Revised 1 June 2018

My Church
Youth and leader engagement platform for churches

Data Protection Policy

This policy is a GDPR-compliant data protection policy that is designed to protect the rights and freedoms of data subjects. It is intended for the general public, our data subjects and our staff members (or volunteers).

Prepared by: **Edan Brooke**

Document version: **2**
Last revision date: **Friday 1 June 2018**

Revised 1 June 2018

1. INTRODUCTION

1.1	**Notice**
	Edan Joseph Brooke (T/A My Church) is committed to protecting the rights and freedoms of data subjects and safely and securely processing their personal data in accordance with all of our legal obligations. My Church is a digital information system designed for use by church organisations, their leaders and the children that regularly attend any of these churches. We are committed to the security and integrity of all information inputted into the system and this policy outlines how we follow data protection legislation including the General Data Protection Regulation. We hold personal data about users of the My Church service and occasionally other individuals for a range of purposes that are critical to the proper operation of the My Church platform and the provision of our service.
1.2	**General Data Protection Regulation ("GDPR")**
	The General Data Protection Regulation 2016 supersedes the Data Protection Directive of 1995 and serves to protect the individual rights and freedoms of natural persons by ensuring that the collection and processing of personal data is controlled and not done without direct consent from the data subject. This policy is intended to cover this new amendment in full, describing how My Church meets its legal obligations and processes all personal data in a safe, secure and ethical manner.

Revised 1 June 2018

2. DEFINITIONS

Proper operation	“Proper operation" is the ability of the My Church information system being able to perform its intended role, which is to process data inputted by users to an extent necessary to provide a meaningful output that can be applied to that organisation or individual's organisational workflow. It also refers to the Management's ability to perform personnel, administrative, financial, regulatory and general business development tasks.
Management	“Management" is any individual or organisation that is responsible for the development, promotion, testing, hosting or otherwise general administration of My Church.
Web 2.0	“Web 2.0" refers to the data and information that is displayed being a direct result of input by a user or data subject.
Raw data	“Raw data" is what is stored in the My Church databases.
Personal data	“Personal data" means any information relating to an identified or identifiable natural person (“data subject"); an identifiable natural person is one 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This personal data may include: individuals' full name, date of birth, phone number, e-mail address, physical address of residence, job title, and place of worship.
Data controller	“Data controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.
Data processor	“Data processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Processing	“Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as 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 or otherwise authorised use thereof.

Supervisory authority	This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioners Office ("ICO").

3. SCOPE

3.1	**Internal scope**
	This data protection policy is enforced upon all Management and staff, who are all required to be aware of the policy and comply with it in full. We may supplement or amend this policy by additional policies and guidelines from time to time to ensure compliance and transparency and to demonstrate our commitment to our users and data subjects. Any new or modified policy will be circulated to staff and relevant personnel before being implemented.
3.2	**Responsibility**
	Edan Brooke has overall responsibility for the day-to-day implementation of this policy and is our data protection compliance manager. You should contact this person for further information about this policy if necessary. Contact details are as follows.

3.2.1	**Postal address**
	You can contact the data protection compliance manager via the postal service by addressing your letter to the following location. It will be delivered securely in a digital format. Armadillo MUMB #10232 8 Parkway Avenue Sheffield West Yorkshire S9 4WA GB
3.2.2	**Telephone number**
	The data protection compliance manager can be contacted by phone at the following contact number. Local (United Kingdom): 0161 738 1165 International: 44161 738 1165
3.2.3	**E-mail address**
	Any e-mails sent to the following e-mail address will be treated as a data protection enquiry. The e-mail address at present is as follows. data@my-church.org

4. PRINCIPLES

4.1	**Compliance declaration**
	My Church shall comply with the principles of data protection ("the Principles") enumerated in the EU General Data Protection Regulation. We will make every effort possible in everything we do to comply with these principles.
4.2	**The Principles**
	There are eight principles of the Data Protection Act 1998 which this policy is designed to cover. These are:

