# *[insert name of organisation]*

**Individual Information Rights Policy**

# Policy summary

The *[insert name of organisation]* use personal information to carry out their many functions as required to support the mission and ministry of the Church of England. Legislation requires and sometimes empowers the [insert name of organisation]to provide goods and services to the wider Church.

The *[insert name of organisation]* therefore collect personal data required for or incidental to the discharge of its functions with the clear understanding that access and controls of such personal data belong to the data subject/s who have specific rights provided to them by data protection legislation.

This policy provides guidance on how the *[insert name of organisation]* will empower individuals to exercise their rights and facilitate the fulfilment of these rights in a transparent and effective manner in compliance with the legislation. The *[insert name of organisation]* will endeavour to ensure that in applying this policy, they will do so for the benefit of all with whom they come into contact, including the wider Church and the individual data subjects.

Adherence to this policy is mandatory for all *[insert name of organisation]* employees, contractors, agency workers, consultants and volunteers who use personal data held by the *[insert name of organisation]*.

**Contents**

[Policy summary 1](file:///S%3A%5CPrivateShares%5CRecord%20Centre%5CGDPR%5CPolicies%5CTemplate%20Individual%20Information%20Rights%20Policy.docx#_Toc517446972)

[Introduction 3](#_Toc517446973)

[Purpose 3](#_Toc517446974)

[Scope 3](#_Toc517446975)

[Definitions 4](#_Toc517446976)

[Policy 4](#_Toc517446977)

[Policy Statement 4](#_Toc517446978)

[Time scales and response 5](#_Toc517446979)

[Fees and Charges 6](#_Toc517446980)

[Right of Access (Subject Access Request) 7](#_Toc517446981)

[Right to rectification 8](#_Toc517446982)

[Right to erasure 9](#_Toc517446983)

[Right to restrict processing 10](#_Toc517446984)

[Right to data portability 11](#_Toc517446985)

[Right to object 11](#_Toc517446986)

[Rights relating to automated decision making and profiling 12](#_Toc517446987)

[Responsibilities 12](#_Toc517446988)

[Approval and review 13](#_Toc517446989)

[Revision History 13](#_Toc517446990)

[Related policies and procedures 15](#_Toc517446991)

# Introduction

1. The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 provide individuals with specific rights to control how their data is processed by the *[insert name of organisation]*, with certain exemptions and restrictions:
	1. The right of access
	2. The right to rectification
	3. The right to erasure
	4. The right to restrict processing
	5. The right to data portability
	6. The right to object
	7. The right not to be subject to a decision based solely on automated processing or profiling
2. The *[insert name of organisation]* will comply with applicable legislation, and will empower individuals to exercise their rights, and will facilitate the fulfilment of these rights in a transparent, and supportive manner by advising applicants on how to make a request and assisting them in making the request. The *[insert name of organisation]* will endeavour to ensure that in applying this policy, they will do so for the benefit the individual data subjects, and all with whom they come into contact, including the wider Church.
3. Individuals may also obtain and reuse their personal data for their own purposes by having the data moved, copied or transferred from one IT environment to another in a safe and secure way, without affecting its usability.

# Purpose

1. The purpose of this policy is to set out how the *[insert name of organisation]* will comply with requests by data subjects to exercise their rights as listed above (individual rights requests), including how exemptions will be applied. The policy also establishes the principles and mechanism which will be applied by the *[insert name of organisation]* in fulfilling such requests, and how these will be applied to data that is shared or available within the wider Church, or with 3rd party organisations.

# Scope

This policy applies to the *[insert name of organisation]* as listed, and to any separate legal entities owned and controlled by them.

The *[insert name of organisation]* require all those processing personal data on behalf of the *[insert name of organisation]*, including their suppliers, partners, contractors and agents, to act in accordance with this policy.

