SACH

Society For Action In Community Health

INFORMATION TECHNOLOGY

Policy and Procedure Manual

Version 3 - February 2023

SACH

Society For Action In Community Health

INFORMATION TECHNOLOGY

POLICY AND PROCEDURE MANUAL

Version 3 - February 2023

CONTENTS

INTRODUCTION

The SACHIT Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the organization which must be followed by all staff. It also provides guidelines SACHwill use to administer these policies, with the correct procedure to follow.

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

These policies and procedures apply to all employees.

TECHNOLOGY HARDWARE PURCHASING POLICY

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 organization 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 organization.

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 a Windows/MacOS operating systems and integrate with existing hardware-company server.

The desktop computer systems must be purchased as standard desktop system bundle and must be as per the system suggested by the IT specialist and approved by the CEO. Preferred brands include but not limited to Apple (Mac) HP, Dell, Lenovo, etc.

The desktop computer system bundle must include:

Desktop tower

Desktop screen

- Keyboard and mouse- (wireless/wire operated)
- Windows 7 and above operating system, and software - Office 2013 or higher version
- Other auxiliaries such as speakers, microphone, webcam, printers etc (Subject to approval by the CEO/Head of Finance

The minimum capacity of the desktop must be:

- 3 GHzor above
- 8GB RAM
- 2number of USB ports
- Intel i3 or above processor; memory drive of 1TB+

Any change from the above requirements must be authorised by the CEO upon the recommendation from the IT specialist.

All purchases of desktops must be supported under the specific brand's guarantee and/or warranty period and be compatible with the organisation's server system.

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

Purchasing portable computer systems

The purchase of portable computer systems includes notebooks, laptops, tablets etc.

Portable computer systems purchased must run a Windows/MacOS operating systems and integrate with existing hardware-company server.

Theportable computer systems purchased must be as per the system suggested by the IT specialist and approved by the CEO. Preferred brands include but not limited to HP, Dell, Lenovo, Acer, Mac, etc.

The minimum capacity of the portable computer system must be:

- 3GHz or above
- 4GB RAM
- 2 number of USB ports
- Intel i3 or above processor; memory drive of 1TB+

The portable computer system must include the following software provided:

- Software- Office 2013, Adobe, Reader, Google Chrome

Any change from the above requirements must be authorised bythe CEO upon the recommendation from the IT specialist.

All purchases of portable computer systems must be supported under the specific brand's guarantee and/or warranty period and be compatible with the organisation's server system.

All purchases for portable computer systemsmust be in line with the purchasing policy in the financial policies and procedures manual.

Purchasing server systems

Server systems can only be purchased by the IT specialist.

Server systems purchased must be compatible with all other computer hardware in the organisation.

All purchases of server systems must be supported bythe required guarantee and/or warranty period as offered by the brand and be compatible with the organisation's other server systems.

Any change from the above requirements must be authorised by the CEO upon the recommendation from the IT specialist.

All purchases for server systems must be in line with the purchasing policy in the Financial policies and procedures manual.

Purchasing computer peripherals

Computer system peripherals include add-on devices such as printers, scanners, external hard drives etc.

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 organisation.

The purchase of computer peripherals can only be authorised by the Head of Finance, after the recommendation by the IT specialist or team manager.

All purchases of computer peripherals must be supported under the specific brand's guarantee and/or warranty period and be compatible with the organisation's server system.

Any change from the above requirements must be authorised by the CEO upon the recommendation from the IT specialist.

All purchases for computer peripherals must be in line with the purchasing policy in the Financial policies and procedures manual.

Purchasing mobile telephones

A mobile phone will only be purchased once the eligibility criteria is met. Refer to the Mobile Phone Usage policy in this document.

The purchase of a mobile phone must be from authorised suppliers, such as dealers of Samsung, Apple, and other verified vendors offering multiple brands to ensure the organisation takes advantage of volume pricing based discounts provided by the aforementioned authorised suppliers. Such discounts should include the purchase of the phone, the phone call and internet charges etc.