4.2.1	**Lawfulness, fairness and transparency**
	Data collection must be done fairly, legally and transparently. Personal data shall be processed fairly, lawfully and securely. This means My Church must be clear in what data is being collected from a data subject and how it is going to be processed.
4.2.2	**Limitation of purpose**
	We will only collect information from you for specified and lawful purposes that will be described to you in this policy. We must obtain permission to store or process the personal data of a data subject and ask permission again if the purpose of processing or storage changes significantly.
4.2.3	**Relevance**
	All Personal data collected must not be excessive for Proper operation of the system. It is our responsibility to ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained, which should have been made clear to the data subject. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.
4.2.4	**Accuracy**
	The data we hold must be accurate and kept up to date. Any data collected will be stored in a fair context, meaning it will be collected in adequate detail as to not give a false impression in any representation, and that only information that is relevant to the system and/or administration of the system will be collected. Any collection of data shall not extend beyond the required level of detail. If you would like to read more about when information is collected, how it's processed, how it's kept secure, and who has access to this information, please refer to the section of this document entitled "The My Church information system". Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the

		fact that the accuracy of the information is disputed and inform the data protection compliance manager.
	4.2.5	**Retention**
		We are not allowed to store any data for longer than necessary. We must have sufficient and lawful reason for storing any Personal data, and storage of this data must have been authorised by the data subject beforehand. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a fair manner.
	4.2.6	**Confidentiality and integrity**
		We are responsible for keeping any data we collect or store both safe and secure. For further information on how we keep personal information confidential and ensure data integrity, refer to the section of this document entitled “The My Church information system”.
	4.2.7	**Processing in accordance with data protection legislation**
		Personal data must be processed in accordance with the rights of the data subjects, under the Data Protection Act 1998 and the General Data Protection Regulation 2016.
	4.2.8	**Transfer of data outside of the European Union**
		We are not permitted to share data with any persons or organisations outside of the European Union unless the person or organisation is operating in a region with a level of data protection legislation that is deemed acceptable under the Data Protection Act and General Data Protection Regulation legislation and honours the rights of data subjects. All transfers of personal data outside of the European Union must first be agreed with the data protection compliance manager.
4.3	**Measures to ensure compliance**	
	The system is operating and developed in such a way that it is security first. We strive to ensure data protection and the security of our systems and users. We are obliged to keep any personal data we are entrusted with safe and secure against loss or misuse. Where other organisations process personal data as a service on our behalf, data protection compliance manager will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations. We refuse to allow any organisation to process personal data our data subjects provide to us for processing if we have concerns about that organisation's commitment to data protection. Procedures for storing data securely are as follows:	
	4.3.1	**Printed and written documents**

	Should we ever store any personal data on printed paper or on a physical document, it will be kept in a secure place where unauthorised personnel cannot access it. Printed data shall be shredded or otherwise destroyed when it is no longer needed.
4.3.2	**Data stored on an individual employee's computer**
	All computers storing personal data must have adequate security measures in place to prevent unauthorised access to or processing of data. This includes protecting the computer with a strong password that is changed regularly and where password history requirements are enforced. Computer storage mediums must be fully encrypted with the best available and implementable encryption method for that computer.
4.3.3	**Data stored on any portable non-volatile storage medium, such as USB drives**
	All sensitive data stored on removable or portable storage mediums such as USB drives and CDs must be encrypted or password protected and physically locked away in a secure location when they are not being used. When transporting storage devices containing personal data, Management is responsible for ensuring that they are transporting the device in a sensible and secure manner that would not present a risk to data protection or integrity.
4.3.4	**The use of cloud storage services**
	Sometimes the My Church management team may use a cloud storage service to store some data. Any cloud services must be verified and approved by the data protection compliance manager before staff are able to store personal data on them. For a cloud storage service to be approved, it must be fully manageable by our data protection compliance manager and ideally encrypted or with good access control settings.
4.3.5	**Servers**
	Any Server containing personal data must be kept in a secure location with adequate physical access restrictions. My Church is committed to data security so we go above and beyond to ensure data security and compliance with DPA and GDPR. We do so by requiring all servers to log access attempts as well as require 2-factor authentication when a Management user attempts to authenticate. A Server is only accessible by our staff if they prove their identity with a username, password, private key file and 2nd-factor authentication device.
4.3.6	**Backups**
	Data must be backed up regularly and securely, in line with the project's backup procedures. There is an internal policy for backups that is not published.
4.3.7	**Storing data on mobile devices**
	Data should not be saved directly to mobile devices where this can be

