The Representative Body of the Church in Wales

General Privacy Notice 2024/2025
Part One of Four

Procedural information and advice

1 The Representative Body Contact Details

1.1 The Representative Body of the Church in Wales hereinafter referred to as 'the RB', We, Us and Our.

1.2 Our email address for data protection matters is: dataprotection@churchinwales.org.uk

1.3 Data Protection queries may be addressed to us for the attention of The Data Protection Officer at The Representative Body of the Church in Wales, 2 Callaghan Square, Cardiff CF10 5BT

1.4 We are a Data Controller under the provisions of the UK GDPR and the Data Protection Act 2018 and have registered with the UK Information Commissioners office:

ICO Registration Number: Z 6056416

2 Status of key personnel

2.1 The Archbishop of Wales.

2.2 Chief Executive Officer - **Mr Simon Lloyd**

2.3 General Counsel and Head of Legal – **Mr Matthew Chinery**

2.4 We have designated **Mr Robert Linford** as **Data Protection Manager** for the RB.

2.5 The Data Protection Manager also takes the role of Data Protection Officer for the RB.

3 Introduction and Overview

3.1 The Representative Body of the Church in Wales (the "RB") is a charitable institution responsible for looking after the assets of the Church in Wales to ensure that resources are available for the benefit of the whole Church. You can find out more information about us at www.churchinwales.org.uk.

3.2 The RB is committed to the highest standards of information security and treats confidentiality and data security extremely seriously.

3.3 This privacy notice has been prepared in view of the Retained Regulation (EU) 2016/679, which is now assimilated law in the UK, in accordance with section 5 of the Retained EU Law (Revocation and Reform) Act 2023.

3.4 Pursuant to the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) the RB must:

(a) use technical or organisational measures to ensure personal data is kept secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage;

(b) implement appropriate technical and organisational measures to demonstrate that it has considered and integrated data compliance measures into the RB's data processing activities; and be able to demonstrate that it has used or implemented such measures and complied with the data protection principles.

(c) The RB maintains records of its own actions and our interactions with other Data Controllers and our Data Processors to ensure we can suitably demonstrate adherence to the data protection principles. Specifically, we ensure data is processed:

(i) Fairly, Lawfully and Transparently.

(ii) for limited purposes.

(iii) in a manner which is adequate, relevant and not excessive.

(iv) in a manner which is accurate and not kept for longer than necessary.

(v) in accordance with the prescribed rights.

(vi) for no longer than necessary.

(vii) in a manner which is secure and not transferred to countries outside the UK, without appropriate safeguards.

(viii) in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4 **The purpose of this policy is to:**

4.1 protect against potential breaches of confidentiality;

4.2 ensure all our data assets and IT facilities are protected against damage, loss or misuse;

4.3 support the RB's aims in ensuring all Website users, Service users and those holding an Office or position within the Church are aware of and comply with UK law and the RB's procedures applying to the processing of personal data; and

4.4 increase awareness and understanding within the RB of the requirement for information security and our responsibility to protect the confidentiality and integrity of the data we handle.

5 Definitions

5.1 This Policy applies to the following individuals, collectively ("The Cohort")

(a) Members of the Governing Body
(b) Clergy and Former Clergy (meaning clergy who have previously but no longer minister in the Church in Wales);
(c) Office and Post Holders;
(d) Tenants;
(e) Donors;
(f) Individuals who contact us with enquiries or complaints;
(g) Users of our website;
(h) Individuals who undertake training with the us;
(i) Individuals who feature in our newsletters or articles;
(j) Individuals who we engage to provide services to us; and
(k) Individuals who engage with us on social media.

5.2 For the purposes of this Policy the following definitions will apply:

Staff	means staff members of the RB and anyone holding an office or post under the Church in Wales when acting for the RB whether in a paid or volunteer capacity and; where applicable, temporary and agency workers, interns and apprentices; and to the extent permissible under the law any Self-employed data processors engaged under contract to the RB and includes their agents, employees and representatives as appropriate.
The Cohort	means the individuals listed in Section 5.1
business information	means business-related information other than personal information regarding customers, clients, suppliers and other business contacts of the RB;
RB information	means personal data relating to staff, customers, clients and suppliers; and Any other business information; and

Confidential information	Confidential information. (see below). means trade secrets or other confidential information (either belonging to the RB or to third parties) that is processed by the RB;
personal data	means data relating to an individual who can be identified (directly or indirectly) from that data; Personal data is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, e.g. their name, identification number, location data or online identifier.
pseudonymised	means the process by which personal data is processed in such a way that it cannot be used to identify an individual without the use of additional data, which is kept separately and subject to technical and organisational measures to ensure that the personal data cannot be attributed to an identifiable individual;
special category data	means personal data about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic data, biometric data (where used to identify an individual) and data concerning an individual's health, sex life or sexual orientation.

6 Roles and responsibilities

6.1 We consider that Information security is the responsibility of all. However, the RB's **Data Protection Manager** has particular responsibility for:

(a) monitoring and implementing this policy;

(b) monitoring potential and actual security breaches;

(c) ensuring staff are aware of their responsibilities by providing suitable training; and

(d) ensuring compliance with the requirements of the UK GDPR as assimilated law and other relevant legislation and guidance.

