Safeguarding Hubs

Data Processing Agreement

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

It includes a suite of tools that help a parish to comply with the Church of England's safeguarding requirements.

For example, a *Safeguarding Hub* can help a parish:

- 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.

It can also share information with other people or organisations within the Church of England.

Safeguarding Hubs are provided by Clearly Simpler Limited.

Parties to this agreement

'you', 'your'	**The Parochial Church Council (PCC)** You are the data controller, since you determine the purpose and means of processing personal data.
'we', 'us', 'our'	**Clearly Simpler Limited** We are the data processor, since we process personal data on your behalf, and only in accordance with your instructions.

This Data Processing Agreement is between you and us.

Although not party to this Agreement, we also have a legally binding contract with your **Diocesan Board of Finance** (hereafter called your '**diocese**') which refers to this Agreement.

Definition of Terms

Where appropriate, this agreement uses the same definition of terms as used in the UK *General Data Protection Regulation* (GDPR). [1] In summary:

- '**Processing**' includes the collecting, storing, analysing, displaying, sharing and deleting of data.
- '**Personal data**' means any information relating to an identified or identifiable person.

[1] https://www.legislation.gov.uk/eur/2016/679/article/4

About Safeguarding Hubs

Primary purpose

A *Safeguarding Hub* includes a suite of tools that aim to make safeguarding simpler.

These tools 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.

This primary purpose includes the processing of personal data.

Secondary purposes

A *Safeguarding Hub* can share information with other people or organisations within the Church of England for other purposes (see page 6).

These secondary purposes may also involve the sharing of personal data

Personal data

A *Safeguarding Hub* processes personal data relating to past and present Church Officers.

A Church Officer is defined as:

> *"Anyone appointed/elected by or on behalf of the Church to a post or role, whether they are ordained or lay, paid or unpaid."*

Personal data comprises:

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

Personal data is deleted in accordance with the Church of England's policy for the retention of safeguarding records.

Personal data will only be shared with others if there is a lawful basis for doing so.

Our Obligations

This section of the Data Processing Agreement is deemed to be your documented instructions to us in accordance with Article 28 (3) of the UK GDPR. [1]

Processing only on your documented instructions

We will only process personal data in line with your documented instructions (including when making an international transfer of personal data) unless we are required to do otherwise by UK law.

Duty of confidence

We will obtain a commitment of confidentiality from anyone we allow to process personal data. This includes our employees, as well as any temporary workers and agency workers who have access to the personal data.

Appropriate security measures

We will take all security measures necessary to meet the requirements of Article 32 of the UK GDPR on the security of processing. [3]

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

Using sub-processors

We will not engage another processor (a sub-processor) without your prior specific or general written authorisation. If we do employ a sub-processor, we will put a contract in place imposing the same obligations on that sub-processor as found in this section of the Data Processing Agreement.

A sub-processor must also provide sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the UK GDPR's requirements.

We are liable to you for a sub-processor's compliance with its data protection obligations.

Data subjects' rights

We will take appropriate technical and organisational measures to help you respond to requests from individuals to exercise their rights. [4]

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.

---

2 https://www.legislation.gov.uk/eur/2016/679/article/28

3 https://www.legislation.gov.uk/eur/2016/679/article/32

4 We may need to charge an additional fee for this.

Assisting the controller

Taking into account the nature of the processing and the information available, we will assist you in meeting your obligations:

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

End-of-agreement provisions

At the termination of this agreement (see page 7), and for the next 60 days, we will make provision for you to download any personal data that we have processed on your behalf.

Thereafter, we will delete all personal data in a secure manner, in accordance with the security requirements of Article 32 of the UK GDPR. [5]

Backup copies of this data will be deleted in accordance with our usual destruction cycle.

Audits and inspections

We will:

- Provide you 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 you, or by an auditor appointed by you.

