The Parish of
All Saints with St Margaret
Upper Norwood

Information Security Policy

TABLE OF CONTENTS

Introduction

This Policy document encompasses all aspects of security surrounding confidential church information and must be distributed to all church staff and volunteers. All church staff and volunteers must read this document in its entirety and sign the form confirming they have read and fully understand this policy. This document will be reviewed and updated by the Standing Committee and/or PCC of All Saints with St Margaret's on an annual basis or when relevant to include newly developed security standards into the policy and re-distributed to all staff, volunteers and contractors where applicable.

Information Security Policy

Information security involves preserving confidentiality, preventing unauthorised access and disclosure, maintaining the integrity of information, safeguarding accuracy and ensuring access to information when required by authorised users.

In addition to complying with this policy, all users must comply with the Data Protection Legislation and the Data Protection Policy.

'Church data' means any personal data processed by or on behalf of the church.

Information security is the responsibility of every member of staff, church member and volunteer using Church data on but not limited to the Church information systems. Our IT systems may only be used for authorised purposes. We will monitor the use of our systems from time to time. Any person using the IT systems for unauthorised purposes may be subject to disciplinary and/or legal proceedings.

We will ensure information security by:

- Ensuring appropriate software security measures are implemented and kept up to date;
- Making sure that only those who need access have that access;
- Not storing information where it can be accidentally exposed or lost;
- Making sure that if information has to be transported it is done so safely using encrypted devices or services.
- Access to systems on which information is stored must be password protected. Passwords must not be disclosed to others. If you have a

suspicion that your password has been compromised you must change it.

- You must ensure that any personally owned equipment which has been used to store or process Church data is disposed of securely. Software on personally owned devices must be kept up to date. Do not use unsecured wifi to process Church data.
- To recognize the rights of those whose data is used (eg the right to access of information held on themselves and the right to be forgotten)

The PCC of All Saints with St Margaret, Upper Norwood, handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect the cardholder data, cardholder privacy, and to ensure compliance with various regulations, along with guarding the future of the organisation.

The PCC of All Saints with St Margaret, Upper Norwood, commits to respecting the privacy of all its members and to protecting any customer data from outside parties. To this end the PCC are committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.

Staff and volunteers handling sensitive cardholder data should ensure:

- Handle church and cardholder information in a manner that fits with their sensitivity and classification;
- Limit personal use of the PCC of All Saints with St Margaret, Upper Norwood, information and telecommunication systems and ensure it doesn't interfere with your job performance;
- The PCC of All Saints with St Margaret, Upper Norwood, reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
- Do not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Do not disclose personnel information unless authorised;
- Protect sensitive cardholder information;
- Keep passwords and accounts secure;
- Request approval from the Vicar prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit approval from the Vicar;

- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended;
- Information security incidents must be reported, without delay, to the individual responsible for incident response locally: the Vicar.
- The Vicar may appoint at his discretion an Information Security Officer (ISO) to assist him/her by delegation on the duties outlined in this Policy. In that case, the ISO will have the same responsibilities and duties as outlined in this policy to the Vicar.

We each have a responsibility for ensuring our church's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager.

The PCC will receive an annual report on the number of data breaches / subject access requests, annually, from the Information Security Office (ISO) or Vicar.

Network Security

Network information must:

- Be stored using encryption.
- Be password protected where individuals can be identified on access.

All Network information within Church premises must be:

- Fully accessible to the Vicar and ISO at all times.
- Monitored by the Vicar and ISO at least once quarterly.

Acceptable Use Policy

The PCC's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to our established culture of openness, trust and integrity. The PCC is committed to protecting church members, staff and volunteers from illegal or damaging actions, either knowingly or unknowingly by individuals. The PCC will maintain an approved list of technologies and devices and personnel with access to such devices as detailed in Appendix B.

Access to Church devices which contain member's information, including but not only, all Church computers in the office, are restricted to those staff and volunteers with duties that require the use of such computers and are authorised by law to

access members information. No other member of the Church or external party must gain access to the computers, whether through a registered member's session or through a guest account. Guest accounts are never acceptable on Church devices.

Church staff and volunteers are responsible for exercising good judgment regarding the reasonableness of personal use.

Church staff and volunteers should take all necessary steps to prevent unauthorised access to confidential data.

Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts.

All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.

All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.

The List of Devices in Appendix B will be regularly updated when devices are modified, added or decommissioned. A stocktake of devices will be regularly performed and devices inspected to identify any potential tampering or substitution of devices.

Users should be trained in the ability to identify any suspicious behaviour where any tampering or substitution may be performed. Any suspicious behaviour will be reported accordingly.

Postings by church staff and volunteers from a Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of All Saints with St Margaret PCC, unless posting is in the course of business duties.

Church staff and volunteers must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Protect Stored Data

All sensitive cardholder data stored and handled by All Saints with St Margaret PCC and its church staff and volunteers must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by All Saints with St Margaret PCC for business reasons must be discarded in a secure and irrecoverable manner.