The mobile phone must be compatible with the organizations's current hardware and software systems.

The mobile phone purchased must be iPhone, Samsung, Oppo, Redmi, etc.

The request for accessories (a hands-free kit etc.) must be included as part of the initial request for a phone.

The purchase of a mobile phone must be approved by Head of Finance after recommended by the State Head/Program Director prior to purchase.

Any change from the above requirements must be authorised by the CEO upon the recommendation by the Head of Finance.

All purchases of all mobile phones must be supported by guarantee and/or warranty period specified as per the brand's and/or vendor's policy.

All purchases for mobile phones must be in line with the purchasing policy in the Financial policies and procedures manual.

Additional Policies for Purchasing Hardware

Purchasing Policy- As per SACH finance policy

Mobile phone policy

POLICY FOR GETTING SOFTWARE

Purpose of the Policy

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

Procedures

Request for Software

All software must be approved by IT specialist 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 IT Specialist.

All purchased software must be purchased from verified software sellers, the certifications of whom must be presented during the approval processes before procuring the software.

All purchases of software must be supported by guarantee and/or warranty requirements as provided by the companyand be compatible with the organisation's server and/or hardware system.

Any changes from the above requirements must be authorised byCEO upon the recommendation of the IT specialist.

All purchases for software must be in line with the purchasing policy in the Financial policies and procedures 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, it should be notified to the IT Specialistprior to the download or use of such software.

All open source or freeware must be compatible with the business's hardware and software systems.

Additional Policies for Obtaining Software

Purchasing Policy- As per SACH finance policy

POLICY FOR USE OF SOFTWARE

Purpose of the Policy

This policy provides guidelines for the use of software for all employees within the organisation to ensure that all software use is appropriate. Under this policy, the use of all open source and freeware software will be conducted under the same procedures outlined for commercial software.

Procedures

Software Licensing

All computer software copyrights and terms of all software licences will be followed by all employees of the business.

Where licensing states limited usage in terms of number of systems/computers using the software, then it is the responsibility of IT Specialist to ensure these terms are followed.

IT Specialist is 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 the supplier where this is a requirement.

SACH is to be the registered owner of all software.

Only software obtained in accordance with the software policy is to be installed on the organisation's computers.

All software installation is to be carried out by IT Specialist.

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 organisation.

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 new employees to be trained to use existing software appropriately. This will be the responsibility of IT Specialist in co-ordination with the Team Manager.

Employees are prohibited from bringing software from home and loading it onto the business's computer hardware.

Unless express approval from IT Specialist 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 CEO 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 business and must be recorded on the software register by IT Specialist and Finance Executive.

Unauthorised software is prohibited from being used in the business. This includes the use of software owned by an employee and used within the business.

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 IT Specialist, Program-Director and Head of Finance for further consultation, and reprimand-legal action. The illegal duplication of software or other copyrighted works is not condoned within this business and IT Specialist 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 IT Specialist/Program Director for appropriate action.

Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify the Team manager/State Head 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 Program Director for appropriate action.

BRING YOUR OWN DEVICE POLICY

At SACH, we acknowledge the importance of mobile technologies in improving business communication and productivity. In addition to the increased use of mobile devices, staff members have requested the option of connecting their own mobile devices to SACH'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, tablets and or any other equipment for business purposes. All staff who use or access SACH's technology equipment and/or services are bound by the conditions of this Policy.

Procedures

Current mobile devices approved for business use

The following personally owned mobile devices are approved to be used for business purposes:

- Devices such as notebooks-Laptops of brands mentioned in the previous section of this policy.
- Devices such as smart phones or tabletsof brands mentioned in the previous section of this policy.
- Devices pertaining to removable media such as USBs, Hard drives/disks, etc., of brand/specification as approved by the IT specialist can be used by the staff.

