Safeguarding Hubs Service Agreement

A *Safeguarding Hub* is an online system that aims to make safeguarding simpler.

It comprises a suite of tools that help a Parochial Church Council to comply with the Church of England's safeguarding requirements.

For example, a *Safeguarding Hub* can help:

- To keep track of the safeguarding status of church volunteers and employees.
- To create Role Descriptions and Person Specifications.
- To track the safer recruitment of new volunteers.

A Parochial Church Council can use a *Safeguarding Hub* under licence for the duration of this Service Agreement.

Parties to this Service Agreement

This *Service Agreement* is between:

- **Clearly Simpler Limited** – hereafter referred to as 'we', 'us' and 'our'
- **A Parochial Church Council** – hereafter referred to as 'you' and 'your'

Although not party to this *Service Agreement*, we also have a legally binding contract with your **Diocesan Board of Finance** (hereafter called 'your diocese') which is paying the licence fee for your *Safeguarding Hub*.

Definition of Terms

This *Service Agreement* uses the following terms:

- **Church Officer** – Anyone appointed/elected by or on behalf of the Church to a post or role, whether they are ordained or lay, paid or unpaid
- **Hub Owner** – A primary user of a *Safeguarding Hub*, who can also grant access to others
- **UK GDPR** – The United Kingdom's *General Data Protection Regulation*

This *Service Agreement* also uses the terms defined in Article 4 of the UK GDPR. In particular:

- **Personal data** – means any information relating to an identified or identifiable person
- **Processing** – includes the collecting, storing, analysing, displaying, sharing and deleting of data
- **Data controller** – refers to the body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **Data processor** – refers to the body which processes personal data on behalf of the controller

Data protection

Personal data

A *Safeguarding Hub* processes personal data relating to current and past Church Officers (or applicants). This includes:

- Name and email address *– for example, "Fred Smith at fred.smith@gmail.com"*
- Current and past church roles *– for example, "PCC Member from 01/04/19 to 31/03/22"*
- Details of cleared DBS checks *– the certificate number, date, and type of check*
- Details of safeguarding training *– the type of training and date completed*
- Confirmation (or otherwise) that the safer recruitment process has been followed for new appointments *– the steps completed, names of referees, etc.*
- Confirmation (or otherwise) of ongoing support and oversight *– dates of supervision meetings, etc.*

Given that this data reveals that a person belongs to a religious organisation, it must be treated as a 'special category' of personal data, as defined by Article 9 of the UK GDPR. However, it may still be processed under paragraph 2(d) of the article.

Data controller

You are the data controller for the above-mentioned personal data.

The primary purpose of a *Safeguarding Hub* is to help you to comply with the Church of England's safeguarding requirements, as defined by:

- The Church of England's *Safeguarding Code of Practice*; and
- The House of Bishops' safeguarding guidance.

Given that the Church of England's safeguarding requirements have the same force and effect as an Act of Parliament,[1] the lawful basis for processing this data is 'legal obligation'. See paragraph 1(c) of Article 6 of the UK GDPR.

Data processor

We are the main data processor for your *Safeguarding Hub*. We will only process personal data within the UK and in accordance with your documented instructions, including:

- This *Service Agreement* (which incorporates the *Data Processing Addendum* on page 6).
- Your *Safeguarding Hub* settings, which can be changed by your Hub Owner(s) on your behalf.
- Any separate data sharing agreements.

Personal data stored in your *Safeguarding Hub* will be deleted in accordance with the Church of England's policy for the retention of safeguarding records.

Sub-processors

Safeguarding Hubs are hosted on data servers within the UK provided by DigitalOcean LLC.

We currently use no other sub-processors, but we will give you 30 days' notice of any proposed change. If you object to this change, you can terminate this *Service Agreement*.

[1] https://www.parliament.uk/site-information/glossary/church-of-england-measures

Authorised Users

Your *Safeguarding Hub* can be accessed by authorised users on your behalf.

Hub Owner

You must appoint at least one Hub Owner to be the primary user(s) of your *Safeguarding Hub*.

Acting on your behalf, a Hub Owner can:

- Accept this *Service Agreement* with us.
- View and edit all the data in your *Safeguarding Hub*.
- Invite other people to be authorised users, and to change their permissions (see below).
- Change the settings for your *Safeguarding Hub*. These settings determine which features can be used, and how your data might be shared with other people or systems.

You can add or remove a Hub Owner at any time.

Other authorised users

Acting on your behalf, a Hub Owner can invite other people to be authorised users of your *Safeguarding Hub*. Each authorised user has their own set of permissions which determine what they can view and what they can edit.

User registration

No one should access your *Safeguarding Hub* unless they have registered as an authorised user. The registration process requires them:

- To have a unique email address.
- To choose a password.
- To read our Privacy Notice and accept our Terms and Conditions.

Once authorised, they can access your *Safeguarding Hub* via any device that has a web browser (e.g. a mobile phone, tablet or laptop). Accessing the system does not require any data to be stored on their own device.

Removing access

When an authorised user no longer has a legitimate reason for using your *Safeguarding Hub*, it is your responsibility to ensure that their access is removed. This will usually be done by a Hub Owner on your behalf.

An authorised user can also remove their own access at any time.

Technical support

We aim to fix any reported technical problems within 24 hours.

We will make daily backups of your data, which we can use to restore your *Safeguarding Hub* in the event of a system-wide failure. [2]

We will respond to any reasonable requests for technical support from your authorised users. Our employees will only view your *Safeguarding Hub* for this and troubleshooting purposes, and they will:

- Not keep any record of any personal data (including screenshots).
- Not disclose personal data to anyone else.

