2018

LIFE CHURCH

# Information Security Policy v1.0

WORD OF LIFE CHURCH (POOLE)

AUTHOR: KELVIN PAPP

ISSUE DATE: MAY 23, 2018

# Table of Contents

# INTRODUCTION

This Policy document encompasses all aspects of security surrounding the handling of confidential and personal data and must be distributed to all individuals engaged in an administrative capacity. This includes (but is not limited to) trustees, employees, office workers, and those volunteers involved in the collection / processing of personal or confidential data.

All volunteers must read this document in its entirety and sign a copy to indicate that they have read and fully understood its contents.

This document will be reviewed and updated (if necessary) by the board of trustees on an annual basis, or when relevant to incorporate changes to legislation or security standards into the policy. It will be redistributed where applicable.

# AIM AND PURPOSE OF THIS POLICY

Word of Life Church (Poole) handles personal data, and confidential information daily. This information must have adequate safeguards in place to protect those it relates to, the organisation, and to ensure compliance with various regulations such as (but not limited to) the General Data Protection Regulation (GDPR).

## WHO DOES THIS POLICY APPLY TO?

This policy is approved by the board of trustees and applies to:

- Our trustees, staff, and team members (both paid and voluntary)
- Any individual involved in the collection or processing of personal data on behalf of the charity
- Any individual involved in the collection or processing of payments

## CONCERNS, COMPLAINTS, AND COMPLIMENTS

Should anyone have any concerns, complaints, or feedback in relation to this policy please contact:

| | |
|---|---|
| Name: | Kelvin Papp |
| Telephone Number: | +44 7967 967017 |
| Email Address: | kelvin@lifechurchpoole.com |

If would be helpful to have complaints in writing as this avoids any possible misunderstanding. Whether verbal or in writing, complaints will be acted upon at the earliest convenience. The target response for written complains written complaints is 10 days.

## DOCUMENT REVIEW

The trustees will review this policy annually, amending and updating it as required. Communication of changes will be distributed to those effected.

| | |
|---|---|
| Date of Most Recent Review: | 23rd May 2018 |
| Date of Next Review: | 23rd May 2019 |
| Signed (on behalf of Church Trustees): | Steve Martin (Chairman) |

# OVERVIEW

Word of Life Church (Poole) commits to respecting the privacy of all of its users, and to protecting any personal data from unauthorised access. To this end the board are committed to maintaining a secure environment for the control and processing of such data.

Those handling of confidential or personal data should ensure that:

- Information is handled in a manner that fits with its sensitivity and classification;
- Personal data will not be disclosed unless authorised;
- Sensitive information (for example, cardholder data) is protected;
- Any passwords, accounts, or access codes used to secure areas are not disclosed unless authorised;
- Guidance is sought for changes that effect equipment storing or processing personal data;
- Desks and working areas are kept clear of sensitive data;
- Devices containing personal data are locked / password protected when unattended;
- Information security incidents must be reported, without delay, to a Trustee

In addition:

- Charity resources are not to be used to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Word of Life Church (Poole) reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic to validate the application of the provisions outlined within this policy;

We each have a responsibility for ensuring our 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 from a trustee.

# DEFINITIONS

**Anonymisation / Pseudonymisation:** Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a "key" that allows the data to be re-identified.

**Consent:** Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

**Data Breach:** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

**Data Controller:** Any individual (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data is to be processed.

**Data Processor:** An individual (other than an employee of the data controller) who processes the data on behalf of the data controller.

**Data Protection:** The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.

**Data Subject:** The identified or Identifiable Natural Person to which the data refers.

**Identifiable Natural Person:** Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Media:** Any printed or handwritten document, received faxes or emails, USB hard drives, CD or DVD Discs, computer hard drives, etc.

**Personal Data:** Any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person.

**Processed / Processing:** Any operation or set of operations performed on Personal Data or on sets of Personal Data. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**The Church / Charity**: A reference to the Word of Life Church (Poole) organisation and its associated operational structure, including trustees, employees, office workers, and those volunteers involved in the collection and processing of personal or confidential data.

# DATA PROTECTION PRINCIPLES

Word of Life Church (Poole) has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data:

## LAWFULNESS, FAIRNESS AND TRANSPARENCY

Personal Data will be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means that the charity must tell the Data Subject what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).

## PURPOSE LIMITATION

Personal Data will be collected for specified, explicit and legitimate purposes and Processed in a way that is compatible with those purposes. This means that the charity must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only that which is necessary to meet the specified purpose.