Registration of personal mobile devices for business use

Employees when using personal devices for business use will register the device with the IT specialist/HR Department.

Finance Department will record the device and all applications used by the device.

Personal mobile devices can only be used for the following purposes:

- Access to emails on organisation's server/other official mail IDs
- Business/official calls and texts

Each employee who utilises personal mobile devices agrees:

- Not to download or transfer business or personal sensitive information to the device.Sensitive information intellectual property, other employee details, project related information, etc.
- Not to use the registered mobile device as the sole repository for SACH's information. All business information stored on mobile devices should be backed up
- To make every reasonable effort to ensure that SACH'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
- To maintain the device with updated current operating software and appropriate security software to prevent/leak of sensitive data.
- Not to share the device with other individuals to protect the organisation data access through the device
- To abide by SACH's internet policy for appropriate use and access of internet sites etc.
- To notify SACH immediately in the event of loss or theft of the registered device
- Not to connect USB memory sticks from an untrusted or unknown source to SACH's equipment.

All employees who have a registered personal mobile device for official use acknowledge that the organisation:

- 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 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 official use at any time.

Keeping mobile devices secure

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

- 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 CEO grants an exemption. Any requests for exemptions from any of these directives, should be referred to the CEO forwarded by the IT Specialist and Program-director.

Breach of this policy

Any breach of this policy will be referred to Program-director, IT Specialist and Head of Finance who will review the breach and determine adequate consequences, which can include confiscation of the device and or termination of employment.

Indemnity

SACH 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 indemnify SACH against any and all damages, costs and expenses suffered by SACH 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 SACH.

INFORMATION TECHNOLOGY SECURITY POLICY

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 keypad, lock etc.

It will be the responsibility of IT Specialist 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 IT Specialist immediately.

All security and safety of all portable technology, such as laptop, notepads, iPad etc., will be the responsibility of the employee who has been issued with the specific device. Each employee is required to use locks, passwords, etc.,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, Finance Team along with the IT Specialist will assess the security measures undertaken to determine if the employee will be required to reimburse the business for the loss or damage.

All devices such as laptop, notepads, iPads etc., when kept at the office desk is to be secured or stowed away in the specific cabinet, and secured by keypad, lock etc.

Information Security

All official data to be backed up here – either general such as sensitive, valuable, or critical organisational data is to be backed-up.

It is the responsibility of IT Specialist, State Heads/Team Headsto ensure that data back-ups are conducted monthlyand the backed up data is keptsecured at a locker facility (provided at HO) or at the employees home.

All technology that has internet access must have anti-virus software installed.It is the responsibility of IT Specialist/Team Heads 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 subjected to consequences post review by the upper management (CEO/Finance Head/Program Director)

Technology Access

Every employee will be issued with a unique identification code to access the business technology and will be required to set a password for access.

Each password is to be created so in order to ensure highest level of security, such as number of alpha and numeric etc.,and is not to be shared with any employee within the business.

IT Specialist and HR department 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 IT Specialist 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.

Employees are only authorised to use business computers for personal use whilst on travel, during field visits, etc., specifically for internet usage, accessing personal mail IDs, etc.

For internet and social media usage, refer to the Human Resources Manual.

It is the responsibility of IT Specialist to keep all procedures for this policy up to date.

INFORMATION TECHNOLOGY ADMINISTRATION POLICY

Purpose of the Policy

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

Procedures

All software installed and the licence information must be registered on the organisation assets list maintained by the HR Department. It is the responsibility of IT Specialist to ensure that this registered is maintained. The register must record the following information:

- What software is installed on every machine
- What licence agreements are in place for each software package
- Renewal dates if applicable.

IT Specialist is responsible for the maintenance and management of all service agreements for the business technology. Any service requirements must first be approved by CEO/Finance Head.

IT Specialist is responsible for maintaining adequate technology spare parts and other requirements including requirements such as toners, printing paper etc.