7 Scope of the Policy

7.1 The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the RB, in whatever media. This includes information held on computer systems, hand-held devices, phones, paper records, and information transmitted orally.

7.2 This policy applies to the Cohort, who should act on and interpret this policy in both the letter and the spirit of the applicable law.

7.3 The Cohort must be familiar with this Privacy Notice and comply with its terms.

7.4 The RB information covered by this policy includes Confidential information.

7.5 This policy has been drafted with care to ensure that it is clear and easy to understand.

7.6 We will review and update this policy regularly in accordance with our data protection and other obligations.

7.7 We may amend, update or supplement the policy at any time.

7.8 We will circulate any new or modified policy when it is adopted.

8 General principles of data protection

8.1 All RB information must be treated as commercially valuable and protected from loss, theft, misuse or inappropriate access or disclosure.

8.2 Personal data, and special category data, must be protected against unauthorised and/or unlawful processing and against accidental loss, destruction or damage, by the use of appropriate technical and organisational measures.

8.3 RB information (other than personal data) is owned by the RB and not by any individual or team.

8.4 RB information must be used only in connection with work being carried out for the RB and not for other commercial or personal purposes;

Personal data must be used only for the specified, explicit and legitimate purposes for which it is collected.

9 Information management

9.1 Personal data must be processed in accordance with:

(a) the data protection principles, set out in this data protection policy;

(b) this data protection policy generally; and

(c) all other relevant RB policies.

9.2 In addition, all information collected, used and stored by the RB must be:

(a) adequate, relevant and limited to what is necessary for the relevant purposes;

(b) kept accurate and up to date;

9.3 The RB will take appropriate technical and organisational measures to ensure that personal data is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage, including:

(a) pseudonymisation of personal data where necessary;

(b) encryption of personal data. e.g. for onward transmission by email;

Personal data and confidential information will be kept for no longer than is necessary and stored and destroyed in accordance with the RB's records retention policy.

10 Lawfulness of processing

10.1 There are 6 lawful bases for data processing.

10.2 In relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues, review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing.

10.3 The lawful bases for data processing are as follows:

(a) **Consent:** Where we process information with the specific consent of the individual concerned, whether for our services or for referral to our professional partners.

(b) **Contract:** 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.

(c) **Legal Obligation:** The processing is necessary for a compliance with a legal obligation to which the Controller is subject.

(d) **Vital Interests:** The processing is necessary in order to protect the vital interests of the data subject or of another natural person.

(e) **Public Task:** The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

(f) **Legitimate Interests:** The processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

10.4 Except where the processing is based on consent, we shall satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose); and

(a) document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

(b) include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);

(c) where 'special category data is processed, also identify a lawful special condition for processing that data and document it; and

(d) if criminal records data are processed, also identify a lawful condition for processing that data, and document it.

10.5 When determining whether the RB's legitimate interests are the most appropriate basis for lawful processing, we will:

(a) conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision;

(b) if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);

(c) keep the LIA under review, and repeat it if circumstances change; and

(d) include information about our legitimate interests in our relevant privacy notice(s).

Lawful Bases for Processing – Special Note

10.6 We must always have a lawful basis for processing Personal Data. However, certain post or office holders due to their type of office, appointment, rank and/or status within the Church, are not engaged under a traditional employment contract and an Employer/Employee relationship may not exist.

10.7 Nevertheless, in such cases the arrangements for their appointment to their role within the Church will be deemed to be a Contract for the purposes of determining the lawful basis for processing their Personal Data under the Data Protection Act and UK-GDPR.

10.8 A non-exhaustive list of such arrangements include:

(a) Stipendiary and Non Stipendiary Clerics

(b) Other Ministry licensed by a Bishop (e.g. LLMs)

(c) Voluntary service within the Church

(d) A range of other posts and offices

10.9 The authority for this action is pursuant to the Welsh Church Act 1914 and the constitution of the Church in Wales to facilitate the operational activity of the Church.

Special Category Data

10.10 Some Personal Data needs additional care and security this is Special Category data, sometimes referred to as ‘sensitive personal data’ or ‘sensitive personal information’.

10.11 Special Category Data means personal data about an individual’s race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic data, biometric data (where used to identify an individual) and data concerning an individual’s health, sex life or sexual orientation.

10.12 The RB may from time to time need to process special category data. We will only process special category data if:

10.12.1 we have a lawful basis for doing so as set out above; and

10.12.2 one of the special conditions for processing special category data applies:

(a) the data subject has given explicit consent;

(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the RB or the data subject;

(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

(d) processing relates to personal data which are manifestly made public by the data subject;

(e) the processing is necessary for the establishment, exercise or defence of legal claims; or

(f) for reasons of substantial public interest; or

(g) for the purposes of preventive or occupational medicine.

10.13 When we deal with Special Category data for the Cohort the lawful bases are those provided for in Article 9(2) of the UK GDPR which are assessed on a case-by-case basis.