## DATA MINIMISATION

Personal Data will be adequate, relevant and limited to what is necessary. This means that the charity will not store any Personal Data beyond that that which is strictly required.

## ACCURACY

Personal Data will be accurate and kept up to date. This means that the charity will have processes in place to identify and address out-of-date, incorrect, or redundant Personal Data.

## STORAGE LIMITATION

Personal Data will be kept in a form which permits identification of Data Subjects for no longer than is necessary. This means that the charity will, wherever possible, store Personal Data for only as long as is needed to support its objectives, or where needed to satisfy legislative or regulatory requirements.

## INTEGRITY & CONFIDENTIALITY

Personal Data will be Processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful Processing, accidental loss, destruction, or damage. The charity will use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data at all times.

## ACCOUNTABILITY

The board of trustees will be responsible for and able to demonstrate compliance with this policy. This means the charity must demonstrate that the data protection principles outlined above are met for all Personal Data for which it is responsible.

# INFORMATION SECURITY POLICY

## COLLECTION OF PERSONAL DATA

Word of Life Church (Poole) will only obtain Personal Data in support of its objectives through lawful and fair means and with the knowledge and consent of the individual concerned. Such consent for the collection, processing, and / or transfer of their Personal Data will be established through the following principles:

- Ensuring that the request for consent is presented in a manner which is clearly distinguishable, using clear and plain language.
- Ensuring the consent is freely given.
- Documenting the date, method and content of the consent, in addition to its intended use.
- Providing a simple method for a Data Subject to withdraw their Consent at any time.

Consent may be provided electronically, or in writing.

Children are unable to consent to the Processing of Personal Data. Consent must be sought from the person who holds parental responsibility over the child

## DATA PROCESSING

Word of Life Church (Poole) uses the Personal Data it collects for the following broad purposes:

- The general running and administration of the charity.
- To fulfil the objectives of the charity, including the provision of pastoral care to its attendees

The use of a personal information should always be considered from the individuals perspective – considering whether its use for the intended purpose would align with the consent under which it was provided. For example, the provision of pastoral care to a church member who has provided details on a church contact form would likely be legitimate, however the passing on of details to a third party to support the targeting of other services would not.

There are some circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the Personal Data was collected. In any circumstance where consent has not been expressly provided for specific activity being completed, the following additional conditions must be considered to determine the fairness and transparency of any further processing:

- Any link between the purpose for which the Personal Data was collected and the reasons for intended further processing.
- The context in which the Personal Data has been collected, in particular the relationship between the Data Subject and the Data Controller.
- The possible consequences of the intended further processing for the Data Subject.
- The existence of appropriate safeguards relating to further Processing, which may include encryption, anonymisation or pseudonymisation.

## DATA QUALITY

Word of Life Church (Poole) will adopt all necessary measures to ensure that the Personal Data it collects and Processes is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject.

The measures adopted by the charity to ensure data quality include:

- Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification.
- Keeping Personal Data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required.
- Restriction, rather than deletion of Personal Data where:
    - The law prohibits erasure
    - Erasure would impair the legitimate interests of the Data Subject
    - The Data Subject disputes that their Personal Data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

Word of Life Church (Poole) will contact individuals on an annual basis to request confirmation that any details collected remain unchanged.

## NETWORK SECURITY

The IT systems and equipment in use at Word of Life Church (Poole) are not intended or secured to conform to recognised standards (such as Payment Card Industry Data Security (PCI DSS), or Cyber Essentials). However, technical, procedural and organisational measures are in place to protect against accidental loss or destruction of personal / sensitive data. These include encryption of the data at rest and in transit (where possible), and measures to securely dispose of IT hardware at the point of replacement.

Cardholder data resulting from payment transactions should never be stored electronically.

Personal Data relating to individuals attending the church is stored electronically to support the day to day operations of the charity. This includes the provision of pastoral care, general charity administration, and financial auditing requirements (e.g. Gift Aid submission).

## ACCEPTABLE USE POLICY

The intentions in publishing an acceptable use policy are not intended to impose restrictions that are contrary to the established culture at the church of openness, trust and integrity. The purpose of these guidelines is to ensure the protection of all individuals from illegal or damaging actions, either knowingly or unknowingly.

- Individuals are responsible for exercising good judgment when it comes to the reasonableness of using charity equipment for personal use.