		avoided. If data must be saved to a mobile device, this mobile device must not be "jailbreaked" or "rooted", must run security software that is up-to-date, and must have an encrypted filesystem.
	4.3.8	**General technical measures to ensure the security and integrity of data**
		Sufficient practical measures to ensure security and integrity of data must be enforced. For instance, two-factor authentication for system administration interfaces.
4.4	**Accountability and transparency**	
	We are accountable for our collection and processing of personal data and we have a responsibility to be transparent in this collection, processing and retention. This accountability and transparency is something we take very seriously as a project that is clearly built on and operating in line with a Christian ethos. Therefore, being ethical and transparent and responsible for our actions is of utmost importance to us. As part of this demonstration of transparency, we must indicate how we comply with each of the Principles. Staff and Management are responsible for keeping a record of how all the data processing activities they are responsible for comply with each of the Principles. This must be kept up to date and approved by the data protection compliance manager and should be published in this policy, or in a supplementing policy.	

5. PROCEDURES

5.1	**Fair and lawful processing**
	We must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening. If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased. However, we do everything possible in the form of policies and procedures to ensure unlawful processing never happens. Should you believe your data has / is being processed unlawfully, insecurely or unfairly, we urge you to contact the data protection compliance manager so we can correct this as quickly as possible.
5.2	**Controlling data and processing data**
	My Church is classified as a data controller and data processor. We must maintain our appropriate registration with the Information Commissioners Office ("ICO") in order to continue lawfully controlling and processing data. We do so under the name "Mr Edan Joseph Brooke" (T/A "My Church", "LandHost" and "Exfusion"), registered at postcode "S9 4WA".

As a data processor, we have the following obligations:

- Fully co-operate with the Information Commissioners Office or other supervisory authority.
- Ensure that personal data is processed securely.
- Keep accurate records of processing activities.
- Handle any personal data breaches according to organisational policy and according to all legislation.

If you have any queries relating to how we process or handle data please contact the data protection compliance manager, who will be able to provide further information and add it to this policy if necessary.

5.3 Lawful basis for processing data

If you are representative, supervisor or leader at a church organisation, you must ensure that any data you, as a data subject and / or user of the My Church system, are inputting into the system is legal and that you have the right to share it with us as outlined by your own organisation's data protection policy and procedures. Any data you enter must have a written lawful basis approved by the person responsible for data protection at your organisation. It is your responsibility to check the lawful basis for any data you are working with and ensure all of your actions comply with relevant legislation.

Likewise, My Church is also bound by legislation when processing data and we must establish a lawful basis for processing data. We are committed to transparency, honesty and fairness in this and aim to make it as clear as possible for you to understand how we are processing your data.

We have a lawful basis for processing data if any one of the following conditions is true:

5.3.1	**By means of consent**
	This means we hold clear and explicit consent to process a data subject's personal data for a specified and agreed purpose. As a user of the My Church system, this means you have registered an account with us and have agreed to our privacy policy during the process. This is our basis for processing personal data for the majority of persons.
5.3.2	**To prepare a contract**
	If the processing of data is necessary to fulfil or prepare a contract for an individual, we have a lawful basis for processing the personal data of that individual.
5.3.3	**If we are legally obliged to process the data**
	If My Church is legally obliged to process an individual's personal data, we are processing the data on a lawful basis. This may include but is not limited to sharing data with law enforcement agencies as may be required