# Definitions

|  |  |
| --- | --- |
| **Data Subject** | The individual to whom the data being processed relates. |
| **Personal Data** | Any information that relates to an identifiable living individual. |
| **Data Controller**  | A body or organisation that makes decisions on how personal data is being processed. Each of the *[insert name of organisation]* are separate data controllers. |
| **Data Processor**  | These are parties that process data on behalf of a Data Controller, they do not have the ability to make any decisions about how the data should be processed. They must always be designated through a Contract or a Data Processing Agreement. |

# Policy

# Policy Statement

1. In dealing with the processing of valid request(s) the *[insert name of organisation]* will be guided by the following principles:
* The *[insert name of organisation]* will comply with the request unless exemptions or restrictions apply.
* The *[insert name of organisation]* will always provide an acknowledgement of the receipt of the request.
* The *[insert name of organisation]* will accept requests by phone, email, letter and social media.
* The *[insert name of organisation]* will respond to the request as prescribed by the legislation, shown in the section below: <Timescales and responses>.
* The *[insert name of organisation]* will provide a response in compliance with the duties placed upon it as Data Controller
* The *[insert name of organisation]* will support the individual to make the request clear to enable them to get the best possible response.
* The *[insert name of organisation]* will ensure that partner organisations or 3rd party processors are made aware of such requests and are expected to collaborate with the *[insert name of organisation]* and the data subject in order to fulfil them.
* Failures to follow this policy may be investigated by the *Data Compliance Officer (DCO)* and the ICO, in the event of a complaint to them by the data subject.

# Time scales and response

In responding to request(s) the *[insert name of organisation]* will meet the following timescales:

1. Provide an acknowledgement of the receipt of any request within 5 working days of receipt
2. Provide a response as required by law and set out in the table below:

|  |  |
| --- | --- |
| **Individual Rights Request** | **Timescale** |
| Right of access (Subject Access Request) | One calendar month |
| Right to rectification | One calendar month |
| Right to erasure | One calendar month |
| Right to restrict processing | One calendar month |
| Right to data portability | One calendar month |
| Right to object | One calendar month |
| Right to challenge automated decision making or profiling | Not specified, but without undue delay |

Should there be an issue verifying the identity of the requestor there may be an impact on providing a response within the stated timeframes.

In some circumstances the response time may be extended by a further 2 months if the request is complex or there are numerous requests from the same individual.

The *[insert name of organisation]* will provide a written response to all requests, and this will use the format most appropriate to the data subject.

Where relevant and possible the *[insert name of organisation]* will provide remote direct access to the information or through electronic means, or by providing access to information on-site. Where this is not practical, for either technological or security reasons, the requestor will be provided with a copy of the information held by the *[insert name of organisation]*. This will usually be done electronically, but in some instances, will be provided in hard copy through either direct collection by the requester or through secure email or secure postal delivery.

Where the data subject requests a specific format that is not required by the legislation, the *[insert name of organisation]* will endeavour to comply if no additional costs are associated with such provision e.g. purchase of specialised or proprietary formats.

**Identification**

An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone). If the personal data involves third party data, redaction of the information may be necessary. Advice should be sought from the *DCO* where necessary.

The *[insert name of organisation]* will only comply with a request where they are able to verify that the person making the request has a legitimate right to do so, and whether the information requested falls within the definition of personal data as defined above. The *[insert name of organisation]* may request additional information from the requestor in order to confirm their identity. We will let the individual know as soon as possible that we need more information from them before responding to their request. The period for responding to the request begins when we receive the additional information.

The *[insert name of organisation]* will **not** comply with requests where the identity of the requester cannot be verified.

**Third party requests**

The *[insert name of organisation]* will accept individual rights requests made by appropriate 3rd parties on behalf of a data subject. These may include:

* Parent or legal guardian
* Legal representative
* Someone with legal power of attorney
* A third party with the written and verified permission of the data subject.

# Fees and Charges

All the *[insert name of organisation]* will comply with a request free of charge. However, the *[insert name of organisation]* reserves the right to make a reasonable administrative charge if:

* The *[insert name of organisation]* consider that the request is manifestly unfounded or excessive;
* The request is a repeat of a previous request made, and to which the *[insert name of organisation]* involved has already fully responded; or
* A request is made for a copy of information that the *[insert name of organisation]* has previously provided

The *[insert name of organisation]* will contact the individual within one month of the date of receipt of a valid request, to inform them that a fee will be charged and will not comply with the request until payment has been received.

