INFORMATION TECHNOLOGY POLICY MANUAL

[GUIDELINES AND PROCEDURES]

A COMPREHENSIVE GUIDELINE TO THE EMPLOYMENT AND/ USE OF INFORMATION TECHNOLOGY AT SALT UNIVERSITY COLLEGE

February, 2022

Table of Contents

Introduction 1

Technology Hardware Purchasing Policy 2

Purpose of the Policy 2.1

Procedures 2.2

Policy for Getting Software 3

Purpose of the Policy 3.1

Procedures 3.2

Policy for Use of Software 4

Purpose of the Policy 4.1

Procedures 4.2

Bring Your Own Device Policy 5

Purpose of the Policy 5.1

Procedures 5.2

Information Technology Security Policy 6

Purpose of the Policy 6.1

Procedures 6.2

Information Technology Administration Policy 7

Purpose of the Policy 7.1

Procedures 7.2

Website Policy 8

Purpose of the Policy 8.1

Procedures 8.2

E-Campus Policy 9

Purpose of the Policy 9.1

Procedures 9.2

Electronic Transactions Policy 10

Purpose of the Policy 10.1

Procedures 10.2

IT Service Agreements Policy 11

Purpose of the Policy 11.1

Procedures 11.2

Emergency Management of Information Technology 12

Purpose of the Policy 12.1

Procedures 12.2

Introduction

The SALT University CollegeIT Policy Manual provides the policies and procedures for selection and use of IT within the institution, and must be adhered to by all students, faculty and staff.

Information Technology is the use of computers to create, process, store, retrieve, and exchange all kinds of electronic data and information

This manual will provide guidelines that SALT University College will use to administer all IT related policies. SALT University College will 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.

Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.

These policies and procedures apply to Students, Faculty and Staff.

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 University Collegeto ensure that all hardware technology for SALT University Collegeis appropriate, provides value for money and where applicable, integrates with other existing technology being used in the Institute. The objective of this policy is to ensure that there is minimal diversity of hardware within the Institute.

Procedures

Purchase of Hardware

The purchase of all desktops, servers, portable computers, computer peripherals and mobile devices must adhere to this policy. All computer hardware, software and mobile device related purchases must be recommended by the IT Manager and authorised by the Assistant Registrar (IT Support Services).

Purchasing desktop computer systems

The desktop computer systems purchased must run on a Windows 10 pro or Mac OS operating system and integrate with existing hardware such as printers, scanners and wireless access points. The desktop computer systems must be purchased as standard desktop system bundle and must include:

All in one Desktop or Desktop tower

Desktop screen of 23.8” (24 inch)

- Keyboard and mouse
- Windows 10 or Mac Os, and software e.g. Office 2016, Chrome, Java 8, NET 4.7.x and an office 365 subscription package
- Speakers, microphones, webcams, printers etc.

The minimum capacity of the desktop must be:

- 1.5 GHz -gigahertz
- 4GB RAM
- 500 HDD / 128 SSD
- Intel Core i5
- 2 USB ports
- 1 HDMI port
- 802.11a/b/g/n/ac

Any change from the above requirements must be recommended by the IT Manager and authorised by the Assistant Registrar

All purchases of desktops must be supported by basic 1- year manufacturer warranty.

Purchasing portable computer systems

The purchase of portable computer systems includes notebooks, laptops, tablets, phones, iPads. Laptops and notebooks computer systems purchased must be able to run a Windows 10 Pro or Mac OS operating system and integrate with the existing hardware eco-system.

Ipads and other tablets purchased must be able to integrate with the existing hardware eco-system

The minimum capacity of a laptop and notebook portable computer system must be:

- 1.5 GHz - gigahertz
- 8GB RAM
- 2 USB ports
- Intel Core i5
- 1 HDMI port
- 802.11a/b/g/n/ac

The portable computer system must include the following software provided:

- Office 2016
- Google Chrome
- Java 8
- .NET 4.7.x

  Any change from the above requirements must be recommended by the IT Manager and authorised by the Assistant Registrar (IT Support Services)

All purchases of all portable computer systems must be supported by the basic 1- year manufacturer warranty.

The minimum capacity of Ipad and tablet computer system must be:

- Screen size of 9.7 inches
- A9 chipset
- 4 gig RAM
- 32 GB SSD/ 128 GB SSD

Purchasing server systems

Server systems can only be purchased by the IT Manager and authorised by The Rector.

