Ann Street Presbyterian Church Trust (ASPCT)

Information Technology

Policy and Procedure Manual

Table of Contents

Ann Street Presbyterian Church Trust (ASPCT) Information Technology Policy and Procedure Manual 1

1. Introduction 2

2. Users 2

a) Employees and volunteers that use ASPCT ITEN as part of their function for the ASPCT and is covered as a matter of course by the ITSA; 2

b) Parties that use their own computers and ITEN under the ITSA: Ann Street Church Ministry Team, Church volunteers, collectively church users. 2

c) Parties that use the ITEN only for access to the internet and are not covered under the ITSA (e.g. City Bible Forum, Langham Partnership) 2

3. Policy of use for all Users 2

4. Hardware Policy 4

a) Purpose 4

b) Standard equipment and their purchase 4

5. Software Policy 5

c) Purpose of the Policy 5

d) Procedures 5

6. Bring Your Own Device Policy 7

e) Procedures 7

f) Indemnity 9

7. Information Technology Security Policy 9

a) Purpose of the Policy 9

b) Physical Security 9

c) Information Security 10

d) Technology Access 10

e) Systems Passwords 11

f) Software Passwords 11

8. Information Technology Administration Policy 11

g) Purpose of the Policy 11

h) Procedures 11

9. Emergency Management of Information Technology 12

i) Purpose of the Policy 12

j) Procedures 12

1. Introduction

The Ann Street Presbyterian Church Trust (ASPCT) is committed to the appropriate and efficient use of its information technology (IT) equipment and infrastructure. This document provides the policies and procedures for the use of IT equipment and infrastructure that it provides to its employees, volunteers and other parties.

All Users of the ASPCT IT equipment, network and other infrastructure (ITEN) must abide with the procedures, rules and guidelines as set out below and as may be amended from time to time.

ITEN is maintained by an IT consultant, currently MANTAQ Solutions, under an Information Technology Service Agreement (ITSA).

2. Users

The following categories of Users are identified:

a) Employees and volunteers that use ASPCT ITEN as part of their function for the ASPCT and is covered as a matter of course by the ITSA;
b) Parties that use their own computers and ITEN under the ITSA: Ann Street Church Ministry Team, Church volunteers, collectively church users.
c) Parties that use the ITEN only for access to the internet and are not covered under the ITSA (e.g. City Bible Forum, Langham Partnership).

3. Policy of use for all Users

All Users must adhere to the following:

i. Only authorized users may use the ITEN or a part of the ITEN

ii. Subject to point iii and iv below, all Users must be authorized by the Trustees of the ASPCT;

iii. The Trustees have authorized the Minister and Session Clerk of the Ann Street Church to designate Church Users;

iv. Parties covered by a separate agreement to occupy office space are considered a User;

v. An authorized User must obtain an assigned user account (name and email address, as required), which is identified by a username, from the Manager of the

APCT who will make the necessary arrangement to have the account set up under the ITSA, or access to the internet as may be applicable.

vi. A User may be given access to a range of IT Facilities and is to use these facilities in a manner which is ethical, lawful, effective and efficient. A User may only use those facilities they have been authorized to use.

vii. Where access to ITEN is password protected a User must not make this available to any other person. Users may also not disclose their password to another persona or access ITEN on behalf of another person. In case of breach of these rules the Trustees may consider disciplinary action that include, but is not limited to, dismissal or denial of further access to ITEN.

viii. Each User, while using their account, is responsible for all information sent from, intentionally requested, solicited or viewed from their account, and publicly accessible information placed on a computer using their account.

ix. A User must use be aware the ITEN resources are limited and use the resource for the purpose intended, although a reasonable amount of personal use is permitted;

x. A User must not attempt to circumvent the intention of these rules and must not attempt to subvert the security of ITEN.

xi. A User must immediately inform the Manager of ASPCT or a Trustee when said User becomes aware of any breach of security or an attempt to breach the security of ITEN.

xii. A User may not interfere with ITEN systems.

xiii. A User may not create or install or try to create or install any form of malicious software on ITEN.

xiv. ITEN may not be used for any purpose that may be deemed sexist, abusive, offensive, obscene or indecent; the creation or transmission of material which

may result in a person experiencing harassment, intimidation, harm, distress or sexual discrimination, or be defamed or breach copyright.

xv. ITEN may not be used for unauthorized commercial activities or personal gain; and

xvi. ITEN may not be used for the transmission of any material that contravenes any relevant federal or state legislation.

4. Hardware Policy

a) Purpose

This policy provides guidelines for the purchase of hardware to ensure that the technology is appropriate, and integrates with other technology for the business as far as possible. The objective of this policy is to minimize as far as possible diversity in hardware. The policy is also to ensure cost efficiency.

b) Standard equipment and their purchase

Computers

The computer systems purchased must be able to run the relevant Windows and Microsoft Office version and integrate with the existing business server system. A preference is to purchase Hewlitt Packard equipment.