**Data Processors**

A request made by a data subject may, where relevant, include personal data held by 3rd party data processors who are working under the instruction of one or more of the *[insert name of organisation]*. Such data processors are obliged, insofar as this is possible, to assist the data controller(s) in responding to such requests.

The *[insert name of organisation]* will contact the relevant processor and provide either:

* The details of the request and ask for copies of relevant personal data; and/or
* Instructions on what actions to take in response to a request (e.g. amend inaccurate data)

The relevant *[insert name of organisation]* will provide the requestor with details of a processor who holds their data.

The relevant *[insert name of organisation]* will obtain from the processor confirmation that they have complied with a request or instruction within one month of their receipt of such a request.

**Shared** **data**

Data subjects have rights over their shared data, and these are not limited by data sharing arrangements.

**Refusing a request**

If a request has been refused, the *[insert name of organisation]* will inform the requester, within one month of the receipt of a valid request:

* + The reason for refusal;
	+ The right to request a review by the DCO
	+ That they have the right to make a complaint to the ICO;
	+ That they have the right to apply to a court for a judicial remedy

The *[insert name of organisation]* will also provide this information if they request a reasonable administration fee or need additional information to identify the individual.

**Review and complaints**

In the event of a refusal or a response which the data subject considers is unsatisfactory, the requestor may contact the *[insert name of organisation]* to request clarification or help with amending the request.

Should a response not meet the expectations of the requestor then a request for a review can be made to the DCO*.*

Alternatively, the requestor is entitled to contact the Information Commissioner’s Office (ICO) directly.

All responses issued by the *[insert name of organisation]* will contain the details of how a requestor may request a review or make a complaint.

# Right of Access (Subject Access Request)

An individual has the right to access their personal data. This is commonly referred to as a” Subject Access Request” or “SAR”. The individual is entitled to:

* confirmation that you are processing their personal data;
* a copy of their personal data; and
* other supplementary information which is contained in your privacy notice, but which you should be able to provide on request even if it has been published on a website, or previously given the data subject at the point of data collection:
	+ the purposes of your processing;
	+ the categories of personal data concerned;
	+ the recipients or categories of recipient you disclose the personal data to;
	+ your retention period for storing the personal data or, where this is not possible, your criteria for determining how long you will store it;
	+ the existence of their right to request rectification, erasure or restriction or to object to such processing;
	+ the right to lodge a complaint with the ICO or another supervisory authority;
	+ information about the source of the data, where it was not obtained directly from the individual;
	+ the existence of automated decision-making (including profiling); and
	+ the safeguards you provide if you transfer personal data to a third country or international organisation.

Information may be redacted to protect the rights and freedoms of other individuals’ whose data is included in the information requested.

Children have a right of access to the information held about them, even though in the case of young children under the age of 13, these rights may be exercised by those with parental responsibility for them. Before responding to a Subject Access Request for information held about a child, the *[insert name of organisation]* will consider whether the child is mature enough to understand his/her rights and where appropriate will usually respond directly to the child. However, the *[insert name of organisation]* may allow the parent to exercise the child’s rights on his/her behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

The *[insert name of organisation]* will supply the information we hold when we send out a response, even if this is different to that held when we received the request, on the basis that the data may have been amended or deleted in the normal course of business.

The *[insert name of organisation]* will not amend or delete the data if it would not otherwise have done so.

It is an offence to make any amendment with the intention of preventing its disclosure, and the *[insert name of organisation]* may take action against an employee or other user of its data who intentionally and willfully makes such an amendment.

The *[insert name of organisation]* will keep a copy of the information provided to the data subject for a period of 7 years from the date of response.

Generally, the *[insert name of organisation]* will not provide information under the right of access if:

* + The *[insert name of organisation]* is not the data controller, or does not have authority from the data controller to release the information;
	+ The information is not considered to be personal data;
	+ The data concerns another individual, unless that person has consented to the disclosure or it is reasonable to comply without that person’s consent.

# Right to rectification

An individual has the right to to have inaccurate personal data rectified or completed if it is incomplete.