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

All purchases of server systems must be supported by 24 x7 service support and 4- hour response onsite support warranty every year and be compatible with the Institute's other systems.

Any change from the above requirements must be recommended by the IT Manager and authorised by Rector.

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 that is currently being used at the Institute.

The purchase of computer peripherals can only be recommended by the IT Manager and authorised by The Rector.

All purchases of computer peripherals must be supported by a basic 1-year manufacturer warranty and be compatible with the Institute's existing computer systems.

Any change from the above requirements must be recommended by the IT Manager and authorised by the Assistant Registrar (IT Support Services).

Purchasing mobile telephones

The purchase of a mobile phone must be from Samsung, Infinix and Tecno to ensure the University Collegetakes advantage of volume pricing-based discounts provided by the suppliers. Such discounts should include the purchase of the phone, other accessories, promotions on the phone call and internet charges etc.

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

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 recommended by the IT Manager and authorised by the Assistant Registrar (IT Support Services) prior to purchase.

Any change from the above requirements must be recommended by the IT Manager and authorised by the Assistant Registrar (IT Support Services) and Finance Manager.

All purchases of all mobile phones must be supported by a guarantee and/or warranty.

Policy for Getting Software

Purpose of the Policy

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

Procedures

Request for Software

All software, including MySQL, firewall must be recommended by the IT Manager and authorised by Assistant Registrar (IT Support Services) 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 recommended by the IT Manager and authorised by Assistant Registrar (IT Support Services).

All purchased software must be purchased from reputable software sellers. All purchases of software must be supported by 1- year manufacturer warranty and be compatible with the Institute's server and/or hardware system.

Any changes from the above requirements must be recommended by the IT Manager and authorised by Assistant Registrar (IT Support Services).

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, the IT Manager must recommend such and the authorisation of the Assistant Registrar (IT Support Services) must be obtained prior to the download or use of such software.

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

Any change from the above requirements must be recommended by the IT Manager and authorised by the Assistant Registrar (IT Support Services).

Policy for Use of Software

Purpose of the Policy

This policy provides guidelines for the use of software for all employees within the University Collegeto 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 adhered to by Students, Faculty and Staff of the Institute.

Where licensing states limited usage (i.e. number of computers or users etc.), then it is the responsibility of the IT Manager to ensure these terms are followed.

The IT Manager 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.

SALT University Collegeis to be the registered owner of all software purchased and used.

Only software obtained in accordance with the getting software policy is to be installed on the Institute’s computers.

All software installation is to be carried out by the IT Manager and authorised by the Assistant Registrar

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 Institute.

Prior to the use of any software, the IT Manager must review instructions on any licensing agreements relating to the software, including any restrictions on use of the software.

All Students, Faculty and Staff must receive training for new software where appropriate. This includes new staff to be trained to use existing software effectively. This will be the responsibility of the IT Manager.

Without the express permission of the Assistant Registrar through the IT Manager, Students, Faculty and Staff are prohibited from bringing software from home and loading it onto the Institute's computer hardware.

Unless express approval from the Assistant Registrar (IT Support Services) is obtained, software cannot be taken home and loaded on a Student, Faculty Member and Staff's home computer.

Upon receipt of the required approval, if determined that software can be used on the student, faculty or staff's home computer by the IT Manager, authorisation from the Assistant Registrar (IT Support Services) 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 University Collegeand must be recorded on the software register by the IT Manager.

Unauthorised software is prohibited from being used in the Institute. This includes the use of software owned by staff, faculty and students and used within the Institute.

The unauthorised duplicating, acquiring or use of software copies is prohibited. Any staff, faculty or student who makes, acquires, or uses unauthorised copies of software will be referred to the Assistant Registrar (IT Support Services) for further consultation or reprimand action etc. The illegal duplication of software or other copyrighted works is not condoned within the University Collegeand the Assistant Registrar is authorised to undertake disciplinary action where such an event occurs.

Breach of Policy

Where there is a breach of this policy by a Student, Faculty member or Staff or that individual will be referred to the Assistant Registrar (IT Support Services) for further consultation, 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 Assistant Registrar (IT Support Services) 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 Assistant Registrar (IT Support Services) for further consultation, reprimand action etc.