11 Data Access Rights

11.1 Our **Data Protection Manager** can be contacted for the following data access reasons: -

(a) To obtain a copy of the Personal Data we hold about an individual.

(b) If someone believes any Personal Data or information we hold about them is incorrect or incomplete. Any information or data which is found to be incorrect will be corrected as soon as possible.

(c) To have an individual's personal data removed entirely from our systems.

(d) To make a request regarding Data Portability or any other rights under the data protection legislation.

(e) Data Access is usually free of charge. As soon as we are satisfied as to the identity of the person making the request, we will send them, within a month of the request a copy of the Personal Data we hold relating to them.

(f) As soon as we are satisfied as to the identity of the person making a removal request and the data is not required to be kept for any other lawful reason or purpose it will be removed from our systems forthwith.

(g) As soon as we are satisfied as to the identity of the person making a rectification request the data in question will be corrected or rectified as appropriate in our systems forthwith.

11.2 Data Subjects have rights of access to the data we hold about them. Requests to exercise these rights should be directed to our **Data Protection Manager**.

11.3 Further information about handling a DSAR is available in our Data Subject Access Request Policy in this document.

12 Individuals Data Rights

12.1 We protect the individual's rights provided by the UK GDPR and Data Protection Act 2018 as being the following:

(a) The right to be informed (Confirmation processing is taking place or not.)
(b) The right of access
(c) The right to rectification
(d) The right to erasure
(e) The right to restrict processing
(f) The right to data portability
(g) The right to object
(h) The right not to be subject to automated decision making, including profiling.

12.2 Under the UK General Data Protection Regulation (UK GDPR) and The Data Protection Act 2018 (DPA) Data Subjects have a number of rights with regard to their personal data.

12.3 These rights are protected by design and default in our data protection systems.

12.4 To exercise any of their rights Data Subjects should contact our **Data Protection Manager** using the details given above.

12.5 In our Online presence and Website we provide a method for contacting us and requesting Access to any data held by ourselves subject to the usual legal controls.

12.6 In the event Data Subjects provide their data directly to us for the purpose of a contract, or in circumstances where it is provided by consent, Data Subjects have the right to be provided with their data in a structured, machine-readable format.

12.7 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.

12.8 Where data has been provided by Consent there is a right to withdraw the Consent at any time. However, withdrawal of Consent does not affect the lawfulness of any processing of the data based on the Consent prior to its withdrawal.

12.9 Where we need to process data for the purposes of entering into a Contract with a Data Subject, failure to provide such data it may mean that we cannot establish legal relations between ourselves and the Data Subject and the contract may not be able to go ahead. We will inform the Data Subject if this happens.

12.10 Automated decision making and profiling means making decisions without human intervention, usually with the use of a computer program or software. 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.

12.11 We will retain and use Data Subjects personal information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements. If we need to use the data for a reason it was not collected and the Data Subject is not aware of this, we will inform them and in appropriate cases obtain further consent to such use.

12.12 Where we have not obtained the data personally from the Data Subject, we must provide them with the information described in this Privacy Notice and some additional information.

12.13 The additional information must be provided at least by the time we contact the Data Subjects and in any event within the space of one month after we obtain it.

12.14 If our processing is based on Legitimate Interests, the Data Subjects are entitled to know what and whose Legitimate Interests they are.

12.15 The Data Subjects are entitled to know the purpose of the processing, whether we or someone else is processing it and the categories of Personal Data involved.

12.16 The Data Subjects are entitled to know the source of the information and whether the source is publicly accessible.

12.17 There are some exceptions to this additional information rule. If we obtain Personal Data from a source other than the Data Subjects, the additional information rules will apply unless:-

(a) They already have the information regarding our processing; or

(b) It would take a disproportionate effort or be impossible to provide them with it; or

(c) They are already legally protected under separate provisions; or

(d) We have a legal duty not to disclose it.

12.18 Data Subjects have the right to complain to the Data Regulator at the Information Commissioners Office on 0303 123 1113 or through their website www.ico.org.uk

13 Data Protection Impact Assessments (DPIAs)

13.1 Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where the RB is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

(a) whether the processing is necessary and proportionate in relation to its purpose;

(b) the risks to individuals; and

(c) what measures can be put in place to address those risks and protect personal data.

13.2 Before any new form of technology is introduced, the **Data Protection Manager** will assess whether a DPIA should be carried out.

The RB General Privacy Notice 2024/25
Part Two of Four

Data Under Control
And
Data Security Policies

14 Personal Data under our control

MEMBERS OF THE GOVERNING BODY

14.1 Data under control analysis chart for **Members of the Governing Body**.

Personal Data	Lawful Base(s)	Retention Period	Source of Data Use of Data & Data Sharing
Your name; Your contact details (such as your postal address, telephone number and/or email address); Your Date of Birth; Your Bank Account Details; Your connection with the Church in Wales (which will reveal your religious beliefs).	**Public Task** Use of your Personal Data to provide you with relevant papers and documents and to share with other members of the Governing Body is to ensure the proper operation of the Church. **Special Category Data** If and to the Extent this reveals your religious beliefs, our processing of that Special Category data is carried out with your explicit consent, which is obtained during the application and appointment process of becoming a Governing Body Member. **Archiving** Keeping a record of your name and the dates you were a member of the Governing Body of the Church in Wales is necessary for historical research purposes and is in the public interest.	Your contact details will be retained for the duration of your membership of the Governing Body and Seven years thereafter. Your name and your period of office as a member of the Governing Body of the Church in Wales will be retained indefinitely for historical research purposes.	Your Personal Data is provided to us by the relevant Diocese. Personal Data is shared with our authorised staff and Data Processors. We will share your contact details with other members of the Governing Body to enable members to contact each other to discuss Church in Wales business. Names of Governing Body Members are listed on our Website. Names and periods of office will be shared with interested parties only for historical research purposes.

