

**The Representative Body of the Church in Wales (“The RB”)**

**Staff Privacy Notice Updated January 2024**

**This Privacy notice Contains the Following Sections**

<b>SECTION HEADING</b>	<b>PAGE NUMBER</b>
<b>GENERAL INFORMATION</b>	<b>2</b>
<b>WHAT PERSONAL DATA DO WE HOLD ABOUT YOU?</b>	<b>2</b>
<b>USE OF DATA TABLE – FULL &amp; PART TIME STAFF</b>	<b>3</b>
<b>COMPUTER MONITORING POLICY</b>	<b>5</b>
<b>INTERNATIONAL TRANSFER OF DATA</b>	<b>5</b>
<b>WHAT RIGHTS YOU HAVE UNDER DATA PROTECTION LAW?</b>	<b>6</b>
<b>FEES PAYABLE TO EXERCISE YOUR RIGHTS</b>	<b>8</b>
<b>IDENTITY INFORMATION WE MAY NEED FROM YOU</b>	<b>9</b>
<b>CHILDRENS DATA</b>	<b>9</b>
<b>ACCURACY OF PERSONAL DATA</b>	<b>9</b>
<b>WHERE TO GO IF YOU WANT MORE INFORMATION ABOUT YOUR RIGHTS OR TO MAKE A COMPLAINT</b>	<b>9</b>
<b>THIRD PARTY WEBSITES</b>	<b>10</b>
<b>CONTACT US</b>	<b>10</b>
<b>UPDATES TO THIS PRIVACY NOTICE</b>	<b>10</b>

## **1. General Information**

- 1.1 We are committed to protecting the privacy and security of your Personal data. We have robust information security management systems in place to protect your personal data. We take the security of your information seriously and have implemented appropriate technical and organisational security measures to protect it against any unauthorised or unlawful processing and against any accidental loss, destruction, or damage.
- 1.2 This is a precis Privacy Notice which applies to the Personal Data we process of our Staff Members. A Staff Data Protection handbook both sectionalised and in full format is available on our website.
- 1.3 We are the “data controller” for the Personal data we process. This means that we hold Personal data about our staff members and are responsible for deciding how we store and use that Personal data.
- 1.4 As data controller, we are legally required to provide certain information to individuals whose Personal data we collect, obtain, store and use. That information is contained in this document (our “Privacy Notice”).
- 1.5 It is important that you read this document (together with the Staff Data Protection Handbook and any other Privacy Notices we may provide to you on specific occasions), so that you are aware of how and why we are using your Personal data and the rights you have in relation to your Personal data.
- 1.6 The scope of this Privacy Notice is that it applies to all RB Staff.
- 1.7 As a Data Controller, we will take all the necessary steps to comply with the UK GDPR and Data Protection Act 2018 and other relevant primary and subordinate legislation and Regulations when handling any personal data which you may provide to us. We are responsible for ensuring that data is:
  - 1.7.1 Fairly and lawfully processed
  - 1.7.2 Processed for limited purposes
  - 1.7.3 Adequate, relevant and not excessive
  - 1.7.4 Accurate and Secure;
  - 1.7.5 Not kept longer than necessary
  - 1.7.6 Processed in accordance with your rights
  - 1.7.7 Not transferred to countries outside the UK without safeguards.
  - 1.7.8 In a manner that ensures appropriate security of the personal data.
- 1.8 We will not sell, rent or otherwise disclose the personal information you provide to us through the site to third parties (other than as listed below) unless we are required to do so by law.

## **2. What Personal data do we hold about you?**

- 2.1 As a staff member of the RB we will ask you to provide us with certain Personal data relating to you when you are engaged and at certain points during your employment.
- 2.2 Data protection law protects Personal data which is essentially any information from which an individual can be identified.

2.3 There is a type of Personal data which receives additional protection because of its sensitive or private nature, this is sometimes referred to as ‘special category personal data’ and means Personal data about an individual’s race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual’s health, sex life or sexual orientation.

### **3. The RB Staff – Full & Part Time – Use of Data Table**

<b>Personal Data</b>	<b>Lawful Base(s) and Statutory authority</b>	<b>Retention Period</b>	<b>Source of Data Use of Data &amp; Data Sharing</b>	<b>Types of Personal Data we may use</b>
<p>Your name;</p> <p>Your contact details (such as your postal address, telephone number and/or email address);</p> <p>Next of kin/Family data for contact in an emergency</p> <p>Your Bank Account details (if in a paid post);</p> <p>Your role with the Church in Wales (which may reveal your religious beliefs);</p> <p>Access to your data via the Computer Monitoring Policy. (See section 3.1 below)</p>	<p><b>Consent</b> We may process data with your consent such as in the early stages of applying for a role.</p> <p><b>Contract</b> The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the direct request of the data subject prior to entering into a contract.</p> <p><b>Public Task</b> Use of your Personal Data for administrative purposes, to ensure the smooth and proper running of the Church.</p> <p><b>Special Category Data</b> The lawful authority we rely on to process any information provided as part of an employment application which is special category data, such as health, religious or ethnic information is Article 9(2)(b) of the UK GDPR, which also relates to our obligations in employment and the safeguarding of the employee’s fundamental rights and article 9(2)(h) for assessing an individual’s work capacity as an employee.</p>	<p>Your contact details will be retained for the duration of your employment and for 7 years thereafter.</p> <p>DBS disclosure results will ordinarily be destroyed within six months of receipt.</p> <p>In the event that the disclosure result highlights concerns relating (in the view of our Safeguarding Manager) to safeguarding of children and/or adults at risk, a record of the disclosure results will be retained securely by our Safeguarding Team indefinitely.</p>	<p>Your personal data will usually be provided to us by you directly</p> <p>We will share your contact details with other departments within the RB for specific admin matters including training.</p> <p>We will use your bank account details to pay your wages and any expenses due;</p> <p>We will collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.</p> <p>We carry out DBS checks on behalf of other parts of the Church in Wales, such as on behalf of</p>	<p>We may process the following types of data about you</p> <p><b>Identity</b> <b>Financial</b> <b>Transaction</b> <b>Technical</b> <b>Profile</b> <b>Usage</b> <b>Marketing</b></p> <p>If your name and contact details are not provided you will be unable to be appointed as a staff member or receive salary payments, pension rights or other related financial matters.</p> <p>Further details regarding this are available in section 3.2 below.</p>

	<p>Where DBS Checks are conducted they are part of an automated decision making process pursuant to Article 22 UK GDPR.</p> <p>The information provided by the DBS service is used to assess suitability for appointment to a post.</p> <p><b>Legal Obligation</b> We will only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary for reasons of substantial public interest, namely, safeguarding, preventing or detecting unlawful acts, protecting the public against dishonesty, preventing fraud or suspicion of terrorism or money laundering.</p> <p>This is because the Church in Wales has a Legal Obligation to take all reasonable precautions to ensure that the Church is a safe place for all.</p> <p>Also, Schedule 1 part 1(1) and (2)(a) and (b) of the Data Protection Act 2018 which relates to processing for employment, the assessment of working capacity and preventative or occupational medicine.</p> <p><b>Legitimate Interest</b> This lawful basis is used for our CCTV systems and when staff members use Video conferencing software. (see separate legitimate interest assessments)</p>		<p>the Bishops or Diocese.</p> <p>The information obtained will be used by us in conjunction with other parts of the Church in Wales to determine whether to engage you.</p> <p>Information about criminal convictions will be obtained from the Disclosure and Barring Service ("DBS") if you have agreed to undertake a DBS check through the Church in Wales.</p> <p>We will share your data with certain third party organisations who provide services to assist us with certain matters such as external Human Resources policy providers and software companies.</p> <p>A list of these third parties is available on request.</p>	
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

- 3.1 Monitoring of Computers and Remote/Home workers
- 3.1.1 The Representative Body of the Church in Wales IT team employ robust software protection measures to keep our systems safe but the software is not infallible and care must be taken by employees not to allow computer viruses, bugs etc into the system.
  - 3.1.2 To assist in preventing cyber attacks and hacking, particular care must be taken when opening emails from external sources, if in doubt do not open the email and seek advice from the IT team. Further information is available in the Staff Data Protection Handbook - Email Protection Policy.
  - 3.1.3 To help employees understand the protection mechanisms of the IT systems and aid them to keep the systems safe, we have developed a Computer Monitoring Policy for our Staff Data Protection Handbook.
  - 3.1.4 The Computer Monitoring Policy explains that the Representative Body has the ability to monitor the use of its computers whether in use in their offices or remotely, the information available includes when the user logged on and off, which Websites were accessed and which software was used during the period of activity e.g. Microsoft Teams, Outlook etc.
  - 3.1.5 The Computer Monitoring Policy is an entirely reactive policy i.e. users are not actively monitored while they are working but the information is available should it be necessary to review it at a later time.
  - 3.1.6 The Computer Monitoring Policy is available to all staff members in Section 11.9 of the data protection staff handbook on the Provincial staff Portal:  
DOCUMENTS>STAFF GUIDANCE>STAFF DATA PROTECTION HANDBOOK
- 3.2 The types and categories of data we may collect from you includes the following:
- 3.2.1 **Identity data:** name, username, title, date of birth. Contact data: billing and delivery address, email address, phone number.
  - 3.2.2 **Financial data:** payment card details (processed by a third-party payment services provider and not stored by us).
  - 3.2.3 **Transaction data:** details of products purchased, amounts, dates etc.
  - 3.2.4 **Technical data:** IP address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform based on your Cookie preference choices.
  - 3.2.5 **Profile data:** username and password, enquiries, purchases or orders made by users.
  - 3.2.6 **Usage data:** information about how users use our Website based on Cookie permissions selected.
  - 3.2.7 **Marketing and communications data:** A record of Website users preferences in receiving marketing from us.

#### **4. International Transfer of Your Information**

- 4.1 We do not generally operate outside of the United Kingdom or transfer any of your personal data outside of the United Kingdom but we may maintain professional contacts in other countries, such as for arranging visits to churches and other institutions around the World.
- 4.2 All Personal data and information collected in any State will be processed in the UK.
- 4.3 Due to the operation of the Internet and other computer based applications Personal data under our control may transit countries outside of the UK.
- 4.4 We will only transfer Personal data outside of the UK if adequate safeguards are in place in the destination country.
- 4.5 Where Personal data is transferred to a third country or an international organisation we will ensure that an adequacy decision or similar authority exists between the UK and the relevant country or area.
- 4.6 Where no adequacy decision exists and we rely on the provisions of Standard Contractual Clauses or Binding Corporate Rules evidence of the safeguards provided thereby will be available upon request.
- 4.7 The Main Establishment for all of our Data Processing is the UK.
- 4.8 The lead supervisory authority is UK Law and the UK Information Commissioners Office whose address is Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

#### **5. What Rights You Have Under Data Protection Law**

As a staff member of the RB you have all the rights associated with all Data Subjects. A precis and explanation of those rights is in the chart below.

<b>Your rights</b>	<b>What this involves</b>	<b>What our obligations are</b>
<b>A right to be Informed</b>	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.
<b>A right of access</b>	This is a right to obtain access to your personal data and various supplementary information.	We must provide you with a copy of 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).
<b>A right to have personal data rectified</b>	This is a right to have your Personal Data rectified if it	We must rectify any inaccurate or incomplete information without

	is inaccurate or incomplete.	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.
<b>A right to erasure</b>	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.
<b>A right to data portability</b>	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  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.
<b>A right to object</b>	This is a right to object to the use of your Personal Data.  The right applies in certain specific circumstances only.	If you object to us using your Personal Data for direct marketing, we must stop using your 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

	<p>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</p>	<p>stop using your Personal Data will depend on the particular circumstances.</p>
<p><b>A right to object to automated decision making</b></p>	<p>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.</p> <p>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.</p>	<p>Where such a decision is made, you must be informed of that fact as soon as reasonably practicable;</p> <p>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;</p> <p>Your request must be complied with within 21 days.</p>
<p><b>A right to restrict processing</b></p>	<p>This is a right to ‘block’ or suppress processing of your Personal Data.</p> <p>This right applies in various circumstances including where you contest the accuracy of your information).</p>	<p>If we are required to restrict our processing of your Personal Data we will be able to store it but not otherwise use it.</p> <p>We may only retain enough information about you to ensure that the restriction is respected in future.</p> <p>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.</p>
<p><b>Legitimate Interests</b></p>	<p>If the processing is based on Legitimate Interests, you are entitled to know what and whose Legitimate Interests they are.</p> <p>This lawful basis is used only after conducting a three part test to ensure the data subjects rights are properly protected</p>	<p>There are some exceptions to the additional information rule. If we obtain your Personal Data from a source other than yourself, the additional information rules will apply unless:-</p> <p>You already have the information regarding our processing; or</p>



<p><i>Data from sources other than the Data Subject.</i></p>	<p>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.</p> <p>You are entitled to know the source of the information and whether the source is publicly accessible.</p>	<p>it would take a disproportionate effort or be impossible to provide you with it; or</p> <p>you are already legally protected under separate provisions; or we have a legal duty not to disclose it.</p>
--------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## **6. Fees payable to exercise your data protection rights.**

- 6.1 You will not usually have to pay a fee to access your Personal data (or to exercise any of the other rights).
- 6.2 Following receipt of a Data Subject Access Request (DSAR) assuming there are no issues relating to your identity, we will send you, without delay and in any case within one Month, the Personal Data we hold relating to you, which we are legally obliged to provide.
- 6.3 In the event we need more time to gather the requested information we will let you know without delay and in any event within one month from receipt of your request.
- 6.4 A fee may be payable for Data Access services if your request(s) are manifestly unfounded or excessive or repetitive in nature. Alternatively, we may choose to ignore this type of request. In these cases we will inform you of our decision and if applicable any fee that may be required.

## **7. Identity information we may need from you**

- 7.1 We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights).
- 7.2 This is another appropriate security measure to ensure that Personal data is not disclosed to any person who has no right to receive it.

## **8. Children's data**

- 8.1 We do not currently employ anyone under the age of 18 years. If this situation changes we will update this policy as necessary.
- 8.2 Our Website is not directed at children.
- 8.3 We will not knowingly collect information from persons under 13 years of age without their parent's or guardian's consent.

## **9. Accuracy of Personal Data**

- 9.1 If any of your personal details change during your employment you should contact the Human Resources team to notify them and provide them with the updated accurate information.

## **10. Where to Go if You Want More Information About Your Rights or to make a Complaint**

- 10.1 The Information Commissioner's Office (ICO) regulates data protection and privacy matters in the UK. They make a lot of information accessible on their website and they ensure that the registered details of all data controllers such as ourselves are available publicly. You can access them here [www.ico.org.uk](http://www.ico.org.uk)
- 10.2 If you feel we have not handled your data correctly, you can make a complaint to the Information Commissioners Office (ICO). Their contact details are [www.ico.org.uk](http://www.ico.org.uk) The ICO's telephone number is 0303 123 1113. However, we hope that you would consider raising any issue or complaint you have with us first. We will always do our very best to solve any problems you may have.

## **11. Third Party Websites**

- 11.1 From time to time our site may contain links to and from the websites of our suppliers or other third party sites.
- 11.2 If you visit any of these sites you should confirm they have their own privacy policies and you should check these before submitting any personal data on their site. We cannot accept any responsibility or liability for the policies on any other Websites.

## **12. Contact us**

- 12.1 You're welcome to get in touch with us to discuss your information at any time.
- 12.2 Our full name is The Representative Body of the Church in Wales.
- 12.3 We are the data controller of the information you provide us with. The term "data controller" is a legal phrase used to describe the person or entity that controls the way information is used and processed.
- 12.4 The Representative Body of the Church in Wales is Registered with the Information Commissioners Office under reference number Z6056416.
- 12.5 We have appointed a Data Protection Officer (DPO) to oversee compliance with this Privacy Notice. If you have any questions about this Privacy Notice or how we handle your Personal data, please contact the Data Protection Officer at The Representative Body of the Church in Wales, 2 Callaghan Square, Cardiff CF10 5BT or [dataprotection@churchinwales.org.uk](mailto:dataprotection@churchinwales.org.uk)

## **13. Updates to this Privacy Notice**

- 13.1 We review the ways we use your information regularly. In doing so, we may change what kind of information we collect, how we store it, who we share it with and how we act on it.

- 13.2 Consequently, we will need to change this Privacy Notice from time to time to keep it accurate and up-to-date. We will keep this policy under regular review to ensure it is accurate and kept up to date.
- 13.3 It is the responsibility of the individual visitor to our Website to keep themselves updated with changes to this policy.