Data sharing

Sharing non-personal data

A *Safeguarding Hub* stores non-personal data, including:

- Statistics regarding the number of people assigned to various church roles
- Statistics regarding DBS checks and safeguarding training
- Role Descriptions and Person Specifications

By accepting this *Service Agreement*, you authorise non-personal data to be shared with the Diocesan Safeguarding Team in your diocese.

Sharing personal data

A *Safeguarding Hub* stores personal data relating to current and past Church Officers (or applicants).

We will only share personal data with other people or systems in accordance with your documented instructions (see '**Data processor**' on page 2).

Data breaches

If we become aware of any breaches of personal data, we will notify your Hub Owner(s) within 12 hours.

Your responsibilities

Given that authorised users have access to personal data, you must take reasonable steps to ensure that they:

- Have a legitimate reason for using your *Safeguarding Hub*.
- Only use your *Safeguarding Hub* for the purposes for which it is intended.
- Notify us promptly if they become aware of, or reasonably suspect any illegal or unauthorised activity, or a security breach involving your *Safeguarding Hub*.
- Do not disclose their password or other login details to anyone else, nor to share their account with others.

---

[2] We do not guarantee to restore data that has been deleted by your authorised users. However, we will make it difficult for such data to be deleted accidently.

- Do not attempt to reverse engineer, decompile, hack, disable, interfere with, disassemble, modify, copy, translate, or disrupt the features, functionality, security, integrity, or performance of *Safeguarding Hubs*.

You must fulfil your legal obligations as the data controller, so that we can lawfully process data on your behalf. For example, you must have a Privacy Notice that lets people know what information is stored and what you will do with it.

Your failure to comply with these responsibilities may constitute a breach of this *Service Agreement* at our sole discretion.

Termination of this Service Agreement

Termination of this Service Agreement by you

You can terminate this *Service Agreement* at any time.

Your Hub Owner(s) will continue to have access to your *Safeguarding Hub* for a period of 60 days after the termination of this *Service Agreement*. This allows time for you to extract any personal data that we have processed on your behalf.

Other authorised users will lose access immediately.

Termination of this Service Agreement by us

We can terminate this *Service Agreement* immediately if you breach its terms or we cease trading; otherwise, we must give you twelve months' notice.

Your Hub Owner(s) will continue to have access to your *Safeguarding Hub* for a further period of 60 days after the notice period. This allows time for you to extract any personal data that we have processed on your behalf.

Other authorised users will lose access at the end of the notice period.

Termination of our contract with your diocese

In the event of our contract with your diocese being terminated, we will allow you to continue using your *Safeguarding Hub* based on a new contract between you and us. That new contract will require you to pay us an Annual Fee.

Data Processing Addendum

The *Data Processing Addendum* on the following pages is an integral part of this *Service Agreement*.

We will give you 30 days' notice of any proposed change to this Addendum. If you object to this change, you can terminate this *Service Agreement*.

Safeguarding Hubs

July 2025

Data Processing Addendum

This Data Processing Addendum forms part of the Service Agreement between **Clearly Simpler Limited** and a **Parochial Church Council** (PCC).

It comprises instructions from the PCC in accordance with Article 28 of the UK General Data Protection Regulation (UK GDPR).

This Addendum also forms part of the legally binding contract between **Clearly Simpler Limited** and the appropriate **Diocesan Board of Finance**.

1. Processing only on the PCC's instructions

Clearly Simpler Limited will only process personal data in line with the PCC's documented instructions unless they are required to do otherwise by UK law. All data will be processed in the UK.

2. Confidentiality

Clearly Simpler Limited will obtain a commitment of confidentiality from anyone they allow to process personal data. This includes their employees, as well as any temporary workers and agency workers who have access to the personal data.

3. Appropriate security measures

Clearly Simpler Limited will implement the necessary security measures to meet the requirements of Article 32 of the UK GDPR on the security of processing.

They will put in place appropriate technical and organisational measures to ensure the security of any personal data that they process.

4. Using sub-processors

Clearly Simpler Limited will provide the PCC with a list of the sub-processors that they engage, and they will give 30 days' notice of any proposed changes to this list. The PCC can object to this change by terminating their Service Agreement.

Clearly Simpler Limited will ensure that their contract with a sub-processor imposes the same obligations on that sub-processor as found in this Addendum.

A sub-processor must implement appropriate technical and organisational measures in such a way that the processing will meet the requirements of the UK GDPR.

Clearly Simpler Limited is liable for a sub-processor's compliance with its data protection obligations.

5. Data subjects' rights

Clearly Simpler Limited will implement appropriate technical and organisational measures to help the PCC to respond to requests from individuals to exercise their rights.

This provision stems from Chapter III of the UK GDPR, which describes how the controller must enable data subjects to exercise various rights and respond to requests to do so, such as subject access requests, requests for the rectification or erasure of personal data, and objections to processing.

6. Assisting the controller

Clearly Simpler Limited will assist the PCC in meeting their obligations:

- To keep personal data secure.
- To notify personal data breaches to the ICO when required.
- To notify personal data breaches to data subjects when required.

7. End-of-agreement provisions

At the termination of their Service Agreement, and for the next 60 days, Clearly Simpler Limited will make provision for the PCC to download any personal data that has been processed on behalf of the PCC.

Thereafter, Clearly Simpler Limited will delete all personal data in a secure manner, in accordance with the security requirements of Article 32 of the UK GDPR.

Clearly Simpler Limited will delete backup copies of this data in accordance with their usual destruction cycle.

8. Audits and inspections

Upon request, Clearly Simpler Limited will provide the PCC with information that demonstrates that their obligations of Article 28 of the UK GDPR have been met.

Clearly Simpler Limited will allow for, and contribute to, any reasonable request for an audit or inspection carried out by an auditor appointed by the PCC.

If the PCC is not satisfied with the response to such requests, they can terminate their Service Agreement.