		under The Data Retention and Investigatory Powers Act 2014 in a rare circumstance.
	5.3.4	**If the data subject's life is endangered and processing is necessary in an extreme circumstance**
		Should the processing of personal data be required to save any person's life, we are processing it on a legal basis. This is referred to as processing data in vital interest.
	5.3.5	**Public function**
		This allows any processing necessary to carry out a public function, a task of public interest or a function that has a clear basis in law.
	5.3.6	**Legitimate interest**
		If the processing of a data subject's personal data is absolutely necessary for our legitimate interests, we can lawfully process it unless there is a good reason to protect the individual's personal data which ultimately overrides the legitimate interest.
5.4	**Deciding which condition to rely on to enable the lawful processing of data**	
	Before My Church processes any data, either by manual administrative means or automated operational means, we will establish that the processing is being done lawfully. To do so, we consider what data we are processing, whether we need to process it, why we need to process it and what we must do to be allowed to process it. We try to avoid processing data for the benefit of anyone other than a customer or user of the My Church platform and we strive to consider the impact that the processing of personal data might have on the data subject. As an example, this means we don't process personal information for marketing purposes unless a data subject explicitly consents to this form of communication. We're also aware that a lot of the personal we process relates directly to children (individuals under the age of consent, which is defined as 13 here in the United Kingdom). Therefore, we seek proper consent from a child's guardian or parent if become aware they are under the age of 13. If we are in any doubt about the age a data subject who registers their personal data on the system and believe they are under the age of 13, we may contact them via telephone or e-mail to confirm they are old enough to give us full consent to process their personal data. Otherwise, if an individual declares they are under the age of 13 when registering for an account (or otherwise accepting an invite to share their details on the system), we ask them to confirm they have parental consent and understand what we process their data for. Where possible, Management will follow up these registrations where deemed necessary by reaching out to the child's guardian to ensure they have consent to register. My Church reserves the right to suspend or delete any user account if we become	

	aware that we may not have a lawful basis to retain the user's personal data. For instance, if we believe a user has attempted to give their own consent to processing but is under the age of 13, we may put the account on hold whilst we carry out enquiries to ensure compliance. If we find that we do not have a lawful basis to retain the data, it will be purged from the My Church system and the data subject will be unable to access our service until they register again with correct consent being given. We always aim to process data by a means that is most transparent to a data subject, relying on consensual or contractual consent in the majority of data processing situations because these are the methods of processing data lawfully that best involve the data subject. If we believe a data subject would be unlikely to agree with the processing of their personal data for a given purpose, we will not process it unless absolutely necessary as we respect the rights of data subjects who entrust us with their personal data. There are measures in place on the My Church system where any implied or otherwise explicitly granted consent or contract can be revoked with immediate effect and your information will no longer be stored on the My Church database or processed by us. However, this has a negative effect on other users as it damages historical records. As an example, if you are a leader and you led a session a year ago but later decide you want us to delete all your data from our system, the session you led would no longer display as having been led by you as we would no longer be storing your personal data. In situations such as this, we would recommend simply closing your account which can be done easily from the account management page. If you still wish for us to stop processing your data and / or delete your personal data from our system, please contact the data protection compliance manager. Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions. We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This is done via our privacy policy. This applies whether we have collected the data directly from the individual or from another source. The “My Church” privacy policy is written, updated and enforced by the data protection compliance manager.

6. SPECIAL CATEGORIES OF PERSONAL DATA

6.1	Special categories of personal data
	Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's: • race • ethnic origin • politics • religion • trade union membership • genetics • biometrics (where used for ID purposes) • health • sexual orientation In most cases where we process special categories of personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed. The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