Bring Your Own Device Policy

At SALT Institute, we acknowledge the importance of mobile technologies in improving business communication and productivity. In addition to the increased use of mobile devices, Students, Faculty and Staff have requested the option of connecting their own mobile devices to SALT Institute’s network and equipment. We encourage you to read this document in full and to act upon the recommendations.

Purpose of the Policy

This policy provides guidelines for the use of personally owned notebooks, smart phones, tablets and laptops for work or academic purposes. All Students, Faculty members and Staff who use or access Salt Institute'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 work or academic purposes:

- Apple products such as iPhone, iPad and smartwatches
- Android products such as smartphones, tablets and smartwatches
- Notebooks / Laptops

Registration of personal mobile devices for use in the Institute

Faculty and Staff when using personal devices for University Collegerelated work will register the device with the IT Manager.

The IT Manager will record the device and all applications used by the device.

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

- Accessing the Institute’s email
- Internet access
- Telephone calls on behalf the Institution

Each Faculty and Staff who utilise personal mobile devices agrees:

- Not to download or transfer University Collegeor personal sensitive information to the device. Sensitive information includes for example intellectual property, student records, faculty or employee details, other sensitive information etc.
- Not to use the registered mobile device as the sole repository for SALT Institute's information. All University Collegeinformation stored on mobile devices should be backed up
- To make every reasonable effort to ensure that SALT Institute'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 up to date operating software and up to date security software etc
- Not to share the device with other individuals to protect the Institute's data access through the device
- To abide by SALT Institute's internet policy for appropriate use and access of internet sites etc.
- To notify SALT University Collegeimmediately in the event of loss or theft of the registered device
- Not to connect USB memory sticks from an untrusted or unknown source to SALT Institute's equipment.

All faculty or staff who have a registered personal mobile device for official work use acknowledge that the Institute:

- 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 staff or faculty wants to sell the device

- Will delete all data held on the device upon termination of the staff or faculty. The terminated staff or faculty can request personal data be reinstated from back up data
- Has the right to deregister the device for Institute's 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 the Assistant Registrar (IT Support Services) grants an exemption. Any requests for exemptions from any of these directives, should be referred to the Assistant Registrar (IT Support Services) through the Head of department for students and through the IT Manager for faculty and staff.

Breach of this policy

Any breach of this policy will be referred to the Assistant Registrar (IT Support Services) who will review the breach and determine adequate consequences, which can include but not limited to consequences such as confiscation of the device and or termination of employment.

Indemnity

SALT University Collegebears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of students, faculty and staff in accessing or using these resources or facilities. All students, faculty and staff indemnify SALT University Collegeagainst any and all damages, costs and expenses suffered by SALT University Collegearising 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 SALT Institute.

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 University Collegeto 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, locks and coded access.

It will be the responsibility of the IT Manager to ensure that this requirement is followed at all times. Any student, faculty or staff, becoming aware of a breach to this security requirement is obliged to notify the Assistant Registrar (IT Support Services).

All security and safety of all portable technology, such as laptop, notepads, iPad etc. will be the responsibility of the student, faculty and staff who has been issued with the laptop, notepads, iPads, mobile phones etc. Each student, faculty and staff are required to use secure and complex passwords 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 Assistant Registrar (IT Support Services) will assess the security measures undertaken to determine if the student, faculty and staff will be required to reimburse the University Collegefor the loss or damage.

All laptops, notepads, iPads etc. when kept at the office desk are to be adequately secured.

Information Security

All sensitive, valuable or critical data belonging to the University Collegeare to be backed up.

It is the responsibility of the IT Manager to ensure that data back-ups are conducted weekly and the backed-up data is kept on the cloud, or at an offsite venue.

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

All information used within the University Collegeis to adhere to the privacy laws and the Institute's confidentiality requirements. Any staff, faculty or student breaching this will be addressed by the appropriate disciplinary action.

Technology Access

Every staff and faculty will be issued with unique identification credentials to access SALT Institute's technology platforms and will be required to reset a password for access every 180 days.

Each password must meet the following requirements;

- Uppercase character
- Lowercase character
- Numbers 0-9
- Non-alphanumeric characters such as (~!@#$%^&*()_-+[{]};:'",<.>/?)

And is not to be shared with any student, staff or faculty within the Institute.

The Assistant Registrar (IT Support Services) is responsible for the issuing of the identification code and initial password for all employees.

Where a student, staff or faculty member forgets the password or is 'locked out' after five attempts}, then the IT Manager authorised by the Assistant Registrar (IT Support Services) is authorised to reissue a new initial password that will be required to be changed when the individual logs in using the new initial password.