All computers must be compatible with the server system.

All computer purchases must be recommended by the IT Consultant as appropriate according to the ITEN, the AST Manager and approved by the Trustees.

Exceptions to the above may be considered in the case where a special need is identified, but Trustees must be informed of the special case prior to obtaining quotes for the equipment.

Server Systems

All server system purchases must be recommended by the IT Consultant as appropriate according to the ITEN, the AST Manager and approved by the Trustees.

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

Any change from the above requirements must be authorised by the Trustees.

Computer peripherals (scanners, printers, etc.)

Computer system peripherals include printers and external hard drives.

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 computer systems.

Computer peripherals purchased must be compatible with all other computer hardware and software in the business.

The purchase of computer peripherals can only be authorised by the AST Manager upon advice of the IT Consultant in line with Trust budgeting and purchasing policies.

Any change from the above requirements must be authorised by the Trustees.

5. Software Policy

c) Purpose of the Policy

This policy provides guidelines for the purchase of software for the ASPCT to ensure that all software used by the business is appropriate, value for money and where applicable integrates with other technology for the Trust. This policy also governs software installed by all Users may affect the ITEN.

d) Procedures

Request for Software by Ann Street Trust (AST) staff

All software, including open source and freeware, must be approved by the AST Manager (upon the advice of the IT Consultant) prior to the use or download of such software.

Request for Software by Church Users

Non-AST Staff do not need to ask permission to download software to their computer systems. However, if any software installed is found to be affecting the ITEN, the Trustees have a right to demand the removal of that software from all systems connected to ITEN. Failure to remove the software will result in the denial of access to ITEN.

Purchase of AST software

The purchase of all software with AST funds must adhere to this policy.

All purchased software must be purchased by the AST Manager or the IT Consultant in consultation with each other.

All purchased software must be purchased from reputable software sellers.

All purchases of software must be supported by and be compatible with the business's server and/or hardware system.

Any changes from the above requirements must be authorised by the Trustees.

Obtaining open source or freeware software

Open source or freeware software is software obtained without payment and usually downloaded directly from the internet.

In the event that open source or freeware software is required, approval by the AST Manager in consultation with the IT Consultant 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 Trustees.

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 (i.e. number of computers or users etc.), then it is the responsibility of the person who downloads the software to ensure these terms are followed.

The IT Consultant is responsible for completing a software audit of all software twice a year to ensure that software copyrights and licence agreements are adhered to and report the result to the Trustees.

Software Installation

All software must be appropriately registered with the supplier where this is a requirement.

ASPCT is to be the registered owner of all software purchased by the Trust.

Only software obtained in accordance with this policy is to be installed on ASPCT computers.

All software installation is to be carried out by the IT Consultant or the AST Manager in consultation with the IT Consultant unless written permission is given by the Trustees to do otherwise.

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 this policy is to be used within the ASPCT.

Prior to the use of any software, the staff must receive instructions on any licensing agreements relating to the software, including any restrictions on use of the software.

Staff may require training for all new software. This includes new staff to be trained to use existing software appropriately. This will be the responsibility of the IT Consultant.

Employees are prohibited from bringing software from home and loading it onto the ASPCT hardware.

Unless express approval from the Trustees is obtained, software cannot be taken home and loaded on a staff person's home computer. Such approval may only be granted in line with licensing and copyright conditions.

Where staff are required to use software at home, an evaluation of providing them with a portable computer should be undertaken in the first instance. Where it is found that software can be used on their home computer, authorisation from the AST Manager 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 ASPCT and must be recorded on the software register by the IT Consultant.

Unauthorised software is prohibited from being used in the ASPCT. This includes the use of software owned by any staff and used within the ASPCT.

The unauthorised duplicating, acquiring or use of software copies is prohibited. Any staff person who makes, acquires, or uses unauthorised copies of software will be referred to the Trustees for further consultation. The illegal duplication of software or other copyrighted works is not condoned within the ASPCT and the Trustees will undertake disciplinary action where such event occurs.

Breach of Policy

Where there is a breach of this policy by a staff person, that person will be referred to the Trustees for further consultation.

Where a staff person is aware of a breach of the use of software in accordance with this policy, they are obliged to notify the Trustees immediately. In the event that the breach is not reported and it is determined that a staff person failed to report the breach, then that person will be referred to the Trustees for further consultation.

Additional Policies for Use of Software

Technology Hardware Policy

Getting Software policy

6. Bring Your Own Device Policy

At ASPCT the importance of mobile technologies for day to day work is recognized and staff may request the connection of their own mobile devices to ITEN. The following outlines the policy for mobile devices.

e) Procedures

Registration of personal mobile devices for business use

Both AST Users and non-AST Staff who have access to the ITEN must register their personal mobile device with the IT Consultant.