7. RESPONSIBILITIES

7.1	Notice
	It is important that we, the data controller and data processor, are aware of our responsibilities and make them clear to our data subjects. It is equally as important that you are aware of your responsibilities and rights.
7.2	Our responsibilities
	• Analysing and documenting the type of personal data we hold. • Checking procedures to ensure they cover all the rights of the individual. • Identify the lawful basis for processing data. • Ensuring consent procedures are lawful. • Implementing and reviewing procedures to detect, report and investigate personal data breaches. • Store data in safe and secure ways. • Assess the risk that could be posed to individual rights and freedoms should

	data be compromised.
7.3	**Responsibilities of the data protection compliance manager**
	• Reviewing all data protection procedures and policies on a regular basis. • Arranging data protection training and advice for all staff members and those included in this policy. • Answering questions on data protection from staff, board members and other stakeholders. • Keeping the Information Commissioner's Office registration active and updating them on any changes to what data we collect / process, why we collect / process it, and how. • Responding to individuals such as clients and employees who wish to know which data is being held on them by us. • Addressing data protection queries from clients, target audiences or media outlets. • Checking and approving with third parties that handle data belonging to our data subjects any contracts or agreement regarding data processing.
7.4	**Responsibilities of the IT Manager**
	• Ensure all systems, services, software and equipment meet acceptable security standards. • Checking and scanning security hardware and software regularly to ensure it is functioning properly. • Researching third-party services, such as cloud services the company is considering using to store or process data, to ensure data protection is adequate etc.
7.5	**Responsibilities of the Marketing Manager**
	• Approving data protection statements attached to emails and other marketing copy. • Ensuring all marketing initiatives adhere to data protection laws and our Data Protection Policy.
7.6	**Your responsibilities as a data subject**
	• Please raise any concerns, notify us of any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay. • Disclose any breaches responsibly, directly to us, so we can address them with minimal complication. • your best to ensure data you provide is accurate and that you have permission to provide it as per any legislation or policies you may be bound by. • Do not use data in any unlawful way. • Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions. • Understand your data protection rights and what our obligations are, as well as what our obligations are not.

	• Be aware of this policy and our other policies and how they affect you as a data subject.

8. RIGHTS OF INDIVIDUALS

8.1	**Notice**
	Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways.
8.2	**Right to be informed**
	You have the right to be informed in relation to our storage, collection or processing of your personal data. We agree to: • Provide privacy notices / policies which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children. • Keep a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.
8.3	**Right of access**
	You generally have a right to access the information we store about you, unless revealing this information to you would be harmful. For instance, we are not obliged to notify you of data we hold about you if it would be detrimental to a criminal investigation or if we are unable to verify your identity. Otherwise, we agree to: • Enable individuals to access their personal data and supplementary information. • Allow individuals to be aware of and verify the lawfulness of the processing activities. Subject access requests are honoured free of charge unless the request is complex or frivolous. In this case, we may need to charge an administration fee.
8.4	**Right to rectification**
	We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete. This must be done without delay, and no later than one month. This can be extended to two months with permission from the data protection compliance manager.
8.5	**Right to erasure**
	We agree to delete or remove an individual's data if requested and there is no compelling reason for its continued processing, unless there is a good lawful reason that the data should not be erased.
8.6	**Right to restrict processing**
	We must comply with any request to restrict, block, or otherwise suppress the

	processing of personal data. We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.
8.7	**Right to data portability**
	We must provide individuals with their data so that they can reuse it for their own purposes or across different services. We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested. If the request for data portability is complex, or we receive numerous requests, the turnaround for this may be up to two months but we agree to provide the data as quickly as reasonably possible. This information will be provided free of charge. Data may not be eligible for portability if it would infringe another data subject's right to confidentiality or information security.
8.8	**Right to object**
	We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task. We must respect the right of an individual to object to direct marketing, including profiling. We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.
8.9	**Rights in relation to automated decision making and profiling**
	We must respect the rights of individuals in relation to automated decision making and profiling. Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

