Culver Church (CC) – Internal document

Document Number: **CCPOL2019** Version: **1.0**	Date Created: **23 January 2019**
Document Description: **Data Protection Policy**	Date Last Updated: **23 January 2019**
7Review Frequency: **Annual**	Maintained by: **CC Data Controller**
Reviewers: Church Leaders	Authorised by: **Church Leaders**

1.0 INTRODUCTION

The General Data Protection Regulation (GDPR) 2018 regulates the processing of information relating to individuals (employees, volunteers, supporters, service consumers, members and trustees). This includes the obtaining, holding, using or disclosing of such information, and covers computerised records as well as manual filing systems and card indexes.

Culver Church (CC) will hold the minimum personal information necessary to enable it to perform its functions. All such information is confidential and needs to be treated with care, to comply with the law.

2.0 SUMMARY OF PRINCIPLES

Data users must comply with the Data Protection principles of good practice which underpin the Act these state that personal data shall:

- Be obtained and processed fairly and lawfully
- Be held under a legal basis which can be - contract, legal obligation, vital interest, public task, legitimate interest or consent.
- Be held only for specified purposes
- Be adequate, relevant but not excessive
- Be accurate and kept up to date.
- Be held for no longer than necessary
- Be accessible to data subjects.
- Be subject to the appropriate security measures.
- Not be transferred outside the EEA (European Economic Area)

Culver Church and all staff / volunteers who process, or use personal data must ensure that they abide by these principles at all times. This policy has been developed to ensure this happens.

3.0 REQUIREMENTS OF THE ACT (NOTIFICATIONS & REGISTRATION)

CC staff / volunteers must notify the CC Data Controller of any filing system or computer database that contains (or will contain) personal data (e.g. name and address). This should include details on how the data is/will be used, where it is stored and the legal basis for holding it. This notification will then be added to the CC's registration that is held by the Information Commissioner for approval.

A retention policy will be prepared and managed by the Data Controller. This will list retention and data review periods for personal data records.

A review/audit of data being held across the organisation will be carried out by the CC data Controller (or nominated deputy) on an annual basis.

As part of the annual review the CC data controller will refer to the checklist on the ICO website to ensure we are up to date with compliance issues.

4.0 RESPONSIBILITIES OF STAFF / VOLUNTEERS

CC is the 'data controller' under the Act and is therefore ultimately responsible for implementation. However day to day matters, the registration of systems and requests for access will be dealt with by the 'CC Data Controller'.

It is the responsibility of the CC Data Controller to:

- Assess the understanding of the obligations of CC under GDPR
- Be aware of our current compliance status
- Identify and monitor problem areas and risks and recommend solutions
- Promote clear and effective procedures and offer guidance to staff on data protection issues.

It is **NOT** the responsibility of the CC Data Controller to apply the provisions of GDPR. This is the responsibility of the individual collectors, keepers and users of personal data. Therefore staff / volunteers are required to be aware of the provisions of GDPR, such as keeping records up to date and accurate, and its impact on the work they undertake on behalf of CC.

It is the responsibility of the Activity Leaders to identify all computer and manual systems within their respective service areas that contain personal data and to keep the CC Data Controller informed for notification purposes.

Any breach of the Data Protection Policy, whether deliberate, or through negligence may lead to disciplinary action being taken or even a criminal prosecution.

5.0 DATA SECURITY

All staff /volunteers are responsible for ensuring that:

- Any personal data they hold, whether in electronic or paper format, is kept securely.
- Personal information is not disclosed deliberately or accidentally either orally or in writing to any unauthorised third party.

There are a number of good practices that staff / volunteers should follow

- In emails with multiple recipients, especially going outside of CC, the blind ccs option should be used in order not to circulate contact details to all recipients.
- All technology and other storage devices should be password protected in order to minimise the risk of a data breach.

6.0 REQUESTS FOR ACCESS TO / CORRECTIONS TO / ERASURE OF / RESTRICTION ON PROCESSING / DATA PORTABILITY OF PERSONAL DATA

CC employees, volunteers, supporters, service consumers, members and trustees have the right to access personal data that is being kept about them insofar as it falls within the scope of GDPR, if appropriate request that corrections are made if there are inaccuracies, request that the data to be erased, request the restrictions are put on the processing of their personal data or to request a copy of the personal data held on them so that they can transfer it to another organisation.

Any person wishing to exercise any of their rights above should make their request in writing to the CC Data Controller.

CC aims to comply with requests as quickly as possible, but the CC must comply with a request within thirty days of receipt of the request.

CC does not need to comply with a request for access to personal information where it has received an identical or similar request from the same individual unless a reasonable interval has elapsed between compliance with the original request and the current request.

CC does not need to rectify data if: (a) it is believed the data is correct (b) if it is a reasonable opinion and the person whose opinion it is is recorded, or (c) if the claim is manifestly unfounded or excessive - taking into account if the request is repetitive in nature. If CC decides not to rectify data in line with a request they will notify the person requesting the notification and explain the decision, whilst making the requester aware of their right to make a complaint to the ICO or another supervisory body.

CC does not need to erase personal data if it is necessary to comply with a legal obligation, if it is needed for the performance of a task in the public interest or in the exercise of a public authority.

7.0 SUBJECT CONSENTS

For every activity or event where personal data is obtained it is the responsibility of the activity or event leader to agree with the CC Data Controller the legal basis for holding the data. If the basis of holding the data is Consent, the activity leader must obtain specific consent from individuals before capturing and storing their personal information. This consent must include:

- The legal basis for requesting that information
- What the information will be used for and/or who it will be shared with
- The length of time it will be held for
- Specific approval for how to contact the individual
- Information on their rights to remove consent
- How to obtain a copy of CC's data privacy notice (see Appendix 1)