Consequences of not providing your data

14.1.1 If your name and contact details are not provided you will be unable to act as a member of the Governing Body as we will not be able to provide you with the information relevant to your role.

Circumstances in which we may send your Personal Data outside the UK

14.1.2 On occasion there may be an opportunity to visit other Churches overseas within the Anglican Communion. In such circumstances, we will need to send

some of your Personal Data to the overseas Church in order to arrange your visit.

14.1.3 We will only transfer your Personal Data in such circumstances where we have your explicit consent to do so.

CLERGY AND FORMER CLERGY

14.2 Data under control analysis chart for **Clergy and Former Clergy**.

Personal Data	Lawful Base(s)	Retention Period	Source of Data Use of Data & Data Sharing
Your name; Your contact details (such as your postal address, telephone number and/or email address); Your Date of Birth; Your National Insurance number and tax code Your bank details, payroll details and tax status information Your salary, honorarium, pension and benefits details Your Bank Account Details; Your Date of Ordination; Information relevant to the provision of a house for duty; Details of any disciplinary matter;	**Public Task** We will use your name and contact details to correspond with you in relation to Church in Wales relevant business; We will use your National Insurance number, tax code, bank details, payroll details and tax status information to pay you any salary or honorarium and for benefit and pension purposes; We will use your Personal Data to deal with any disciplinary and/or grievance issues which may arise relating to you or in respect of which you may be able to provide relevant information; We will use your Personal Data to assist the Bishop with making and managing your appointment; We will use your Personal Data to provide you with a house for duty and for administrative purposes in relation to such house; We will collect information about criminal convictions if it is appropriate given the nature of the role and	We will keep your Personal Data for as long as you are engaged by us and for a period of up to 70 years after your death. The reasons for keeping your personal data for this length of time include to comply with HMRC requirements and because some claims can be brought up to 6 years after your engagement ends. For these purposes you remain engaged by the us if you are a member of a Church in Wales pension scheme. DBS disclosure results will ordinarily be destroyed within six months of receipt. Your personal file will contain a pro-forma that will indicate the date of receipt of the DBS disclosure information and whether results were acceptable. 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	His Majesty's Revenue and Customs (HMRC) in connection with your pay and benefits Banks and other financial institutions in connection with your pay and benefits Pensions providers and administrators (and related third parties who provide administrative, actuarial and clerical support to those providers and administrators) for providing and administering your pension Payroll provider to enable us to pay you The results of DBS checks carried out on behalf of other parts of the Church in Wales will be shared with those parts of the Church in Wales. The Archbishops' Council (of the Church of England) so that details of the office/position that you hold can be included in the Crockford database and in the Crockford's Clerical Directory. Further biographical information and contact details will only be included with your consent. We will publish some Personal data of Clerics so

Health information; Any other information recorded on the Infonet; Your connection with the Church in Wales (which will reveal your religious beliefs); Information about criminal convictions.	where we are legally able to do so. **Legal Obligation** We carry out DBS checks on behalf of other parts of the Church in Wales, such as on behalf of the Bishops or Diocese. The information obtained will be used by us in conjunction with other parts of the Church in Wales to determine whether to engage you. 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. 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. DBS Checks are part of an automated decision making process pursuant to Article 22 UK GDPR. The information provided by the DBA service is used to assess suitability for employment or appointment to a post. **Special Category Data** If and to the	securely by our Safeguarding Team indefinitely. Information on your clergy personal file pertaining to your ministry is kept until 70 years after your death for your assistance, to comply with the Church's safeguarding requirements, and for historical purposes. Our policy in respect of Clergy personal files, including a retention schedule policy, is available separately on our website.	the public can contact them for pastoral support and to promote their Ministry. Such data will be published on the Church in Wales Website and will include: 1. Name and 2. Church in Wales Email Address. Other Personal Data such as Postal Address and Telephone number may be published after discussions with the individual Cleric.

	Extent our processing of your Personal Data reveals your religious beliefs, our processing of that Special Category data is carried out on the grounds that you have made this information public by virtue of your ordination. **Archiving** Keeping a record of your name and the dates you were a member of the Clergy in the Church in Wales is necessary for historical research purposes and is in the public interest.		

Consequences of not providing your data

14.2.1 Failure to provide personal contact details, tax details, bank details, pension and benefit details will prevent us from being able to engage with you for your Ordination or other religious matters, pay you and/or provide you with benefits.

14.2.2 If a Cleric has any Objections to the publication of their identity data on the Website, for personal safety or other reasons, they should notify the Head of IT so an assessment of their concerns can be made.

14.2.3 Each case will be assessed on its merits. Alterations may be made, especially where personal safety is involved but the general policy will be that a Cleric in Public Ministry for the Church should be contactable by the public

Circumstances in which we may send your Personal Data outside the UK

14.2.4 On occasion there may be an opportunity to visit other Churches overseas within the Anglican Communion. In such circumstances, we will need to send some of your Personal Data to the overseas Church in order to arrange your visit.

14.2.5 We will only transfer your Personal Data in such circumstances where we have your explicit consent to do so.

OFFICE HOLDERS AND POST HOLDERS

14.3 Data under control analysis chart for **Office Holders and Post Holders**.

Personal Data	Lawful Base(s)	Retention Period	Source of Data Use of Data & Data Sharing
Your name; Your contact details (such as your postal address, telephone number and/or email address); Your Bank Account details (if in a paid post); Your connection with the Church in Wales (which will reveal your religious beliefs);	**Public Task** Use of your Personal Data for administrative Purposes, to provide you with relevant papers and documents and to share with other members of various committees is part of the proper running of the Church in Wales. Listing your name on the provincial website as an office/post holder will be done pursuant to your role. **Special Category Data** If and to the extent processing your Personal data reveals your religious beliefs, our processing of that information will be carried out because you have manifestly made the information public in accepting the role within the Church in Wales. Where DBS Checks are conducted they are part of an automated decision making process pursuant to Article 22 UK GDPR. The information provided by the DBS service is used to assess suitability for appointment to a post. **Legal Obligation** 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	Your contact details will be retained for the duration of your office and for 7 years thereafter. Your name and your period of office will be retained indefinitely for historical research purposes. DBS disclosure results will ordinarily be destroyed within six months of receipt. 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.	Your personal data will be provided to us either by you directly or by the relevant Diocese and or Bishop. We will share your contact details with other members of the committee or body you are an office holder of to enable members to contact each other to discuss Church in Wales business. We will record your name and the fact that you were an Office/Post Holder of the Church in Wales and the dates of your period of office for historical research purposes. We will use your bank account details to pay you any expenses due; We will use your Personal Data to provide you with information relevant to your office, such as meeting papers and issues for discussion at committee meetings. 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. We carry out DBS checks on behalf of other parts of the Church in Wales, such as on behalf of the Bishops or Diocese. The information obtained will be used by us in conjunction with other parts of the Church in Wales to determine whether to engage you. Information about criminal convictions will be obtained from the Disclosure and Barring Service (“DBS”) if you

	unlawful acts, protecting the public against dishonesty, preventing fraud or suspicion of terrorism or money laundering. 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 **Archiving** Keeping a record of your name and the dates you held an office or post in the Church in Wales is necessary for historical research purposes and is in the public interest.		have agreed to undertake a DBS check through the Church in Wales.

Consequences of not providing your data

14.3.1 If your name and contact details are not provided you will be unable to be appointed as an office holder as we will not be able to provide you with information relevant to your office.

Circumstances in which we may send your Personal Data outside the UK

14.3.2 On occasion there may be an opportunity to visit other Churches overseas within the Anglican Communion. In such circumstances, we will need to send some of your Personal Data to the overseas Church in order to arrange your visit.

14.3.3 We will only transfer your Personal Data in such circumstances where we have your explicit consent to do so.

TENANTS OF OUR BUILDINGS AND ANY GUARANTORS

14.4 Data under control analysis chart for **Tenants of our buildings and any guarantors**.

Personal Data	Lawful Base(s)	Retention Period	Source of Data Use of Data & Data Sharing
Tenant and/or guarantor name; Tenant and/or guarantor contact details (such as postal address, telephone number and/or email address, together with alternative contact details for deposit scheme); Tenant and/or guarantor Bank Account Details; Information provided from referees/previous landlords of tenant; Information from credit reference agencies; Tenant and/or guarantor salary details;	**Contract** The use of the tenant's Personal Data to enter into a tenancy agreement; for correspondence in relation to the tenancy and associated matters; to collect payment and return any deposit paid will be necessary for the purposes of taking steps prior to entering into a contract with the tenant and for the performance of the contract between us. The use of the tenant's and/or guarantor's Personal Data to assess reliability and ability to pay the rent will be necessary for the purposes of taking steps prior to entering into a contract with the tenant and for the performance of the contract between us. Credit Checks are part of an automated decision making and profiling process pursuant to Article 22 UK GDPR. The information provided by the Credit Agency is used to assess the suitability of Tenants and /or their Guarantors ad to ensure as far as possible that they have the means to make rent payments. **Legal Obligation** We may be required to report details of our Tenants to HMRC or other statutory bodies.	Your Personal Data will be retained for the duration of the tenancy agreement and for 15 years thereafter due to the limitation period on property disputes.	Your personal data will be provided to us by the tenant and/or guarantor, or from the agent advertising the tenancy, arranging the tenancy or managing the tenancy, referees and credit reference agencies. We use this information to assess reliability as a tenant or guarantor and the ability to pay the rent; to enter into a tenancy agreement; to correspond with the tenant and/or guarantor in relation to the tenancy and associated matters; for tenancy administrative purposes; to obtain rent and deposit payment from tenant and/or guarantor and to return any deposit payment. We will share your name and address with: credit reference agency and with referees you notify us of in order to assess your ability to pay the rent and your reliability as a tenant or guarantor; our tenancy managing agents for property management and maintenance purposes; people and organisations we use to carry out repairs and maintenance.

Consequences of not providing your data

14.4.1 Failure to provide us with your Personal Data as requested will mean that we cannot enter into a tenancy agreement with the tenant.

DONORS

14.5 Data under control analysis chart for **Donors**

Personal Data	Lawful Base(s)	Retention Period	Source of Data Use of Data & Data Sharing
Your name; Your contact details (such as your postal address, telephone number and/or email address); Your Bank Account Details; Whether you are a UK taxpayer; Your connection with the Church in Wales (which may reveal your religious beliefs).	**Contract** Processing your data will be necessary for the purposes of entering into a contract and for the performance of the contract between us. **Legal Obligation** We will report details of donors to HMRC as necessary to obtain tax reimbursements. Donations allow the Church in Wales to further the interests of the Church in Wales and its aims. If and to the extent that your donation to the Church in Wales reveals your religious beliefs, our processing of that Special Category Personal Data is conducted with your explicit Consent.	Your Personal Data including your contact details will be retained for the duration of the giving and for Seven years thereafter.	Your Personal Data is provided either directly from the donor or from the relevant Diocese/Parish. We will use the Personal Data in order to process your donation (whether a one off or a regular donation) and to obtain any tax reimbursements through gift aid. We will share your name, amount of your donation and whether tax is reclaimed with the Parish treasurer for parish accounting and records purposes. We will share your Personal Data with HMRC in order to obtain any gift aid tax reimbursement, where applicable.

Consequences of not providing your data

14.5.1 Failure to provide us with your name address and bank account details will mean we cannot process any donation other than a cash or cheque donation.

INDIVIDUALS WHO CONTACT US WITH ENQUIRIES/COMPLAINTS

14.6 Data under control analysis chart for **Individuals who contact us with Enquiries/Complaints**

Personal Data	Lawful Base(s)	Retention Period	Source of Data Use of Data & Data Sharing
Your name; Your contact details (such as your telephone number or email address); Details of your enquiry; Your connection with the Church in Wales (which may reveal your religious beliefs), if relevant.	**Consent** Use of your Personal Data for the purpose dealing with your enquiry or complaint is based on your Consent. Keeping a record of your enquiry or complaint in order to deal with it, is based on your Consent. **Special Category Data** Where the details of your enquiry reveal your religious belief because of your connection with or contact with the Church in Wales, our processing of that Special Category Personal Data will be carried out with your explicit Consent. **Legal Obligation** Where the matter involves safeguarding issues or allegations relating (in the view of our Safeguarding Manager) to safeguarding of children and/or adults at risk, the complaint will be dealt with under the lawful basis of Legal Obligation. 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.	Records of your enquiry or complaint are retained until 12 months after the matter is resolved or your Consent is withdraw, which ever comes first. Where the matter involves safeguarding issues or allegations relating (in the view of our Safeguarding Manager) to safeguarding of children and/or adults at risk, a record of the complaint will be retained securely by our Safeguarding Team indefinitely.	Your Personal Data is provided by you when you contact us. (e.g. by making a phone call or emailing us). We will use the Personal Data to deal with your enquiry or complaint; We will make a record of your enquiry /complaint for internal admin purposes.

Consequences of not providing your data

14.6.1 Failure to provide us with your details will mean that we cannot contact you to deal with your enquiry.

14.6.2 In certain limited circumstances we may be able to deal with allegations of misconduct amounting to safeguarding issues anonymously.

INDIVIDUALS WHO UNDERTAKE TRAINING WITH US

14.7 Data under control analysis chart for **Individuals who undertake training with us**

Personal Data	Lawful Base(s)	Retention Period	Source of Data Use of Data & Data Sharing
Your name; Your contact details including, email address and (if a member of the Church in Wales) details of your parish/Diocese. For online training, we may collect technical information, including the internet protocol address used to connect your computer to the internet; the browser type and version; time zone settings; browser plug-in types and versions, operating system and platform; For online training, we may collect information about your visit, including the Uniform Resource Locators ("URL"); clickstream to, through and from our website (including date and time), page response times, download errors; length of visit to certain pages and methods used to browse away from the page. Your attendance record of courses (whether online or in person), dates of completion and marks of any assessments.	**Public Task** There is a duty upon Ordained clergy and LLMs to ensure they attend ongoing training throughout their Ministry, Personal Data in relation to these matters is processed as part of the proper running and organisation of the Church in Wales. **Contract** Where a Contract exists for the provision of training services, processing your data will be necessary for the purposes of entering into a contract and for the performance of the contract between us. **Legal Obligation** Our collection and use of your Personal Data is based on our legal obligation in holding a record of who within our organisation has been trained to what level and on what dates. **Special Category Data** Where the Personal Data processed reveal your religious belief because of your connection with or contact with the Church in Wales, our processing of that Special Category Personal Data will be carried out with your explicit Consent.	We keep records of all completed training for a period of six years from the date of completion. This is so that refresher or updated training can be offered to the appropriate persons at the appropriate time. Certain training information will be contained in Clergy files and retention periods are dealt with in our Clergy Files Policy available on our Website.	Some of the information is collected by us each time you use our website through our use of cookies. Further information about the cookies we use and the purposes for which we use them can be found in our Cookies Policy www.churchinwales.org.uk/cookies/ Some of the information is entered by you into our registration and sign-up forms or entered by us on your request (if asking to be registered on a course). The information you provide is used by us to arrange our training programme and to ensure that training delivery is to the highest possible standards. It is also used to maintain and accurate of record of who has been training, to what level, on what dates. Training courses may be arranged and booked by the relevant Diocese.

Consequences of not providing your data

14.7.1 If you disable our Cookies, you will be unable to use certain parts of/functions on our website.

14.7.2 If you do not provide us with the Personal Data requested in the training sign-up you will be unable to participate in our training resources, whether online or in person.

14.7.3 Some roles within the Church in Wales require completion of specified training, so not providing us with this information maybe you are unable to take up or continue in a particular role within the organisation.

INDIVIDUALS WHO FEATURE IN OUR NEWSLETTERS OR ARTICLES

14.8 Data under control analysis chart for **Individuals who feature in our newsletters or articles.**

Personal Data	Lawful Base(s)	Retention Period	Source of Data Use of Data & Data Sharing
Your name; Your geographical location; Your association with the Church in Wales, which is likely to reveal your religious beliefs; Any other personal details you provide to us as part of your story.	**Consent** Use of your Personal Data for the purpose of writing the newsletter or article is based on your Consent. **Special Category Data** Once the Newsletter is printed and disseminated it may indicate your Religious beliefs and affiliation to the Church. The legal ground for processing this Special Category Personal Data is that the information is manifestly made public by your original consent to publication. **Archiving** Newsletters are a valuable source of historical information and as such once published are retained indefinitely in the public interest for historical research purposes.	Unless you withdraw your consent prior to printing, articles and newsletters remain available on our website indefinitely, in the archived section for reference purposes and for disseminating information about the Church in Wales to the public.	Your Personal Data is provided by you when you agree to feature in a newsletter or article. We will use the Personal Data provided within the article or newsletter; the article or newsletter will be posted on our website and/or will be printed in our Highlights magazine or other in house publications.

Consequences of not providing your data

14.8.1 Failure to provide us with your details will mean that we cannot contact you to deal with your enquiry.

14.8.2 In certain limited circumstances we may be able to deal with allegations of misconduct amounting to safeguarding issues anonymously.

INDIVIDUALS WHO WE ENGAGE TO PROVIDE SERVICES TO US

14.9 Data under control analysis chart for **Individuals who we engage to provide services to us.**

Personal Data	Lawful Base(s)	Retention Period	Source of Data Use of Data & Data Sharing
Your name and contact details; Your bank account details.	**Contract** We will use your Personal Data to enter into an agreement for services with you; for correspondence in relation to the services and associated matters and to make payment for the service(s) provided. The Personal Data will be necessary for the purposes of taking steps prior to entering into a contract with you and for the performance of the contract between us. **Special Category Data** The contract between us may indicate your Religious beliefs and affiliation to the Church. The legal ground for processing this Special Category Personal Data is your explicit consent to entering contractual relations.	We will retain your Personal Data for the duration of the provision of services and for six years thereafter in case there should be any contractual dispute.	Your Personal Data is provided by you when you agree to provide us with services. We will use the Personal Data to enter into an agreement with you, to contact you, to administer the agreement for services and to pay you.

Consequences of not providing your data

14.9.1 Failure to provide us with your Personal Data will mean that we will not be able to engage you to provide us with services nor will we be able to pay you.

15 Engaging with us on Social Media

15.1 Any social media posts or comments you send to us (on the Church in Wales Facebook page, for instance) will be shared under the terms of the relevant social media platform (e.g. Facebook or Twitter) on which they're written and could be made public.

15.2 The Social Media Companies, not us, control these platforms. We are not responsible for this kind of sharing. So, before you make any remarks or observations about anything, you should review the terms and conditions and privacy policies of the social media platforms you use.

15.3 In that way, you'll understand how they will use your information, what information relating to you they will place in the public domain, and how you can stop them from doing so if you're unhappy about it.

16 Types and Categories of Personal Data

16.1 **Identity data:** name, username, title, date of birth. Contact data: billing and delivery address, email address, phone number.

16.2 **Financial data:** payment card details (processed by a third-party payment services provider and not stored by us).

16.3 **Transaction data:** details of products purchased, amounts, dates etc.

16.4 **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.

16.5 **Profile data:** username and password, purchases or orders made by users.

16.6 **Usage data:** information about how users use our website, products and services.