9. PRIVACY NOTICES

9.1	**When to supply a privacy notice**
	The My Church system is largely automated, with most data being collected by electronic means. As such, by continuing the use of the My Church system and by having registered for an account, you are expressing an agreement to our privacy policy, terms and conditions and other policies. Any information you enter into the system is therefore covered by your digital agreement to our privacy policy. In a situation where data may be obtained from a data subject indirectly, we have an obligation to supply a privacy notice within a reasonable period of having obtained the data, which is deemed to be within one month. Exceptions to this are if the personal data has been collected in order to communicate with the individual, which will require the privacy notice to be supplied when the first communication takes place, and if disclosure to another recipient is envisaged, which would require the privacy notice be supplied prior to disclosure of this data.
9.2	**What to include in a privacy notice**
	Privacy notices must be concise, transparent, intelligible and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children. At My Church, we believe in transparency and will

	try to make everything as easy to understand as possible. The following information must be included in a privacy notice to all data subjects. **If you don't believe our privacy policy is in line with these guidelines, please contact the data protection compliance manager as soon as possible so we can make the necessary modifications.** • Identification and contact information of the data controller and the data protection officer or person responsible for data protection where no DPO is appointed (also included in this document by our own discretion). • The purpose of processing the data and the lawful basis for doing so. • The legitimate interests of the controller or third party, if applicable. • The right to withdraw consent at any time. • The category of the personal data (only for data not obtained directly from the data subject). • Any recipient or categories of recipients of the personal data. • Detailed information of any transfers to third countries and safeguards in place. • The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period. • The right to lodge a complaint with the ICO, and internal complaint procedures. • The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject). • Any existence of automated decision making, including profiling and information about how those decisions are made, their significance and consequences to the data subject. • Whether the provision of personal data is part of a statutory of contractual requirement or obligation and possible consequences for any failure to provide the data, where this data has been obtained directly from the data subject.

10. SUBJECT ACCESS REQUESTS

10.1	**What is a subject access request?**
	You as an individual have the right to receive confirmation that your data is being processed. You are also entitled to access to your personal data and supplementary information.
10.2	**Internal procedures for dealing with subject access requests**
	We must provide an individual with a copy of the information they request, provided it relates to them and only them. This must occur without delay, and within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats. Of course, this delivery is to be done as securely as possible and in compliance with the Data Protection Act and General Data Protection Regulation. If complying with a subject access request is complex, the deadline can be extended by two months, but the data subject must be informed within one month.

	Any Management member dealing with the subject access request must obtain express permission from the data protection compliance manager before extending the deadline. We can refuse to respond to certain requests that can reasonably be categorised as unreasonable or illegal, or if divulging the information would compromise a Police investigation or other legal proceedings. Subject access requests must be honoured free of charge unless one of the conditions in section 8.3 warrants an administration fee to be charged. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. We will also usually require identification from the data subject before we are able to comply with a subject access request. This is in the interest of security and data protection and to reduce the risk of identity theft. Once a subject access request has been made, we must not change or amend any of the data that has been requested. Doing so is a criminal offence and would contradict our core project values. However, as the system is automated, some data may change between a subject access request being made and the response being processed. We cannot account for this as data can be modified by system users - not only My Church Management. Also, in our response, data that doesn't pertain to the individual requesting the data will be censored to protect the identity of other individuals where appropriate. We endeavour to respond to subject access requests as soon as reasonably possible, once payment of any applicable administration fee along with any required information has been received.
10.3	**Internal procedures for dealing with data portability requests**
	We must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This must be done free of charge and without delay, and no later than one month. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month and the member of staff that is assigned to dealing with the data portability request must receive express permission from the data protection compliance manager before the deadline can be extended.

11. RIGHT TO ERASURE

11.1	**What is the right to erasure?**
	Individuals have a right to have their data erased and for processing to cease in the following circumstances:

	• Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed. • Where consent is withdrawn. • Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing. • The personal data was unlawfully processed or otherwise breached data protection laws. • To comply with a legal obligation. • The processing relates to a child.
11.2	**Internal procedures for dealing with right to erasure**
	We can only refuse to comply with a right to erasure in the following circumstances: • To exercise the right of freedom of expression and information. • To comply with a legal obligation for the performance of a public interest task or exercise of official authority. • For public health purposes in the public interest. • For archiving purposes in the public interest, scientific research, historical research or statistical purposes. • The exercise or defence of legal claims. If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.
11.3	**The right to object**
	Individuals have the right to object to their data being used on grounds relating to their particular situation. We must cease processing unless: • We have legitimate grounds for processing which override the interests, rights and freedoms of the individual. • The processing relates to the establishment, exercise or defence of legal claims. We must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice that a data subject agrees to during registration. We must offer a way for individuals to object online, which can be done via the contact form or by permanently deleting your account.
11.4	**The right to restrict automated profiling or decision making**
	We may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances: • It is necessary for the entry into or performance of a contract. • Based on the individual's explicit consent. • Otherwise authorised by law. In these circumstances, we must: • Give individuals detailed information about the automated processing.

	• Offer simple ways for them to request human intervention or challenge any decision about them. • Carry out regular checks and user testing to ensure our systems are working as intended.

12. THIRD PARTIES

12.1	Use of third party controllers and processors
	As a data controller and data processor, we must have written contracts in place with any third party data controllers or data processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities. As a data controller, we must only appoint processors who can provide sufficient guarantees under DPA and GDPR and that the rights of data subjects will be respected and protected.
12.2	**Contracts**
	Our contracts must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. Our contracts with data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller. At a minimum, our contracts must include terms that specify: • Acting only on written or otherwise sufficiently digitally approved instructions. • Those involved in processing the data are subject to a duty of confidence. • Appropriate measures will be taken to ensure the security of the processing. • Sub-processors will only be engaged with the prior consent of the controller and under a written contract. • The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR. • The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments. • Delete or return all personal data at the end of the contract. • Submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations. • Nothing will be done by either the controller or processor to infringe on GDPR or any other data protection legislation.

13. CRIMINAL OFFENCE DATA

13.1	Criminal record checks
	Any criminal record checks must be justified by law and cannot be undertaken based solely on the consent of the subject. We cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such. Staff members must have approval from the data protection compliance manager prior to carrying out a criminal record check, and have good reason for doing so. We may obtain DBS certificates for volunteers or staff who have access to sensitive information about children or vulnerable user groups. These certificates are to be renewed at least every 3 years. Applicants who are registered for the DBS Update Service will not require a fresh DBS certificate if their current certificate is of the correct level and type unless new information is available and the DBS Update Service recommends a new DBS certificate be obtained.

14. AUDITS, MONITORING AND TRAINING

14.1	Data audits
	Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. The data protection compliance manager may define regular data audits which must be carried out.
14.2	**Monitoring**
	Everyone must observe this policy. The data protection compliance manager has overall responsibility for this policy. This person's details in §3.2. My Church will keep this policy under review and amend or change it as required. Staff should notify the data protection compliance manager of any breaches of this policy. Staff must comply with this policy fully and at all times. Individuals and data subjects should also notify the data protection compliance manager of suspected or confirmed breaches of policy.
14.3	**Training**
	All My Church staff receive adequate training on provisions of data protection law specific for their role. Completion of this training is compulsory. If a member of staff moves role or responsibilities, they are responsible for requesting new data protection training relevant to their new role or responsibilities. If a member of staff feels that they require additional training on data protection matters, they should contact the data protection compliance manager.

15. REPORTING BREACHES

15.1	**Notice**
	Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as we have become aware of a breach. My Church has a legal obligation to report any data breaches to Information Commissioner's Office within 72 hours.
15.2	**Responsibilities of staff members to report breaches, and failure to comply**
	All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to: • Investigate the failure and take remedial steps if necessary. • Maintain a register of compliance failures. • Notify the Information Commissioner's Office of any compliance failures that are material either in their own right or as part of a pattern of failures. Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action. This is done for the protection of our data subjects and to achieve compliance. Any data protection breaches, known or suspected, must be reported directly to the data protection compliance manager within 24 hours. This should be done via phone or face to face to ensure the data protection compliance manager is aware of the breach. We take compliance with this policy very seriously. Failure to comply puts staff members, data subjects and the organisation as a whole at risk. The importance of this policy means that staff member's failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the data protection compliance manager.