- Individuals should take all necessary steps to prevent unauthorised access to data falling within the scope of this policy.
- Passwords should be kept secure and not shared with others. Authorised users are responsible for the security of their passwords and accounts.
- All PCs, laptops, workstations, tablets, and mobile devices involved in the processing of personal or confidential data should be secured with passwords that are automatically activated.
- All PIN entry devices should be subject to appropriate physical protection, so they cannot be tampered with or altered. Those making use of PIN entry devices should ensure that they are regularly checked for signs of suspicious activity.
- Individuals should be able to identify suspicious behaviour, where any tampering or substitution may have been performed. Any suspicious behaviour must be reported immediately.
- Information contained on laptop, tablet, and mobile devices is especially vulnerable. Special care should be exercised when in possession of these devices.
- Postings by individuals from a charity email address (or associated username) to websites should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the charity (unless posting in support of organisational activity).
- Individuals must use extreme caution when opening e-mail attachments or website links received from unknown senders, which may contain viruses, or malware.

## PROTECTION OF STORED DATA

- All personal and sensitive data stored and processed by the Charity must be securely protected against unauthorised use or access. Any data that is no longer required by the Charity for operational reasons must be discarded in a secure and irrecoverable manner.
- If there is no specific need to see the full Primary Account Number (PAN) on the card payment merchant receipt, it should be masked when displayed.
- PAN's which are not protected as stated above should never be transmitted electronically to the outside network through end user technologies such as Skype, Dropbox, GoTo Meeting etc.

It is strictly prohibited to store:

- The Primary Account Number (PAN) from a card payment merchant receipt on any Word of Life Church (Poole) IT Equipment.
- The contents of the payment card magnetic stripe (track data) on any media whatsoever.
- The CVV/CVC (the 3 numbers 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 personal data must always be labelled to indicate its sensitivity level:

- **Confidential Data** might include information assets for which there are legal requirements for preventing disclosure, financial penalties for disclosure, or data that would cause severe damage to the Charity 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. This includes Personal Data used within the course of normal operation.
- **Public** data is information that may be freely distributed.

## ACCESS TO / SHARING OF DATA

All access to sensitive data will be controlled and authorised.

- Access to sensitive information such as PAN's, other cardholder data, and Personal Data is restricted to users that have a legitimate need to view such information.
- No other individuals should have access to these data types unless they have a genuine need aligned with a Charity objective or requirement.
- If cardholder data needs to be shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained by the charity. At the time of writing, this is not a requirement.
- Should this become a requirement, the charity will ensure a written agreement including an acknowledgement that the Service Provider will be responsible for any data within scope is created.
- A mandatory component of any such agreement will be verification that the 3rd party is compliant with PCI DSS obligations.
- In the case of Personal Data, sharing is prohibited by this policy except where the charity is required to provide such data in accordance with enforcement of the law or with the agreement of the Data Subject (see below).
- Media containing confidential or Personal Data must always be handled and distributed in a secure manner with consideration applied to the nature of the working environment.
- Visitors must always be escorted by a trusted individual aligned to the charity when in areas that enable access to Personal Data. A visitor is defined as a vendor, guest of a trustee / employee / volunteer, service personnel, or anyone who needs to physically enter the premises for a short duration (such as a Church service).
- Point of Sale (POS) devices must be periodically inspected to detect tampering or substitution.
- Volunteers using POS Devices should verify the identity of any third-party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices. In the event of doubt, a trustee should be notified.
- Volunteers must report suspicious behaviour and indications of tampering to a Trustee.
- Strict control is maintained over the storage and accessibility of media. Merchant receipts will be placed into secure storage at the earliest opportunity following the processing of a transaction.
- No sensitive cardholder data should be stored on computer equipment.

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or Consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- By the order of a court or by any rule of law.

If the charity Processes Personal Data for one of these purposes, then it may apply an exception to the Processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question.

## PROTECTION OF DATA IN TRANSIT

All sensitive data must be protected securely if it is to be transported, physically or electronically.

- Card holder data (PAN, track data, etc.) must never be sent over the internet via email, instant message or any other end user technologies. Under no circumstance should such data be transcoded electronically for transmission via IT Systems.
- The transportation of media containing confidential or Personal Data to support 3rd party access (if required) must be authorised by a trustee and logged / inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media.
- If there is a justification to send Personal (non-cardholder) data via email or by any other medium it should be done only with trustee authorisation and via the use of a strong encryption mechanism (i.e. AES encryption, PGP encryption, IPSEC, etc.).