If there is no specific need to see the full PAN (Permanent Account Number), it has to be masked when displayed. PAN'S which are not protected as stated above should not be sent to the outside network via end user messaging technologies like chats, ICQ messenger etc.,

It is strictly prohibited to store:

- The contents of the payment card magnetic stripe (track data) on any media whatsoever.
- The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
- The PIN or the encrypted PIN Block under any circumstance.

Information Classification

Data and media containing data must always be labelled to indicate sensitivity level.

Confidential data might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to All Saints with St Margaret PCC if disclosed or modified. Confidential data includes cardholder data.

Internal Use data might include information that the data owner feels should be protected to prevent unauthorised disclosure.

Public data is information that may be freely disseminated.

Access to the Sensitive Cardholder Data

All Access to sensitive cardholder should be controlled and authorised. Any job functions that require access to cardholder data should be clearly defined.

Any display of the card holder should be restricted at a minimum to the first 6 and the last 4 digits of the cardholder data.

Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to church staff and volunteers that have a legitimate need to view such information.
No other church staff and volunteers should have access to this confidential data unless they have a genuine business need.

If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained as detailed in Appendix C.

All Saints with St Margaret PCC will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the for the cardholder data that the Service Provider possess.

All Saints with St Margaret PCC will ensure that a there is an established process, including proper due diligence is in place, before engaging with a Service provider.

All Saints with St Margaret PCC will have a process in place to monitor the PCI DSS compliance status of the Service provider.

Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.

Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.

Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.

Procedures must be in place to help all personnel easily distinguish between church staff and volunteers and visitors, especially in areas where cardholder data is accessible. "Employee" refers to full-time and part-time church staff and volunteers, temporary church staff and volunteers and personnel, and consultants who are "resident" on Company sites. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to physically enter the premises for a short duration, usually not more than one day.

A list of devices that accept payment card data should be maintained. The list should include make, model and location of the device. The list should have the serial number or a unique identifier of the device. The list should be updated when devices are added, removed or relocated POS devices surfaces are periodically inspected to detect tampering or substitution. Personnel using the devices should be trained and aware of handling the POS devices. Personnel using the devices should verify the identity of and=y third party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices. Personnel using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the appropriate personnel. All Saints with St Margaret PCC sites. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
Strict control is maintained over the external or internal distribution of any media containing card holder data and has to be approved by management. Strict control is maintained over the storage and accessibility of media. All computer that store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use.

Protect Data in Transit

All sensitive data must be protected securely if it is to be transported physically or electronically. Member's data must never be sent over the internet via email, instant chat or any other end user technologies. If there is a business justification to send member's data via email or by any other mode then it should be done after authorization by the Vicar or ISO and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, IPSEC, etc.).

Disposal of Stored Data

All data must be securely disposed of when no longer required by All Saints with St Margaret PCC, regardless of the media or application type on which it is stored.

An automatic process must exist to permanently delete on-line data, when no longer required.

All hard copies of cardholder data must be manually destroyed when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.

All Saints with St Margaret PCC will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.

All Saints with St Margaret PCC will have documented procedures for the destruction of electronic media. These will require:

- All member's data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media;
- If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.
- All cardholder information awaiting destruction must be held in lockable storage containers clearly marked "To Be Shredded" - access to these containers must be restricted.

Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into church practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all church staff and volunteers and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day company practice.

- Distribute this security policy document to all church staff and volunteers to read. It is required that all church staff and volunteers confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A).
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).
- Company security policies must be reviewed annually and updated as needed.

Credit Card (PCI) Security Incident Response Plan

All Saints with St Margaret's PCI Security Incident Response Team (PCI Response Team) is comprised of the Vicar, the Information Security Officer and Merchant Services. All Saints with St Margaret PCC PCI security incident response plan is as follows:

1. An incident must be reported to the Vicar or Information Security Officer.
2. On receiving the report they will advise the PCI Response Team of the incident.
3. The PCI Response Team will investigate the incident and assist the potentially compromised in limiting the exposure of data and in mitigating the risks associated with the incident.
4. The PCI Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary.
5. The PCI Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.

Information Security PCI Incident Response Procedures:
A member of staff or volunteer that reasonably believes it may have an account breach, or a breach of cardholder information or of systems related to the PCI environment in general, must inform All Saints with St Margaret PCI Incident Response Team. After being notified of a compromise, the PCI Response Team, along with other designated staff, will implement the PCI Incident Response Plan to assist and augment departments' response plans.