A technology audit is to be conducted annually by the IT Specialist to ensure that all information technology policies are being adhered to.

Any unspecified technology administration requirements should be directed to CEO/Finance Head

WEBSITE POLICY

Purpose of the Policy

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

Procedures

Website Register

The website register must record the following details:

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

The keeping the register up to date will be the responsibility of IT Specialist

IT Specialist will be responsible for any renewal of items listed in the register.

Website Content

All content on the business website is to be accurate, appropriate and current. This will be the responsibility of Website Management Specialist and IT Specialist.

All content on the website must follow a content plan, covering the required data pertaining to the work of the organisation.

The content of the website is to be reviewed Program-Director and CEO.

The following persons are authorised to make changes to the business website:
CEO
Program-Director
Finance Head

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

All data collected from the website is to adhere to the Privacy Act

ELECTRONIC TRANSACTIONS POLICY

Purpose of the Policy

This policy provides guidelines for all electronic transactions undertaken on behalf of the business.

The objective of this policy is to ensure that 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 of SACH 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 and procedures manual.

All EFT arrangements, including receipts and payments must be submitted to the finance department.

EFT payments must have the appropriate authorisation for payment in line with the financial transactions policy in the Financial policies and procedures manual.

EFT payments must be appropriately recorded in line with finance policy in the Financial policies and procedures manual.

EFT payments once authorised, will be entered into the payment system- Fedbiz system by Finance executive.

EFT payments can only be released for payment once pending payments have been authorised by Finance Head/CEO.

For good control over EFT payments, ensure that the persons authorising the payments and making the payment are not the same person.

All EFT receipts must be reconciled to records fortnightly.

Where EFT receipt cannot be allocated to customer account, it is responsibility of {insert relevant job title here} to investigate. In the event that the customer account cannot be identified within a week, the receipted funds must be returned to source etc. Head of Finance/ CEOmust authorise this transaction.

It is the responsibility of Head of Finance and Finance Executive to annually review EFT authorisations for initial entry, alterations, or deletion of EFT records, including supplier payment records and customer receipt records.

Electronic Purchases

All electronic purchases by any authorised employee must adhere to the purchasing policy in the Financial policies and procedures 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 business credit cards only and therefore adhere to the business credit card policy in the Financial policies and procedures manual.

IT SERVICE AGREEMENTS POLICY

Purpose of the Policy

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

Procedures

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

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

All IT service agreements must be reviewed by a legal advisor/CAbefore the agreement is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by Finance Head/CEO.

All IT service agreements, obligations and renewals must be recorded.

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 CEO.

Where an IT service agreement renewal is required, in the event that the agreement has substantially changed from the previous agreement, the Finance head should review the same before the renewal is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by CEO.

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 Head of Finance and IT specialist who will be responsible for the settlement of such dispute.

EMERGENCY MANAGEMENT OF INFORMATION TECHNOLOGY

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 organisation's hardware, this must be referred to the IT Specialist immediately.

It is the responsibility of IT Specialist to proceed with remedial course of action in the event of IT hardware failure.

It is the responsibility of IT Specialist to undertake tests on planned emergency procedures quarterly to ensure that all planned emergency procedures are appropriate and minimise disruption to organisation's operations.

Virus or other security breach

In the event that the organisation's information technology is compromised by software virus or other possible security breaches, such breaches are to be reported to IT specialist immediately.

IT Specialist is responsible for ensuring that any security breach is dealt with immediately and within a week (depending on the scope of the issue; subject to approval from CEO) to minimise disruption to business operations.

Website Disruption

In the event that business website is disrupted, the following actions must be immediately undertaken:

- Website host to be notified immediately and security measures to be adopted
- IT specialist and Website manager must be notified immediately.

SACH
Society For Action In Community Health

253, 2nd Floor, Shahpur Jat, New Delhi - 110049
Tel.: +91 11 4056 2549, 4611 4888, Email: contactus@sachindia.org
www.sachindia.org