The following table provides the authorisation of access:

Technology – Hardware/ Software	**Persons authorised for access**
E-Campus	IT Manager (Academic Services)
Website	IT Development Manager

Hosting, Emails,	IT Manager (Academic Services) and IT Development Manager
Internet	IT Manager
Digital Payment Integration	IT Development Manager
Video streaming application - Zoom	IT Development Manager

It is the responsibility of the Assistant Registrar (IT Support Services) 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 Institute.

Procedures

It is the responsibility of the IT Manager to ensure that all software installed and license information are kept secured and maintained. The information that is to be kept should include the following information;

- What software is installed on every machine
- What licence agreements are in place for each software package
- 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 recommended by the IT manager and authorised by the Assistant Registrar (IT Support Services)

The IT Manager is responsible for maintaining adequate technology spare parts and other requirements including such as toners, printing paper, laptop charges, mouse, keyboards, batteries, video cables etc.}

A technology audit is to be conducted annually by the IT Development 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

Purpose of the Policy

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

Procedures

Website Register

The website register must record the following details:

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

Keeping the register up to date will be the responsibility of the IT Development Manager.

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

Website Content

All content on the Institute's website is to be accurate, appropriate and current. This will be the responsibility of the IT Development Manager.

All content on the website must follow the objectives of the Institute, content plan, strategy and events.

The content of the website is to be reviewed quarterly

The following persons are authorised to make changes to the Institute's website:

- Michael Offei and his team from AMS Digital Solutions

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

E-CAMPUS POLICY

Purpose of the Policy

This policy provides guidelines for the use of SALT institute's eCampus (My Salt eCampus): a platform for teaching and learning. It will provide a basis for a standardized and structured approach to the use of this medium.

Procedures

Accessing the Platform

My Salt eCampus is accessed through a web browser on your laptop, PC, tablet or notepad (or smartphone). The system requirements for the My Salt eCampus user are modest. All you really need is a solid, reliable internet connection and a modern web browser.

However, these are the general minimum system requirements that we would consider necessary for My Salt eCampus to run efficiently on your system and enable you to participate in the course effectively.

Basic Computer Skills Needed:

- Basic familiarity with the Zoom cloud meeting/video conferencing application
- Saving into .pdf, .docx, .csv, .ppt, etc. and finding files and folders on a computer;
- Copying/cutting and pasting text;
- Using a word processing application, such as Microsoft Word;
- Attaching and uploading documents and assignments;
- Sending and receiving email;

Device and Operating System:

- Intel processor compatible laptops/PCs with Pentium IV 1GHz and above, with Windows 7 (1GB MB of RAM) minimum operating system or better
- Mac - Dual-Core Intel Processor or higher or better, with OS X latest version
- Both PCs and Macs should have a sound card with Speakers and/or Headphone, Microphone/Mouthpiece and Camera (optional)
- Mobile Devices: At present, the eCampus mobile app is not supported due to poor performance. We recommend that on a mobile device you log in to eCampus using the web browser unless you are completing an assessment or activity that has a grading

component. If you are completing an assessment or activity that has a grading component, we recommend that you use eCampus through a desktop browser.

Internet Speed:

- Internet connection (Broadband/DSL preferred but a dial up connection may work) Use a broadband connection (256 Kbit/sec or faster—this will ensure that you can view videos and online presentations) through USB wireless modem, ADSL, T1/T2, fibre optic or cable. 4G and 3G mobile hotspots may be used as well with stable network reception. Dial-up access may be significantly slower.

Internet Browsers:

- Recommended Browsers: Google Chrome or Mozilla Firefox. Firefox and Chrome 32-bit version 50 or later (recommended for optimal compatibility, this has been thoroughly tested on Windows). Safari 10 or later (recommended for optimal compatibility, this has been thoroughly tested on Mac). Note that add-ons and toolbars can affect any browser's performance.

Settings:

- We recommend that the following be enabled: Cookies, Pop-ups (in both Internet browser and security software) and JavaScript

Plug-ins:

- We recommend that you use the latest version of Adobe Flash Player
- Apple QuickTime (latest version)

Resource Viewing:

- We recommend that you use the latest version of the free Adobe Acrobat Reader DC. (https://get.adobe.com/reader/) **uncheck** the two optional offers boxes before download (McAfee Security Scan Plus and McAfee Safe Connect)
- To view all the resources uploaded to eCampus, you will probably need to have Microsoft Office (Word, Excel, PowerPoint) or an equivalent (e.g. Open Office, Viewer) installed.

