event that the agreement has substantially changed from the previous agreement, a lawyer should conduct the review and be present before the renewal is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by the Executive Director.

In the event that there is a dispute to the provision of IT services covered by an IT service agreement, it must be referred to the Operations Manager who will be responsible for the settlement of such dispute.

Emergency Management of Information Technology

Policy Number: 009

Policy Date: 24/08/2021

Purpose of the Policy

This policy provides guidelines for emergency management of all information technology within the business.

Procedures

IT Hardware Failure

Where there is failure of any of the organization's hardware, this must be referred to the Technical Officer immediately.

It is the responsibility of the IT manager to undertake tests on planned emergency procedures weekly to ensure that all planned emergency procedures are appropriate and minimise disruption to the activities of the organization.

Virus or other security breach

In the event that the organization's information technology is compromised by software virus, such breaches are to be reported to the IT Manager immediately. The IT Manager is responsible for ensuring that any security breach is dealt with within 8 hrs to minimise disruption to the organization's activities.

Website Disruption

In the event that the organization's website is disrupted, the following actions must be immediately undertaken:

- Website host to be notified.
- The IT Manager must be notified immediately.

- The Operations Manager.