

Data Protection and Security Practice Notes: Safeguarding Team

Case Work and Core Groups

This version dated: 16th June 2022

Approved by: *Poli Shajko*

Purpose of this Document

This document provides a basis for Oxford Diocesan Board of Finance (ODBF) to demonstrate its compliance to the General Data Protection Regulation (EU) 2016/679, in the area described above. It is for use by ODBF staff and for data protection auditing purposes, to assess the day to day handling of personal data.

1 Area of work

- *Case work & core group reports*

2 Personal data being processed

Sensitive personal information including the following:

- *Names, address, email, DOB, employment history*
- *Case work records including witness statements*
- *Action/alleged action*
- *Contact details for other agencies*
- *History of offending behaviour*
- *Specialist assessments on individuals*

2.1 Source of the data

- *Telephone*
- *Email*
- *Individual contact*
- *3rd party including statutory agencies*
- *Police*
- *Bishops eg Blue Files*

3 Data processing activity

3.1 Purpose/scope of the processing

To meet the Diocesan responsibilities in respect of investigating safeguarding concerns.

3.2 Lawful basis for processing

- *Consent – consent is obtained to process data for assessing and providing counselling and support, and to share it with 3rd parties.*
- *Legitimate interest – information may be processed to undertake safeguarding tasks, including doing all that we reasonably can to ensure that no-one is at risk of harm during Church of England activities.*

Legitimate Interest Assessment

The summary below sets out the basis of the legitimate interest:

<i>We have a specific purpose with a defined benefit</i>	<i>The processing is an essential part of the Church of England's response to the dealing with safeguarding matters to protect individuals from harm, in particular those that are the most vulnerable, (children and/or vulnerable adults).</i>
<i>The processing is necessary to achieve the defined benefit.</i>	<i>The processing is necessary to investigate an allegation/concern effectively and to manage any subsequent risk as well as to help improve safe working practices in and around Church activities and ensure that the Church is a safe place for everybody.</i>
<i>The purpose is balanced against, and does not override, the interests, rights and freedoms of data subjects.</i>	<i>There is the risk of significant harm to others if unsuitable individuals are appointed to positions of authority and responsibility where they can be trusted by others. Similarly, there is a risk of harm to individuals where safe working practices are not adopted or cannot be reviewed and improved. The duty to protect individuals from harm, overrides any risks to the rights and freedoms of data subjects as appropriate safeguards have been put in place.</i>

3.3 Processing undertaken

- *Recording all information received and requested on SafeBase.*

3.4 Data storage and security

- *H: drive limited access by Safeguarding Team and HR Director.*
- *SafeBase limited access by Safeguarding Team and HR Director.*

4 Data sharing

Where necessary (or required), we collect from or share information with:

- Related organisations eg Oxford Diocesan Board of Education
- Parishes e.g. Parochial Church Councils (PCCs) and relevant PCC members, diocesan bodies, bishops' offices and cathedrals.

- Bodies covered by the Church of England Information Sharing Framework or Agreement
- candidates, prospective employees, employees or other staff members (including contractors, workers, consultants and volunteers, including members of any “Core Group”)
- legal representatives
- parties and individuals involved in or connected with legal claims, inquiries, reviews and dispute resolution (including mediation and arbitration)
- healthcare, social and welfare organisations or providers of health, social care or welfare services
- educational institutions
- governance bodies and committees
- 3rd party data processors
- local and central government
- both houses of parliament and members of parliament
- regulatory and statutory bodies
- law enforcement and prosecuting authorities
- courts and tribunals and providers of legal services
- members of the judiciary
- charitable, religious and voluntary organisations
- survey and research organisations
- statutory, public, regulatory or other legal or independent reviews or inquiries, including any “lessons learned” reviews

5 Retention and destruction

5.1 Data retention policy

Data is destroyed immediately when cases cease to be active or in accordance with timescales shown.

- Clergy – 70 years from date of cleric’s death¹.
- Lay Church Officers (*Someone who is appointed to role on behalf of the Church whether they are ordained or lay – paid or unpaid e.g.: Churchwarden, Parish Safeguarding Officer & volunteers.*) – 75 years following end of role². (Safeguarding Record Retention, Church of England, 2017).

5.2 Destroying data

- *unwanted documents are shredded*
- *Electronic data is deleted.*
- *Hard copies are shredded.*

¹ See ‘[Personal Files Relating to Clergy](#)’ page 10 paragraph 34 (May 2018)

² See ‘Safeguarding Record Retention’, Church of England (2017)