Cornerstone Collective
Data Protection Policy

Version:	2.0
Date of Issue:	20th July 2021
Review Date:	Within 1 year from date of issue
Applicability:	This policy is applicable to all churches under the name 'Cornerstone Collective of Churches'.
Summary:	This document provides details of the management of data in relation to data protection laws.
Document Owner:	Anna Wood

Contents

1. Introduction

As a registered charity Cornerstone Collective is required to comply with UK and EU data protection laws. Data protection policies are designed to protect information, in particular personal data, which is important to Cornerstone Collective Churches, its employees, congregation members, suppliers and any other individuals associated with the running of Cornerstone Collective.

Having relevant policies in place also enable Cornerstone Collective to comply with applicable data protection legislation and regulations, including the EU General Data Protection Regulation 2016/679 (GDPR).

This document is the over-arching policy relating to data protection for Cornerstone Collective, other data management policies sit alongside this policy to ensure that Cornerstone Collective of Churches comply with legal legislation.

2. Data Protection Principles and Requirements

The following principles must be complied with in relation to the processing of all data, and any personal data that is processed must be compliant with these:

- personal data must be processed in a fair, lawful and transparent manner
- personal data must be obtained only for one (or more) specific, explicit and legitimate purpose(s) and must not be further processed in any manner incompatible with that/those purpose(s)
- personal data must be adequate, relevant and not excessive in relation to the purpose(s) for which it is processed
- personal data must be accurate and, where necessary kept up to date, with every reasonable step having been taken to ensure that personal data that is inaccurate (with regard to the purpose(s) for which it is processed) is immediately deleted or rectified
- personal data processed for any purpose(s) must not be kept longer than necessary to meet that/those purpose(s)
- appropriate technical and organisational measures must be taken against unauthorised or unlawful data collection or processing.

When data is processed it should be considered as to whether Cornerstone Collective are the Data Controller or Data Processor (see definitions). In most instances Cornerstone Collective would be considered the Data Controller i.e. when it gathers information directly from the data subjects i.e. employees or Church members.

2.1.Rights of the Data Subjects

Personal data must be processed in accordance with the rights of data subjects. Data subjects generally have the ability to have access to their personal data upon request and may also be entitled to a number of other rights including:

- the right to rectification of inaccurate personal data
- the right to erase/delete personal data, commonly referred to as the "right to be forgotten"
- the right to restrict processing under certain circumstances
- the right to data portability
- the right to object (i.e. where personal data are processed for direct marketing purposes) to automated individual decision-making

In the circumstance that a data subject access request form is submitted, for example by an employee, the request should be managed in accordance with the Data Subject Access Request Policy. In accordance with GDPR, requests are to be responded to within one calendar month, and any requests should be logged in accordance with the Data Subject Access Request Policy. All requests received should be referred to the Operations Director immediately.

2.2.Privacy Notices

It is a requirement that data subjects must be informed of the following:

- How their personal data is used, including about the types of data collected
- The purposes for which the data are collected
- Any third party to whom their personal data may be disclosed
- The rights available to them

It is the responsibility of Cornerstone Collective to inform data subjects the purpose for which their data will be used. Any personal data kept by Cornerstone Collective should be used and processed in accordance to what was notified to the data subject at the time that consent was provided. If further or alternative use is needed consent must be sought from the data subject and acceptance must be provided in writing, this would be completed in the method of another privacy notice.

As stated in Section 2, in many circumstances Cornerstone Collective will act as the Data Controller, therefore it is important that any gathering of data must be justifiable. In many cases it should be for the following:

- Consent provided by the data subject (not required for employees)
- Necessary to comply with a legal obligation

Sensitive personal data should only be processed where it is absolutely necessary to do so. Additional consideration should be given to the secure storage and transmission of sensitive personal data, and access rights should be strictly limited. One of the following conditions must be satisfied in order to process sensitive personal data:

- the explicit consent of the data subject must be obtained, except where consent is precluded under applicable laws;
- the processing must be necessary for an obligation of Cornerstone Collective as an employer under employment law;
- the vital interests of the data subject need to be protected (e.g. in a medical emergency or other life or death situation); or
- the processing must be necessary for the purpose of legal proceedings or obtaining legal advice.

If at any point Cornerstone Collective are looking to implement new technology or considering changing the processes in which the storage of personal data is affected then it is recommended that a Data Protection Impact Assessment (DPIA's) is carried out, further information of DPIA's can be found the Information Commissioners Office's website (www.ico.co.uk).

2.3.Gaining Consent for Children

For some processes within Cornerstone Collective is it required that we collect personal/sensitive data relating to children. The gathering and processing of a child's data (considered as being under 18 years of age) require particular attention as the child(ren) may not be aware of the risks involved.