 The individual is entitled to:

* The rectification of personal data that is inaccurate if it is incorrect or misleading as to any matter of fact;
* Have incomplete personal data completed;
* Be informed in writing if the request has been granted

The *[insert name of organisation]* will ask the data subject to provide evidence of the alleged data inaccuracy and/or incompleteness.

When the data subject challenges the accuracy of their data the *[insert name of organisation]* will check if data held on the individual is accurate or needs to be rectified, taking account of the evidence of inaccuracy or incompleteness provided by the data subject.

The *[insert name of organisation]* will rectify inaccurate or incomplete data belonging to the data subject, or a supplementary statement will be added to the incomplete data, instead of an amendment to the existing data, depending on the purposes for the processing.

Generally, the *[insert name of organisation]* will not rectify data if:

* The *[insert name of organisation]* are content that the data is accurate, in which case the individual will be informed of their right to make a complaint to the ICO.
* The request is either repetitive, excessive or is noticeably unfounded; or
* The personal data must be maintained in its existing form for evidential purposes.

On receipt of a valid request, the *[insert name of organisation]* will restrict the processing of the personal data in question during verification of its accuracy.

Where possible the *[insert name of organisation]* will rectify the data held either electronically or on paper. Where this is not practical for technological or security reasons, or where the *[insert name of organisation]* is satisfied that the data is accurate, the *[insert name of organisation]* will provide the requestor with a supplementary document explaining their decision.

# Right to erasure

An individual has the right to have their personal data erased if:

* The personal data is no longer necessary for the purpose which it was originally collected or processed;
* Consent was the lawful basis for holding the data and the data subject has withdrawn consent;
* The *[insert name of organisation]* are relying on legitimate interest as a basis for processing and the data subject objects to the processing of their data, and there is no overriding legitimate reason to continue this processing;
* Personal data is being unlawfully processed as in the case of direct marketing and the individual objects to such processing;
* It is necessary for compliance with a legal obligation to which the [*insert name of organisation*] is subject;

Where the data processed was collected from children, special attention will be given to any request for erasure if the processing of the data is based upon consent given by a child and especially for processing of their personal data on the internet.

Generally, the *[insert name of organisation]* will not erase personal data held under the right to erasure where processing is necessary for:

* Exercising the right of freedom of expression and information;
* Compliance with a legal obligation;
* The performance of a task;
* Public health purposes in the public interest;
* The purposes of preventative or occupational medicine.

The *[insert name of organisation]* will restrict the processing of the personal data in question during verification of its accuracy.

The *[insert name of organisation]* will make all reasonable efforts to comply with the data subject’s wishes where possible and will erase or otherwise remove the data held either electronically or on paper from the processing activity.

# Right to restrict processing

An individual has the right to request the restriction of processing to their personal data. This is not an absolute right and only applies in certain circumstances, as follows:

* Where the accuracy of the personal data is contested by the individual and the controller is verifying the accuracy of the data;
* Where personal data has been unlawfully processed and the individual requests restriction instead of erasure of their data;
* Where the controller no longer needs the personal data but the data subject requests that the data be kept so as to establish, exercise or defend a legal claim;
* Where the data subject has objected to processing of their personal data under Article 21(1) of the GDPR pending the verification of whether the legitimate grounds of the controller override those of the data subject;

Generally, the *[insert name of organisation]* will restrict the processing of the personal data in question whilst considering its accuracy or its legitimate grounds for processing the data in question.

The *[insert name of organisation]* will not process restricted personal data held under the right to restrict processing except to store it unless:

* The data subject has given consent;
* It is for the establishment, exercise or defence of legal claims;
* It is for the protection of the rights of another individual;
* It pertains to substantial public interest.

Where processing has been restricted, no processing of such personal data will be undertaken, except for storage and legitimate disposal.

Generally, where possible the *[insert name of organisation]* will restrict processing of the data held either electronically or on paper. Where this is not practical for technological or security reasons, or in circumstances where the right to restriction does not apply, the *[insert name of organisation]* will provide the requestor with a written explanation for its decision.

# Right to data portability

An individual has the right to obtain and reuse their personal data for their own purposes across different services, in order to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

An individual is only entitled to data portability where:

* The processing of personal data is based on the individual’s consent **or** on the performance of a contract; and
* the individual has provided personal data to the controller; and
* processing is carried out by automated means (excludes paper files).