## DISPOSAL OF STORED DATA

- All data will be securely disposed of when no longer required by the charity, regardless of the media or application type on which it is stored.
- A quarterly review of electronic data should be undertaken by device / data owners with a view to deleting data which is no longer required.
- All hard copies of Personal Data must be destroyed when no longer required. The use of hard copies of such data is discouraged.
- A quarterly process must be in place to confirm that card machine merchant receipts that are no longer required for accounting purposes have been destroyed.
- It is a requirement that all hard copies of Personal or confidential data are crosscut shredded, incinerated or pulped so they cannot be reconstructed at the point of disposal.
- All data awaiting destruction must be held in secured storage containers clearly marked “To Be Shredded”. Access to these containers is to be restricted.

## SECURITY AWARENESS AND PROCEDURES

The policies and procedures outlined within this document must be incorporated into regular practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and volunteers.

To this end, the charity will ensure that:

- Regular reviews of handling procedures for confidential and Personal data will be undertaken, along with periodic security awareness meetings to incorporate these procedures into day to day operation.
- This security policy document will be distributed to all to all individuals engaged in an administrative capacity or involved in the collection / processing of personal data or payments. It is a requirement

that all such individuals confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A).
- This Information Security Policy will be reviewed annually and updated as needed.

## CREDIT CARD (PCI) SECURITY INCIDENT RESPONSE PLAN

The Word of Life Church (Poole) PCI Security Incident Response Team (PCI Response Team) is comprised of the Charity trustees and Merchant Services. The Word of Life Church (Poole) PCI security incident response plan is as follows:

- Any incident will be reported immediately to a member of the PCI Response Team.
- The PCI Response Team will investigate the incident and seek to limit the exposure of cardholder data, and to mitigate the risks associated with the incident.
- 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.
- 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.

An individual that reasonably believes that a breach of cardholder information has occurred must inform the 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.

A response plan to accommodate a systems compromise is not required given the absence of the need to use IT Systems in support of card payment processing at Word of Life Church (Poole).

Credit card companies have individual, specific requirements that the Response Team will address when reporting suspected or confirmed breaches of cardholder data. Upon confirmation that a security breach has occurred, a member of the PCI Response Team will alert all relevant parties affected by the compromise.

## SUBJECT ACCESS REQUESTS

The charity will accommodate requests to enable and facilitate the exercise of Data Subject rights related to:

- Information access.
- Objection to Processing.
- Restriction of Processing.
- Data portability.
- Data rectification.
- Data erasure.

If an individual makes a request relating to any of the rights listed above, the charity will consider each such request in accordance with all applicable Data Protection laws and regulations. No administration fee will be

charged for considering and / or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data Subjects are entitled to obtain, based upon a request made in writing to the Office of Data Protection and upon successful verification of their identity, the following information about their own Personal Data:

- The purposes of the collection, Processing, use and storage of their Personal Data.
- The source(s) of the Personal Data, if it was not obtained from the Data Subject;
- The categories of Personal Data stored for the Data Subject.
- The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients.
- The envisaged period of storage for the Personal Data or the rationale for determining the storage period.

All requests received for access to or rectification of Personal Data must be directed to the board of trustees who will record each request as it is received. A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative. Data Subjects shall have the right to require the charity to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If the charity cannot respond fully to the request within 30 days, the trustees will make available the following information to the Data Subject, or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request.
- Any information located to date.
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided.
- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature).
- The name and contact information of the individual who should be contacted for follow up.

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information will be redacted or withheld as may be necessary or appropriate to protect that person's rights.

## BREACH REPORTING

Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Data must immediately notify a trustee, providing a description of what occurred.

All reported incidents will be investigated to confirm whether or not a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, the charity will follow the relevant authorised procedure based on the criticality and quantity of the Personal Data involved. For severe Personal Data Breaches, the board of trustees will schedule an emergency meeting to coordinate and manage the Personal Data Breach response.

# APPENDICIES

## APPENDIX 1: INFORMATION SECURITY POLICY ACKNOWLEDGEMENT

**Volunteer Name (Print):**

I agree to take all reasonable precautions to ensure that sensitive information entrusted to Word of Life Church (Poole) will not be disclosed to unauthorised persons.

I understand that I am not authorised to use confidential or Personal Data obtained by the charity for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of a trustee.

I have access to a copy of the Information Security Policy, I have read and understand it, and I understand how it impacts the areas I operate within.

I agree to abide by the policies and other requirements found in the Information Security Policy. I understand that non-compliance may lead to criminal and / or civil penalties.

I also agree to promptly report all violations or suspected violations of this Information Security Policy to a trustee.

Signature: .....

Print Name: .....

Date: .....