Incident Response Notification

Escalation Members:

Escalation – First Level:

- The Vicar
- The Information Security Officer
- Executive for Credit Collections Company and Merchant Services Legal Counsel
- Risk Manager (usually, the Churchwardens unless delegated otherwise)

Escalation – Second Level:

- All Saints with St Margaret PCC
- Standing Committee

External Contacts (as needed):

- Merchant Provider Card Brands
- Internet Service Provider (if applicable)
- Internet Service Provider of Intruder (if applicable) Communication Carriers (local and long distance) Business Partners
- Insurance Carrier
- External Response Team as applicable (CERT Coordination Center 1, etc) Law Enforcement Agencies as applicable inn local jurisdiction

In response to a systems compromise, the PCI Response Team and designees will:

- Ensure compromised system/s is isolated on/from the network.
- Gather, review and analyze the logs and related information from various central and local safeguards and security controls
- Conduct appropriate forensic analysis of compromised system.
- Contact internal and external departments and entities as appropriate.
- Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required.
- Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.

The credit card companies have individually specific requirements that the Response Team must address in reporting suspected or confirmed breaches of cardholder data.

Transfer of Sensitive Information Policy

- All third-party companies providing critical services to All Saints with St Margaret PCC must provide an agreed Service Level Agreement.
- All third-party companies providing hosting facilities must comply with All Saints with St Margaret PCC's Physical Security and Access Control Policy.
- All third-party companies which have access to Card Holder information must:
  - Adhere to the PCI DSS security requirements.
  - Acknowledge their responsibility for securing the Card Holder data.
  - Acknowledge that the Card Holder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law.
  - Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure.
  - Provide full cooperation and access to conduct a thorough security review after a security intrusion by a Payment Card industry representative, or a Payment Card industry approved third party.

User Access Management

Access to Church data and computer devices is controlled through a formal user registration process. Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out.

There is a standard level of access; other services can be accessed when specifically authorized by the Vicar, ISO or following the approval by the PCC or Standing Committee. The job function of the user decides the level of access the staff member or volunteer has to data.

Each user will be given a copy of their new user form to provide a written statement of their access rights, signed by an IT representative after their induction procedure. The user signs the form indicating that they understand the conditions of access. Access to all All Saints with St Margaret PCC systems is provided by the Vicar, ISO or PCC and can only be started after proper procedures are completed.

As soon as an individual leaves All Saints with St Margaret PCC employment, all his/her system logons must be immediately revoked.

Access Control Policy

Access Control systems are in place to protect the interests of all users of All Saints with St Margaret PCC computer systems by providing a safe, secure and readily accessible environment in which to work.

All Saints with St Margaret PCC will provide all church staff and volunteers and other users with the information they need to carry out their responsibilities in an as effective and efficient manner as possible.

Generic or group IDs shall not normally be permitted, but may be granted under *exceptional* circumstances if sufficient other controls on access are in place following written authorisation by the Vicar or ISO. This access must be time limited and restricted to the minimum necessary. The written record of authorisation and access must be kept by the Parish Administrator.

The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorization provided by the Vicar. It should be restricted to the Vicar and ISO **only**.

Access rights will be accorded following the principles of least privilege and need to know.

Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.

Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification.
Access to All Saints with St Margaret PCC IT resources and services will be given through the provision of a unique Active DiVicary account and complex password.

No access to any All Saints with St Margaret PCC IT resources and services will be provided without prior authentication and authorization of a user's All Saints with St Margaret PCC Windows Active DiVicary account.

Password issuing, strength requirements, changing and control will be managed through formal processes. Password length, complexity and expiration times will be controlled through Windows Active DiVicary Group Policy Objects.

Access to Confidential, Restricted and Protected information will be limited to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed or revoked must be made in writing.

Users are expected to become familiar with and abide by All Saints with St Margaret PCC policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.

Access for remote users shall be subject to authorization by the Vicar or ISO and be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.

Access to data is variously and appropriately controlled according to the data classification levels described in the Information Security Management Policy.

Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, SQL database rights, isolated networks and other methods as necessary.

A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT Services to review users' access rights. The review shall be logged and IT Services shall sign off the review to give authority for users' continued access rights.

Appendix A: Agreement to Comply Form

THE PCC OF
ALL SAINTS WITH ST MARGARET, UPPER NORWOOD

AGREEMENT TO COMPLY WITH
INFORMATION SECURITY POLICIES

Full Name: .....

Role/Position: .....

I agree to take all reasonable precautions to assure that company internal information, or information that has been entrusted to All Saints with St Margaret PCC by third parties such as (but not only) members and volunteers, will not be disclosed to unauthorised persons. At the end of my employment, or contract, or when I no longer volunteer with All Saints with St Margaret PCC, I agree to return all information to which I have had access as a result of my position.

I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal manager who is the designated information owner.

I have access to a copy of the *Information Security Policies*, I have read and understand these policies, and I understand how it impacts my job. As a condition of continued employment (paid or volunteer), I agree to abide by the policies and other requirements found in All Saints with St Margaret PCC security policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of information security policies to the Rector and/or the designated Information Security Officer.

Signed -

Date -

Appendix B – List of Devices

Asset / Device Name	Description	Owner / Approved User(s)	Location

Appendix C - List of Service Providers

Name of Service Provider	Contact Details	Services Provided	PCI DSS Compliant & PCI DSS Validation date

This Policy was approved by the PCC on 10 January 2023.

This policy will be reviewed after four years.