It does not include any additional data that any of the *[insert name of organisation]* have created based on the data an individual has provided.

In exercising his or her right to data portability the data subject shall have the right to have personal data transmitted directly from one controller to another where technically feasible.

The *[insert name of organisation]* will:

* Provide portable data in a commonly used format.
* Transmit data directly to another organisation if the individual requests it and if it is technically feasible.

Generally, the *[insert name of organisation]* will not provide information under the right to data portability if:

* The *[insert name of organisation]* is not the Data Controller or does not have the authority from the Data Controller to release the information, or
* The information to be provided infringes upon the rights of another person.

# Right to object

Individuals have the right to object to the processing of their personal data in certain circumstances, where:

* Processing of personal data is based on legitimate interests or the performance of a task in the public interest;
* Processing is for scientific research and statistical purposes.

Individuals have an absolute right to stop their data being used for direct marketing.

On receipt of a valid request the *[insert name of organisation]* will immediately stop processing the data in question.

The *[insert name of organisation]* will endeavour to resolve the reason for the objection, and if the data subject does not agree with the proposed resolution, cease processing their personal data.

The cessation of processing does not require the *[insert name of organisation]* to erase or delete data, unless an erasure request has been made and agreed.

The *[insert name of organisation]* will decline request under the right to object if:

* The *[insert name of organisation]* can establish compelling legitimate grounds for the processing, which supersede the rights, freedom and interest of the data subject;
* Processing carried out for scientific, historical research or statistical purposes unless the processing is necessary for the performance of a task carried out in the public interest
* Processing is for security and legal reasons; or
* The cessation of processing infringes upon the rights of another person.

# Rights relating to automated decision making and profiling

Individuals have the right to object to:

* Decisions made about them solely by automated means without any human involvement;
* Profiling due to automated processing of personal data to evaluate certain attributes about themselves;
* Processing for scientific research and statistical purposes.

Generally, the *[insert name of organisation]* will:

* Implement suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision;
* Will carry out a Data Protection Impact Assessment (DPIA) to identify risk to individuals and show how it is going to deal with them in accordance with the legislation;
* Have a record of the data subject’s explicit consent (where relevant) and be able to show how and when consent was obtained.

The *[insert name of organisation]* will not comply with a request for exemption from processing based solely on automated individual decision-making if the decision is:

* For contractual purposes between the individual and the *[insert name of organisation]*;
* authorising the *[insert name of organisation]* by law to carry out processing under Article 22(1) GDPR;
* Based on the data subject’s explicit consent;
* Necessary for reasons pertaining to significant public interest.

# Responsibilities *[amend this section as required]*

**Trustees (members of the PCC)** are responsible for the approval and implementation of this policy and related policies, for informing the trustees of current legislative requirements that may affect their criminal and civil liability and for ensuring that Directors meet their responsibilities for fulfilling individual rights requests. They are responsible for ensuring that they are aware of the legislative requirements as stated in this policy, for monitoring or progressing response times and responses and for working across the *[insert name of organisation]* to ensure a consistent approach to the receipt and response to individual rights requests.

**Data Compliance Officer** is responsible for ensuring that individual information rights requests are effectively managed and that responses that fall outside the required timescales are reviewed and escalated where necessary and for establishing arrangements for independent reviews where required where complaints are made by data subjects or the ICO regarding individual rights or data processing, reviewing refusals and making final determination on appeals relating to refusals.

**All staff,** contractors, agency workers, consultants and volunteers who have access to personal data held by the *[insert name of organisation]* are responsible for assisting colleagues who are responsible for individual rights requests by providing the necessary information or changes to the information or processing of that information in a timely way; and for ensuring that no deletion or amendment is made to such data to prevent disclosure.

# Approval and review

|  |  |
| --- | --- |
| Approved by |  |
| Policy owner |  |
| Policy author |  |
| Date |  |
| Review date |  |

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version No | Revision Date | Previous revision date | Summary of Changes |
| 1.0 |  |  | New policy |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |