YR EGLWYS YNG NGHYMRU THE CHURCH IN WALES

CORFF CYNRYCHIOLWYR YR EGLWYS YNG NGHYMRU
THE REPRESENTATIVE BODY OF THE CHURCH IN WALES

PRIVACY NOTICE – PROVINCIAL SAFEGUARDING TEAM

This document is prepared pursuant to Section 39 Schedule 1 Part 4 Data Protection Act 2018.
The Church in Wales committed to maintaining your trust by protecting your personal data. Personal data is any information relating to an identified or identifiable person. The Church in Wales Safeguarding Team, which is part of the Representative Body of the Church in Wales, will process your personal data in a transparent and lawful way.

1. Data controller(s)

1.1 This privacy notice is provided for and on behalf of the Representative Body of the Church in Wales ("the RB") to explain what to expect when the RB collects your personal information.
The RB is the relevant data controller for these purposes. Its full name and address is as follows: *The Representative Body of the Church in Wales, 2 Callaghan Square, Cardiff, CF10 5BT.*

2. Why we collect and use your personal data

2.1 Personal information is collected to enable the RB to carry out their safeguarding responsibilities to support the mission and ministry of the Church in Wales and its members, including the following activities:

- Promoting and supporting the mission and ministry of the Church in Wales
- Provision of training and education
- Provision of safeguarding services
- The provision of legal advice
- Liaison with public, statutory and regulatory enquiries (including legal and independent reviews and inquiries) and courts and tribunals
- Litigation, dispute resolution and judicial process (including liaison with external advisers)
- Publishing resources, reports and reviews
- Corporate administration and all activities we are required to carry out as data controllers
- Undertaking research and statistical analysis
- Managing archived records for historical and research reasons, including the management of administration of access to our collections
- Maintaining our own accounts and records
- Ensuring the safety of those that work for or are employed by a legal entity that forms part of the institutional Church in Wales, including contractors and office holders, members of the Church in Wales and members of the public

3. The categories of personal data we collect:

3.1 The types of information we process include:

- personal details
- contact information

- family details
- lifestyle and social circumstances
- employment and education details
- housing needs

We also process "special categories" of information that may include:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- health;
- sex life; or
- sexual orientation
- criminal allegations, proceedings or convictions.

We process personal information about:

- current, retired and prospective clergy
- employees and office holders
- volunteers
- attendees at worship and events
- complaints of misconduct and unlawful acts
- individuals involved in or connected with legal claims, inquiries, reviews and dispute resolution
- professional advisers and consultants
- children and parents
- individuals whose safety has been put at risk

4. The lawful basis for using your information

4.1 As set out above we collect personal data, including some "special categories" of information. We collect and use personal data under one or more of the legal bases which are set out in Article 6 of the UK-GDPR.

4.2 We collect and use "special categories" of data under one or more of the legal bases which are set out in Article 9 of the UK-GDPR. We may also process personal data relating to criminal convictions and offences on the basis allowed in Article 10 of the GDPR.

4.3 Personal data

- Public task – we may need to process your information where it is necessary to undertake a duty or task in the public interest. In particular, this includes making sure that the provision of services and activities by the Church in Wales is safe for all members of the public and so far as possible assists in upholding the law and preventing the commission of any offences.

- Public task – we may need to process your information in order to undertake tasks and duties which relate to the operational aspects of the Church in Wales and includes sharing and receiving data with and processed by the various bodies and officials which make up the Church in Wales. This includes doing all that we reasonably can to ensure that no

member of the public, members of the Church in Wales or anybody who works for or is employed by a legal entity which is part of the Church in Wales, including contractors and office holders, is at risk of harm in connection with the activities of the Church in Wales. See in that regard, the Church in Wales Safeguarding Policy:

https://www.churchinwales.org.uk/en/publications/administration-and-business/Safeguarding_Documents/

- Legal obligation – we may need to process your information in order to comply with a legal obligation imposed on us, for example, the Inquiries Act 2005 can compel bodies to provide certain information, which may include personal data, for the purposes of a statutory inquiry; or a referral to the Disclosure and Barring Service under the Safeguarding Vulnerable Groups Act 2006, or an order of a court or tribunal.

4.4 **Special categories & criminal information**

- Substantial public interest (protecting the public against dishonesty etc.) – we may need to process your information for a reason of substantial public interest. In particular, this condition is met where it is necessary for the exercise of a "protective function", as defined in Schedule 1, Paragraph 11(2) Data Protection Act 2018, including the protection of members of the public generally against seriously improper conduct and from any failures in connection with the Church in Wales's activities, or for safeguarding purposes.

- Legal claims – we may need to process your information where it necessary to do so for the establishment, exercise or defence of legal claims or in connection with judicial process.

- Archiving - we may process your information for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes including the organisation, preservation of, and controlled access to, segments of the Church's history.

4.5 We will only use your personal data for the uses and purposes set out above, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original use and purposes. If we need to use your personal data for an unrelated purpose, we will notify you and will explain the legal basis which allows us to do so.

4.6 Where we need to use the lawful basis of Legitimate Interest we will conduct a legitimate Interest Assessment in regard to processing your personal data. Such an assessment will be published in our data protection documents.

4.7 We will consider whether the purpose of the proposed processing is balanced against and does not override, the interests, rights and freedoms of data subject(s).

4.8 In regard to Safeguarding matters such considerations will include whether there is a risk of significant and/or serious harm to others, especially in cases where unsuitable individuals are or may have been appointed to positions of authority and responsibility and/or roles where they are trusted by others and/or have unsupervised access to at-risk persons.

4.9 We consider that this risk is greatest where allegations are not identified and/or properly addressed. Consequently, we may consider this risk to be balanced when it does not override, your interests, rights and freedoms.

5. Who we collect from or share your information with:

5.1 Where necessary or required to meet the purposes listed, we collect from or share information with:

- parishes, dioceses, bishops and cathedrals
- candidates, prospective employees, employees or other staff members (including contractors, workers, consultants and volunteers, including members the Provincial Safeguarding Panel (which offers expert assistance to bishops and RB employees)
- 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 or health, social care or welfare services
- educational institutions
- governance bodies and committees
- 3rd party data processors
- local and central government
- 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

6. Transfer of Personal Data outside the UK

6.1 Your personal data will not be sent to countries outside the UK~~,~~ without the necessary safeguards.

6.2 The RB does not share your information with Countries outside of the UK without safeguards being in place that are equivalent to the UK data protection legislation or the GDPR.

7. How long do we keep your information?

7.1 The length of time data is retained is laid out in our retention schedule which is appended to this notice (and, in relation to clergy, in our Clergy Personal Files Policy, available separately on our website).

8. Security

8.1 We are committed to ensuring that your personal data is secure. To prevent unauthorised access or disclosure, we have put appropriate technical and organisational measures in place to safeguard your information.

8.2 The RB assure this by complying with relevant security best practice standards. If a data breach does occur, we will do everything in our power to limit the damage and comply with the Information Commissioner's guidance.

8.3 In the case of a high-risk data breach, and depending on the circumstances, we will inform you about the remedial actions to prevent any further damage. We will also inform the Information Commissioner's Office of any qualifying data breaches.

8.4 The procedures and related standards we apply include limiting access to data on a need to know basis and regularly testing and auditing our security practices and technologies. Employees and temporary workers are required to follow policies and procedures and complete mandatory annual training to understand data protection and information security.

8.5 All RB personnel receive training in data protection and the responsible use of Personal Data. Third party Data Processors are engaged on contractual arrangements containing requirements of confidentiality and data processing security.

8.6 We recognise the need for structural and organisational data security and have included such measures within our internal data protection systems by design. The following policies deal with the forward planning and organisational security arrangements.

8.7 **Antivirus and Online protection**

8.8 We employ World leading cyber security software, known as 'Darktrace', which includes unique Artficial Intelligence (AI) learning algorithms to ensure maximum security for our IT systems.

8.9 **Data Transfers.**

8.10 Personal Data under our control will only be transferred to a third party Data Controller under the terms of a written data processing or data sharing contract and where we have received sufficient guarantees of safeguards from them as Data Controllers in their own right.

8.11 Personal Data sent by email will be encrypted where possible.

8.12 Where it is necessary to transfer the password or encryption code for an email it will not be transferred with the same email.

8.13 SMS transfers of Personal Data will be kept to an absolute minimum and only sent to telephone numbers which have previously been satisfactorily identified as the correct recipient, ideally after a confirmatory voice call on that particular line.

8.14 Particular attention and special care will be taken when transporting Personal Data offsite. Such as transporting removable media and computers for homeworking. Confirmation should be made prior to such activity that the device is encrypted at rest.

8.15 **Data Storage**

8.16 Personal Data is held by us in secure electronic devices such as computers, Tablets, mobile phones and separate back up devices, computers and Internet Cloud based servers.

8.17 Data is also held by us in paper form in files relating to individuals, which are secured by managed access protocols and by virtue of the physical security at their location.

8.18 We have no plans to introduce new technology such as face recognition, biometrics or fingerprint recognition into our Data Processing activities but if such a change is made or planned to be made, we will complete a Data Protection Impact Assessment and update this policy statement.

8.19 Hard copies of Personal Data will be kept securely in a locked room or area, a locked cupboard or secure filing system.

8.20 Removable Media containing Personal Data are kept securely in a locked cupboard or secure filing system or encrypted.

9. Automated decision making without access to human intervention.

9.1 Generally your personal data will not be used for any automated decision making without access to human intervention.

9.2 However, there may be occasions where we use authorised agencies to discover information in relation to your status such as Criminal records, DBS checks and Credit agency searches. In such matters the computer information will be accepted by Ourselves, although there are procedures for challenging such information by you. (See 'Your Rights' below).

10. Your rights

10.1 You have the following rights regarding your personal data:

Your rights	What this involves	What our obligations are
A right to be Informed	This is the right to know if we are processing information about you.	• Subject to certain exemptions, we must respond to any requests you make to know if we are processing your data.
A right of access	This is a right to obtain access to your personal data and various supplementary information.	• We must provide you with a copy or your Personal Data and the other supplementary information without undue delay and in any event within one month of receipt of your request; • We cannot charge you for doing so save in specific circumstances (such as where you request further copies of your Personal Data).
A right to have personal data rectified	This is a right to have your Personal Data rectified if it is inaccurate or incomplete.	• We must rectify any inaccurate or incomplete information without

		undue delay and in any event within 1 month of receipt of your request; • If we have disclosed your Personal Data to others, we must (subject to certain exceptions) contact the recipients to inform them, that your Personal Data requires rectification.
A right to erasure	• This is a right to have your Personal Data deleted or removed. • This right only applies in certain circumstances (such as where we no longer need the Personal Data for the purposes for which it was collected). • We have the right to refuse to delete or remove your personal data in certain circumstances.	• If this right applies, we must delete or remove your Personal Data without undue delay and in any event within one month of receipt of your request; • If we have disclosed your Personal Data to others, we must (subject to certain exceptions) contact then recipients to inform them that your Personal Data must be erased.
A right to data portability	• This is a right to obtain and re-use your Personal Data for your own purposes; • It includes a right to ask that your Personal Data is transferred to another organisation (where technically feasible). • This right only applies in certain limited circumstances. • Following a request relating to Data Portability we will transmit the relevant personal data to the data subject or their nominated data controller where it is possible and technically feasible for us to do so.	• If this right applies we must provide your Personal Data to you in a structured, commonly used and machine reasonable form • Again, we must act without undue delay and in any event within 1 month of receipt of your request; • We cannot charge you for this service.
A right to object	• This is a right to object to the use of your Personal Data.	• If you object to us using your Personal Data for direct marketing, we must stop using your

	• The right applies in certain specific circumstances only. • You can use this right to challenge our use of your Personal Data based on our legitimate interests; • You can also use this right to object to use of your Personal Data for direct marketing	Personal Data in this way as soon as we receive your request. • If you object to other uses of your Personal Data, whether we have to stop using your Personal Data will depend on the particular circumstances.
A right to object to automated decision making	• This is a right not to be subject to a decision which is made solely on the basis of automated processing of your Personal Data where the decision in question will have a legal impact on you or a similarly significant effect. • We may use Automated decision making about you if it is necessary for entering into or performing a Contract with you or where you Consent to the actions.	• Where such a decision is made, you must be informed of that fact as soon as reasonably practicable; • You then have 21 days from receipt of the notification to request that the decision is reconsidered or that a decision is made that is not based solely on automated processing; • Your request must be complied with within 21 days.
A right to restrict processing	• This is a right to 'block' or suppress processing of your Personal Data. • This right applies in various circumstances including where you contest the accuracy of your information).	• If we are required to restrict our processing of your Personal Data we will be able to store it but not otherwise use it. • We may only retain enough information about you to ensure that the restriction is respected in future. • If we have disclosed your Personal Data to others, we must (subject to certain exceptions) contact them to tell them about the restriction on use.
Legitimate Interests	• If the processing is based on Legitimate Interests, you are entitled to know what and whose Legitimate Interests they are.	• There are some exceptions to the additional information rule. If we obtain your Personal Data from a source other than yourself, the additional

Data from sources other than the Data Subject.	• This lawful basis is used only after conducting a three part test to ensure the data subjects rights are properly protected • If we process data about you but we have not obtained the data personally from you, we must provide you with the information described in this Privacy Notice and some additional information. • You are entitled to know the source of the information and whether the source is publicly accessible.	information rules will apply unless:- • You already have the information regarding our processing; or • it would take a disproportionate effort or be impossible to provide you with it; or • you are already legally protected under separate provisions; or • we have a legal duty not to disclose it.

10.2 If you wish to exercise these rights, please contact the Church in Wales Data Protection Officer using the contact information provided below.

11. Complaints or concerns

11.1 If you have any concerns or queries about how the RB handle your personal data, please contact the Church in Wales Data Protection Officer at dataprotection@churchinwales.org.uk or write to us at The Church in Wales, 2 Callaghan Square, Cardiff, CF10 5BT.

11.2 You also have the right to make a complaint at any time to the Information Commissioner at https://ico.org.uk/concerns/ or:

Information Commissioner's Office
Wycliffe House
Water Lane Wilmslow Cheshire SK9 5AF
Tel: 0303 123 1113 (local rate)

Appendix:
Safeguarding Records - Retention Policy

Summary

This document provides guidelines to those in the Church in Wales for the retention of safeguarding records, both in the context of the ongoing Independent Inquiry into Child Sexual Abuse and following the conclusion of the Inquiry.

For the purpose of this guidance safeguarding records includes:

- **Allegations/Concerns:** Any information that relates to allegations of abuse by clergy, office holders or members of the Church in Wales or any information that relates to a concern around a risk of potential harm to a child or adult e.g. referral information, advice and guidance offered to parishes, case files and records.
- **Risk Assessments:** Any information that relates to risk assessments and managing risk in church settings.
- **Employment**: Any information that relates to the recruitment, support and training of clergy, office holders and employees in line with good practice in safer recruitment (including information from the Disclosure and Barring Service).
- **Discipline:** Any information that relates to disciplinary action in relation to a member of the clergy, office holder, employee or member of the Church in Wales e.g. clergy personal files, supervision files, personnel files, disciplinary tribunal files, provincial court files.
- **Governance:** Any information that relates to the safeguarding leadership and governance and safeguarding practices and policy e.g. minutes of provincial safeguarding panel, safeguarding advisory group, policy development, training delivery records, Quality Assurance processes and outcomes etc.

This policy covers:

- The requirements of the Independent Inquiry into Child Sexual Abuse
- The requirements of the *Data Protection Act* insofar as it relates to safeguarding
- What types of records to keep and how long to keep them for

Independent Inquiry into Child Sexual Abuse (IICSA)

In March 2015 the UK Government announced the establishment of an inquiry into child sexual abuse in various institutions. At the outset of the Inquiry organisations within the scope of the Inquiry (which included the Church in Wales) were asked with regard to their records and record keeping "to ensure that everything of potential relevance to the Inquiry is retained".

The Inquiry consulted with the Information Commissioner's Office and issued detailed guidance on document retention: '*Retention Instructions and Data Protection requirements*'[1] which confirms not only that prolonged retention of records necessary for the Inquiry would not contravene the Data Protection Act goes further in stating that '*Under Section 21 of the Inquiries Act 2005 the Inquiry has the power to order the production of documents. Failure to comply with such an order without reasonable excuse is an offence punishable by imprisonment (Section 35 of the Inquiries Act 2005). It is also an offence for a person, during the course of an Inquiry, to destroy, alter or tamper with evidence that maybe relevant to an Inquiry, or deliberately to do an act with the intention of suppressing evidence or preventing it being disclosed to the Inquiry*'.

[1] https://www.iicsa.org.uk/key-documents/115/download/2018-07-25-guidance-note-retention-instructions-data-protection-requirements-version-2.pdf

This request supersedes any existing retention schedules and policies. All records which may be relevant to the Inquiry should **NOT BE DESTROYED** but must be retained and then should be reviewed after the Inquiry is complete. Relevant material will include:

- Case work related files
- Case work related referral/enquiries/support and advice
- Risk assessments and agreements
- Quality Assurance information e.g. audits, data returns, action and improvement plans
- Files relating to Education establishments, recruitment and safeguarding
- HR Staff files non clergy: current and leavers
- HR Staff files: Employment tribunal cases
- HR Staffing reviews; HR Staffing reviews (Diocesan Bishop's Staff)
- Clergy Personal files: current and leavers
- Clergy discipline: Discipline case files
- Files on appointments to councils, committees and other bodies
- Files and papers relating to Subject Access Requests
- Safeguarding leadership and governance e.g. Governing Body, Representative Body, Provincial Safeguarding Panel e.g. meeting agenda and minutes
- Details of blemished DBS checks, referrals , update schedules and risk assessments
- Any separate records of allegations/concerns in relation to Church Officers.

If in doubt consult the Church in Wales Safeguarding Team or the Head of Legal Services.

Retention Schedule – Categories and Retention Periods

Please note that any records which may hold any relevance to the Independent Inquiry into Child Sexual Abuse (IICSA) should **NOT BE DESTROYED AND MUST BE RETAINED.** Some of the retention periods in this guidance note may differ from previous guidance.

NB: In relation to the Clergy, please also refer to the Clergy Personal Files Policy.

	Description	**Record Keeping**	**Retention**
Casework	Records of child or adult protection incident or concerns within a Parish/Diocese/Cathedral etc. or family where the church either reports concerns or is involved in supporting and monitoring a child adults or families. This includes risk assessments and 'agreements' (including worship agreements)	It is essential that a record of any safeguarding allegations and concerns, and how these are handled-how the information was followed up; actions taken; decisions reached and eventual outcomes - should be kept.	70 years after last contact with the individual concerned.
	Records that relate to safeguarding concerns/allegations about office holders paid or unpaid including details of how these are handled, followed up, actions taken, decisions reached and eventual outcome	It is essential that a record of any safeguarding allegations and concerns, and how these are handled-how the information was followed up; actions taken; decisions reached and eventual outcomes - should be kept.	75 years after employment/volunteering ceases. In the case of clergy, 70 years after death, in accordance with the Clergy Personal Files Policy.

	Description	Record Keeping	Retention
Activities	Records of any children's activities, Sunday school/junior church/youth club/choirs and related safety risk assessment		50 years after the activity ceases.
	Description	**Record Keeping**	**Retention**
Employment	Personnel records relating to lay workers who do not work with children and vulnerable adults		6 years after employment ceases
	Personnel records relating to lay workers whose role involves contact with children and vulnerable adults including applications, references, disciplinary matters, job descriptions, training and termination documentation. All documentation concerning allegations, investigations and risk assessments regardless of findings.		75 years after employment
	Description	**Record Keeping**	**Retention**
Discipline	Record of Discipline Tribunal complaints including copies of the complaint, report of preliminary officer/committee, respondent's evidence, proctor's supporting evidence, judgment/findings		70 years after respondent's death.

Version 09/23 – I
June 2023