Security:

- We will not recommend usage of special antivirus; each user is responsible for their own computer security. It is recommended that the latest Windows 10 users constantly update their Windows Security (formerly Windows Defender) manually so it can take care of all malicious files.
- With all firewalls, ensure that you enable uploading of files.
- Please note that eCampus and/or SALT University Collegecannot be held responsible for any upgrades in software or hardware needed as a result of enrolling onto a course. Further, eCampus and/or SALT University Collegecannot be held liable for any malicious software obtained as a result of downloading or uploading files from our server. Whilst all the files uploaded by eCampus and/or SALT University Collegeare checked for malicious software eCampus and/or SALT University Collegeis not responsible for content uploaded by malicious third parties or legitimate users.
- The University Collegeapplies the relevant National Data Protection and Privacy guidelines to ensure protection of information.
- 24/7 technical support available to assist all users overcome challenges promptly.
- The use of automatic cloud storage and local/manual database backup tools to effectively and efficiently restrict information access that promotes data security and data integrity.

My Salt eCampus Usage

My Salt eCampus, a medium to enhance teaching and learning, as well as innovation at the University Collegecan be used by all faculty and students for the purposes herein stated.

It is the responsibility of the IT Manager with the authorisation of the Assistant Registrar (IT Support Services) to ensure that the needed resources for eLearning and research are available and readily accessible on demand.

Any challenges or concerns that may arise in the use of eCampus should be directed to the IT Manager for immediate resolution or the needed assistance.

There shall be consistent evaluation carried out by Assistant Registrar (IT Support Services) to ensure that challenges to effective pedagogy and research are duly taken care of.

Electronic Transactions Policy

Purpose of the Policy

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

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 SALT University Collegethat where appropriate, payments and receipts should be made by EFT. All EFT payments and receipts must adhere to all finance policies by the Institute.

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 of the Institute.

EFT payments must be appropriately recorded in line with finance policy of SALT Institute

EFT on the website payments such as fee payments and donations will be entered into the finance records by the Finance Manager

EFT payments can only be released for payment once pending payments have been authorised by the Rector.

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 customer records biweekly.

Where EFT receipts cannot be allocated to customer accounts, it is the responsibility of the Finance Manager to investigate.

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

Electronic Purchases

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 Institute's credit cards only.

IT Service Agreements Policy

Purpose of the Policy

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

Procedures

The following IT service agreements can be entered into on behalf of SALT Institute:

- Provision of general IT services
- Provision of network hardware and software
- Repairs and maintenance of IT equipment
- Provision of custom business 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 the recommendation for execution received, then the agreement may be approved by Assistant Registrar (IT Support Services)

The IT Manager is responsible for all IT service agreements, obligations and renewals to be recorded and placed in a secure location.

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 Assistant Registrar, IT Support Services.

Where an IT service agreement renewal is required, in the event that the agreement has substantially changed from the previous agreement, the IT Manager should review before the renewal is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement may be approved by Assistant Registrar (IT Support Services)

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 Assistant Registrar IT Support Services 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 Institute.

Procedures

IT Hardware Failure

Where there is failure of any of the Institute's hardware, it must be referred to the IT Manager immediately.

It is the responsibility of the IT Manager to

- Capture data at the time of failure
- Contain the damage and minimise risks

In the event of IT hardware failure

It is the responsibility of the IT Manager to undertake tests on planned emergency procedures annually to ensure that all planned emergency procedures are appropriate and minimise disruption to business operations.

Point of Sale Disruptions

In the event that point of sale (POS) or digital payment system is disrupted, the following actions must be immediately undertaken:

- Digital provider to be notified
- The IT Consultants must be notified immediately
- For all manual transactions, customer identity must be verified

Virus or other security breach

In the event that the Institute's information technology is compromised by software virus or ransomware etc, such breaches are to be reported to the Assistant Registrar immediately.

The IT Manager is responsible for ensuring that any security breach is dealt with within 2 hours to minimise disruption to business operations.

Website Disruption

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

- IT Consultants notified with the appropriate details
- Monitoring of configuration and logs to identify issue
- Website hosting provider notified if external help is needed.