This provision obliges us to be able to demonstrate compliance with the whole of Article 28 to you. For instance, we could do this by giving you the necessary information or by submitting to an audit or inspection. [6]

[5] https://www.legislation.gov.uk/eur/2016/679/article/32

[6] We may need to charge an additional fee for this.

Authorised Users

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

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

Types of authorised user

There are three types of authorised user at a parish level:

- **Hub Owner**
  There can be only one Hub Owner at any given time.
  The Hub Owner has full access to all data in the entire *Safeguarding Hub*. They can also act on your behalf:
  - To invite other people to be Hub Administrators and Responsible People.
  - To change your privacy settings relating to data sharing (see page 6).
- **Hub Administrator**
  A Hub Administrator has full access to all data in the entire *Safeguarding Hub*. They must accept an invitation issued by the Hub Owner on your behalf.
- **Responsible Person**
  A Responsible Person has restricted access to the roles and people for whom they are responsible. They must accept an invitation issued by the Hub Owner on your behalf.

You must appoint the Hub Owner and must instruct them regarding your requirements for inviting other authorised users.

User registration

To become an authorised user, someone must first accept a personal invitation (usually sent by the Hub Owner). They must also choose a password, read our Privacy Notice and accept our Terms and Conditions. [7]

Once authorised, they can access their *Safeguarding Hub* via any device that has a web browser (e.g. a mobile phone, tablet or laptop).

Removing access

When an authorised user no longer has a legitimate reason for accessing the *Safeguarding Hub*, it is your responsibility to ensure that their access has been removed.

This will usually be done by the Hub Owner on your behalf.

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

[7] https://www.parishdashboards.org.uk/api/privacy

Data Sharing

A *Safeguarding Hub* can share information with other people or organisations within the Church of England.

Sharing non-personal data

You have no control over the sharing of non-personal data from your *Safeguarding Hub*.

Example A

An authorised diocesan user can see the number (but not the names) of people in your parish who have:

- Outstanding safeguarding training.
- Overdue DBS checks.

This statistical data could help your diocesan safeguarding team to monitor compliance throughout the diocese, and to identify parishes that need more support.

Example B

An authorised diocesan user can see the *Role Descriptions and Person Specifications* that you use in your parish, and the number (but not the names) of people assigned to these roles.

This information could help your diocesan mission team to plan some training events for youth workers.

Sharing personal data

You have full control over the sharing of personal data from your *Safeguarding Hub*.

This control is exercised via data sharing settings that are only available to the Hub Owner on your behalf.

As the data processor, it is your responsibility to ensure that there is a valid lawful basis for the sharing of personal data with others.

Example C

The safeguarding records of your parish are being audited by your diocesan safeguarding team.

For the duration of this audit, you might grant the auditors access to all personal data that is stored in your *Safeguarding Hub*.

Other Terms and Conditions

Our services

For the duration of this agreement, we will provide you with:

- A license to use a *Safeguarding Hub* for the primary purpose stated on page 2.
- Automatic daily backups of your data.
- Technical support.

We will process all personal data in accordance with our obligations stated on pages 3 and 4.

Termination of this agreement by you

You can terminate this agreement at any time, and without the need to give any reason.

Your Hub Owner will continue to have access to your *Safeguarding Hub* for a period of 60 days. This allows time for you to download any personal data that we have processed on your behalf (see page 4).

Other authorised users will have their access ended immediately.

Termination of this agreement by us

We can terminate this agreement with twelve months' notice, but only for a good reason. No notice is required if you breach this agreement.

Your Hub Owner will continue to have access to your *Safeguarding Hub* for a further period of 60 days. This allows time for you to download any personal data that we have processed on your behalf (see page 4).

Other authorised users will have their access ended at the end of the notice period.

Termination of our contract with your diocese

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

Acceptable use of your Safeguarding Hub

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 stated on page 2.
- 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*.

Your failure to take reasonable steps may constitute a breach of this agreement at our sole discretion.