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

Personal mobile devices can only be used for the following ASPCT purposes: email and calendar access, business internet access, business telephone calls and contacts.

Each User who utilises personal mobile devices agrees:

- Not to download or transfer business or personal sensitive information to the device. Sensitive information includes intellectual property, financial records, and confidential employee details.
- Not to use the registered mobile device as the sole repository for ASPCT.
- To make every reasonable effort to ensure that ASPCT 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
- Not to share the device with other individuals to protect the business data access through the device.
- To abide by the conditions of this policy for appropriate use and access of internet sites etc.
- To notify ASPCT 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 ASPCT equipment.

All Users who have a registered personal mobile device for ASPCT use acknowledge that ASPCT:

- 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 being a User. The terminated User can request personal data be reinstated from back up data
- Has the right to deregister the device for ASPCT 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 Trustees grant an exemption. Any requests for exemptions from any of these directives, should be referred to the AST Manager.

Breach of this policy

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

f) Indemnity

Ann Street Presbyterian Church Trust bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of Users in accessing or using ITEN. All Users indemnify ASPCT against any and all damages, costs and expenses suffered by ASPCT 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 ASPCT.

7. Information Technology Security Policy

a) 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.

b) Physical Security

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

It will be the responsibility of the AST Manager to ensure that this requirement is followed at all times. Any User becoming aware of a breach to this security requirement is obliged to notify the Trustees immediately.

All security and safety of all portable technology (laptops, notepads, tablets, smart phones, etc.) will be the responsibility of the User to whom they have been issued. Each User is required to use passwords for login access 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 Trustees will assess the security measures undertaken to determine if the employee will be required to reimburse the business for the loss or damage.

All portable technology provided by the ASPCT when kept at the office is to be secured by passwords and locked doors.

c) Information Security

All sensitive, valuable, or critical business data is to be backed-up on the network server. No User is allowed to delete ASPCT data without express permission by the Trustees.

It is the responsibility of the IT Consultant to ensure that data back-ups are conducted and the backed up data is kept on the ASPCT server.

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

All information used within the business is to adhere to the privacy laws and the ASPCT's confidentiality requirements. At no time should access to sensitive, valuable or critical ASPCT data be given to anyone without express permission by the Trustees. Any User breaching this will be brought before the Trustees for further consultation.

d) Technology Access

Every User will be issued with a unique user name to access the Trust technology and will be required to use a password for access every time they log on to the server.

Each password is to be at least 8 characters composed of upper and lowercase letters, digits and non-alphanumeric characters. It is not to be shared with anyone and must be changed every 180 days.

The IT Consultant is responsible for the issuing of the unique username and initial password for all Users.

Where a staff person forgets the password or is ‘locked out’ after several attempts, then the IT Consultant 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.

The following table provides the authorisation of access:

Technology – Hardware/ Software	Persons authorised for access

Users are only authorised to use business computers for personal use provided it does not incur additional cost to the Trust, does not disrupt or interfere with their work or the operation of the Trust; and does not violate any state or federal law.

It is the responsibility of the AST Manager to keep all procedures for this policy up to date.

e) Systems Passwords

The IT Consultant will keep all system passwords. A copy of all system passwords will be kept in a sealed envelope in a secure place by the AST Manager. In case of an emergency the system passwords can be accessed in the presence of two Trustees who will sign a declaration as to the reason for accessing the systems passwords.

f) Software Passwords

All software passwords will be kept by the AST Manager. A copy of all software passwords will be kept in a sealed envelope in a secure place by the AST Manager. In case of an emergency the software passwords can be accessed in the presence of two Trustees who will sign a declaration as to the reason for accessing the systems passwords.

8. Information Technology Administration Policy

g) Purpose of the Policy

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

h) Procedures

All software installed and the licence information must be registered with the IT Consultant and listed in the Software Register. It is the responsibility of the IT Consultant to ensure to maintain the Register. 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.

The AST 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 IT Consultant and Trustees.

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

Any unspecified technology administration requirements should be directed to the AST Manager.

9. Emergency Management of Information Technology

i) Purpose of the Policy

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

j) Procedures

IT Hardware Failure

Where there is failure of any of the business's hardware, this must be referred to the Trust Manager immediately.

It is the responsibility of the Trust Manager to notify the Trustees and seek assistance from the IT Consultant in the event of IT hardware failure.

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

Virus or other security breach

In the event that the business's information technology is compromised by software virus or otherwise such breaches are to be reported to the IT Consultant immediately.

The IT Consultant is responsible for ensuring that any security breach is dealt with quickly to minimise disruption to business operations.