The measures detailed in section 2 of this document are still relevant when processing children's data and compliance with data protection principles should be central when processing and managing the data.

Cornerstone Collective still have a responsibility to lawfully process children's data, and in all circumstances, unless justified in an alternative lawful basis for processing, consent should be sought via Privacy Notice from their parent or legal guardian.

For any online content/service provided by children only children over the age of 13 or over are able to provide their own consent (proposed by the Data Protection Bill). For any children under this age consent must be sought from their parent or legal guardian.

Any Privacy Notices relating to the data of a child must be clear and understandable to both the child and their legal guardian.

It should be noted that children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and to have their personal data erased.

3. Accuracy and Retention

Any personal data held must be kept relevant and accurate as much as practically possible and should not be kept (retained) for longer than necessary in-line with the reason why it was originally gathered for. Data, that has out lived its need, should be disposed of unless required for a legal/regulatory requirement.

4. Security of Data

Appropriate measures should be undertaken to protect data held both electronically and physically. Even though Cornerstone Collective does not operate using a classification of documentation system, it should be considered that any sensitive information relating to a person or persons should be restricted and be on a 'need to know' basis.

Only approved Cornerstone Collective Church e-mail systems should be used. However, where possible personal/sensitive information should not be transported using e-mail, but if it is necessary to do so, if available, a secure e-mail system should be used.

Any personal/sensitive data should be stored within Cornerstone Collective buildings in a locked filing cabinet, with only those who are deemed to be in the 'need to know' category able to access it. The Operations Pastor is responsible for ensuring that this is adhered to.

5. Data Breaches

According to the ICO a personal data breach means 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data'.[1]

In the event that there is a breach of data, the breach should be contained and rectified as soon as possible. Any person(s) affected by the breach should be informed at the earliest opportunity in writing by the Operations Pastor (or assigned deputy).

It is the responsibility of all employees and volunteers of Cornerstone Collective to report any suspected breaches to the Operations Pastor. The Operations Pastor will then decide on which next steps should be taken.

[1] www.ico.org.uk

When a personal data breach has occurred, the likelihood and severity of the resulting risk to people's rights and freedoms must be established. If this is significant then the ICO must be notified within 72 hours of Cornerstone Collective finding out about the breach (please see www.ico.org.uk for details on how to report an incident).

If it was deemed that the incident is not reportable then it is required that the reason for not reporting the incident to be documented.

Details of any breach, whatever the severity, should be recorded by the Operations Pastor.

6. Sharing of Data

Data should only be shared with those outside Cornerstone Collective (or in the 'need to know' category) if it is deemed essential to the operations of Cornerstone Collective or if it is a legal requirement.

On all occasions consent is needed from the data subject (or legal guardian for under 18's).

Data shared should be done in a secure manner and, prior to the data being shared, the intended use by the third part should be documented.

If a particular disclosure is required to meet a legal obligation (for example to a government agency or police force/security service) or in connection with legal proceedings, the personal data may be provided so long as the disclosure is limited to that which is legally required.

Any data sharing requests must be approved by the Operations Pastor.

7. Non-Conformance

If Cornerstone Collective were found to be in breach of data protection laws, the Collective Churches could face fines and enforcement notices, and this would also, potentially, have a negative impact on the gospel work being undertaken across Cornerstone Collective. If an enforcement action was taken against Cornerstone Collective there would be a time and cost implication and additionally the associated publicity would, potentially, have a negative impact on public perception of the gospel, as Cornerstone Collective Churches may be perceived as persons who do not respect the privacy rights of individuals.

8. Definitions

Term Used:	**Definition**
Data Controller	This is a person or company who, either alone or jointly with others, determines the purpose for which, and the manner in which, personal data is processed.
Data Processor	The entity that processes data on behalf of the Data Controller
GDPR	United Kingdom General Data Protection Regulation (2018)
ICO	Information Commissioners Office

Sensitive Personal Data	Certain types of personal data are considered to be 'sensitive' or be 'special categories' of personal data. Additional care needs to be taken when handling such data. Particular care should be taken when collecting and using this type of data (often an individual's explicit consent, or a legal obligation, to do so will be sought). Sensitive personal data means any information relating to: • medical and biometric information • racial or ethnic origin • criminal convictions • political opinions • religious beliefs or political or philosophical opinion • trade union membership • sex life or sexual orientation • genetic data While financial data (such as bank account or credit card details or salary information) are not included in the above-mentioned list of sensitive personal data, this information should be treated as sensitive by their very nature.