Safeguarding Hubs Service Agreement

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

It has 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 a church:

- 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.

For the duration of this *Service Agreement*, a PCC may use their *Safeguarding Hub* under licence. We will make daily backups of your data, and we will provide system support for your users.

Parties to this Service Agreement

This *Service Agreement* is between:

- **Clearly Simpler Limited** – hereafter referred to as 'we', 'us' and 'our'
- **The Parochial Church Council** (PCC) – 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'). Your diocese 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 PCC to a post or role, whether they are ordained or lay, paid or unpaid
- **Hub Owner** – The 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 past and present Church Officers. 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 information 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 this 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 in accordance with your documented instructions, including:

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

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 a data server 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 nominate one Hub Owner to be the primary user of your *Safeguarding Hub*.

Acting on your behalf, your Hub Owner can:

- View and edit all the data in your *Safeguarding Hub*.
- Invite other people to be authorised users, and to change their permissions.
- Change the settings for your *Safeguarding Hub*. These settings determine which features can be used, and how your data might be shared.

You can change your nominated Hub Owner at any time.

Other authorised users

Acting on your behalf, your 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 Hubs* 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 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 your Hub Owner on your behalf.

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

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 your diocese.

Sharing personal data

A *Safeguarding Hub* also stores personal data relating to past and present Church Officers (see page 2).

By accepting this *Service Agreement*, you authorise your diocesan safeguarding team to access your *Safeguarding Hub* for any of the following reasons:

- To provide system support.
- To provide safeguarding advice.
- To audit safeguarding records.

You also authorise our employees to access your *Safeguarding Hub* to provide system support.

You can authorise the sharing of personal data for other purposes via:

- Any separate *Data Sharing Agreement*.
- Your *Safeguarding Hub* settings, which can be changed by your Hub Owner on your behalf.

Your responsibilities

Given that authorised users have access to personal data, you must take reasonable steps to ensure they have a legitimate reason for using your *Safeguarding Hub,* and that they understand the need for confidentiality.

You must take reasonable steps to ensure that your authorised users:

- Keep their password and any other login details confidential.
- 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 permit their account to be used by someone else.
- 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 you have and what you'll do with it.

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

Data Processing Addendum

The *Data Processing Addendum* on page 6 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*.

Termination of this Service Agreement

Termination of this Service Agreement by you

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

Your Hub Owner 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 download any personal data that we have processed on your behalf.

Other authorised users may lose access immediately.

Termination of this Service Agreement by us

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

Your Hub Owner 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 download any personal data that we have processed on your behalf.

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

Termination of our contract with your diocese

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

Safeguarding Hubs

January 2025

Data Processing Addendum

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

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

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

1. Processing only on the PCC's instructions

Clearly Simpler Limited will only process personal data in line with the PCC's documented instructions (including when making an international transfer of personal data) unless they are required to do otherwise by UK law.

2. Confidentiality

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

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

5. Data subjects' rights *

Clearly Simpler will take 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 *

Taking into account the nature of the processing and the information available, Clearly Simpler 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.
- To carry out data protection impact assessments (DPIAs) when required.
- To consult the ICO where a DPIA indicates there is a high risk that cannot be mitigated.

7. End-of-agreement provisions

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

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

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

8. Audits and inspections *

Clearly Simpler will:

- Provide the PCC with all the information that is needed to show that the obligations of Article 28 have been met.
- Allow for, and contribute to, audits and inspections carried out by the PCC, or by an auditor appointed by the PCC.

This provision obliges Clearly Simpler to be able to demonstrate compliance with the whole of Article 28 to the PCC. For instance, they could do this by giving the PCC the necessary information or by submitting to an audit or inspection.

* Clearly Simpler may charge an extra fee for work associated with sections 5, 6 and 8 of this Addendum.