16.7 **Marketing and communications data:** record of Website users preferences in receiving marketing from us about the products we sell.

17 Sharing Your Personal Data with others

17.1 SERVICE PARTNERS

Information about our service partners	Our service partners are other businesses that we enter into contracts with. They include: Suppliers and sub-contractors; Suppliers of IT products and services; We haven't included the names of our service partners in this privacy notice because we will deal with different service providers from time to time. However, if you would like further information about any of our current service providers, please contact us on 029 2034 8200
Why we need to share your Personal Data	We use suppliers and sub-contractors to perform certain aspects of our contracts with our tenants. For example, providing maintenance services; We use suppliers of IT products and services in connection with the supply, maintenance and/or improvement of our IT network.
The legal grounds we rely upon	The sharing of your personal data with suppliers and sub-contractors is necessary for the performance of our **Contract** with them; The sharing of your personal data with businesses used by us in connection with the supply, maintenance and/or improvement of our IT network is based on **Contracts** we hold with the supplier and **Data Processing Agreements** which allow us to provide them with any of your Personal Data Under our control.

17.2 OTHER PARTS OF THE CHURCH IN WALES

Information about the different parts of the Church in Wales	Information about the structure of the Church in Wales can be found at www.churchinwales.org.uk .
Why we need to share your Personal Data	where it is necessary in the course of the work and activities of the Church in Wales, for example: sharing details of a complaint with the applicable Parish or Diocese; sharing details about donations received being shared with the applicable Parish or Diocese; sharing details of disciplinary issues relating to clergy with the applicable Bishop.
The legal grounds we rely upon	We will share Personal data with other parts of the Church in Wales when: We have a **legal Obligation** to do so. It is necessary for the performance of a **Contract** It is carried out in the course of the proper running and management of the Church in Wales under the lawful basis of **Public Task**. Where the other part of the Church in Wales is a legal entity in its own right and our data sharing with them is not based on the proper running of the Church under **Public Task** then we will share details with them based on their

	data protection compliance and our Data Controller/Processer agreements with them as applicable
What precautions do we take?	Personal data is only shared within the Church in Wales where this can be done fairly and lawfully, in accordance with the data protection principles and data protection laws. To this end the Church in Wales aims to ensure; that only personal data that needs to be shared in connection with the operations and activities of the Church is shared; that personal data is only shared when it is necessary and appropriate to do so; that personal data is shared on a 'need to know' basis and is not shared more widely than is necessary; and that personal data is shared securely.

17.3 OTHER THIRD PARTIES

Legal or regulatory requirements	On occasion, we may be required to disclose your Personal Data to organisations such as regulatory bodies, the courts and the police to comply with legal obligations we are subject to and/or to prevent fraud or crime. Also to other organisations such as the courts, the police, regulatory bodies, credit reference agencies and/or debt collection and tracing agents;
Protecting our interests	We may need to disclose your Personal Data in connection with steps we need to take to protect our interests or property. For example, if a tenant defaults with payment, we may disclose your Personal Data to credit reference agencies or debt collection or tracing agents. The lawful basis of this activity is that it is necessary for the performance of a contract and is an exception to the general rule against automatic decision making under Article 22(2)a of the UK GDPR
Professional advice and legal action	We may need to disclose your Personal Data to our professional advisers (for example, our lawyers and accountants) in connection with the provision by them of professional advice.
Use of Proprietary Software and Online Services. **Eg. Survey Monkey, Mailchimp or similar services.**	From time to time we may use proprietary software/Services for operational purposes to assist in future planning for Church activities. Such software may be used to gather opinions for the assessment of future proposals; to manage our response to developing technology; evaluate the viewpoint of individuals both within the Church and with the Public to various proposals related to Church matters. The software/service used may generate electronic surveys to be distributed to interested parties under the lawful basis of Public Task. This type of software/service will not be used as marketing activity on behalf of the RB. There is no commercial element to their use, so they do not activate the restrictions on marketing pursuant to the Privacy & Electronic Communications Regs 2003. The communications in these cases may be sent via email/post or text messaging. The retention of this data is likely to be relatively short lived. Generally, the data collected, once evaluated will be kept for no longer than 12 months.

Use of Legitimate Interests **When do we apply the Lawful basis of Legitimate Interest?**	We use the Lawful Base of Legitimate interest sparingly and only when no other basis exists for processing the Personal Data in question. There are two occasions which we have identified the use of Legitimate Interests to be necessary. The first is the use of CCTV camera equipment. The second is the use of Video Conferencing. We have conducted Legitimate Interest Assessments for each of the two activities and they showed that the processing was necessary and in the Legitimate Interests of the Church The Legitimate Interest Assessments are reproduced in full in this document. **CCTV:** To protect our premises. To protect the safety of our employees and visitors to the premises. To assist lawful authorities in the prevention and detection of crime. **Video Conferencing:** To facilitate efficient business video & telecommunications. To protect the safety of our employees and participants on the call from unnecessary real world travelling. To support the primary objectives of Representative body of the Church in Wales.

18 Monitoring of Computers and Remote/Home workers

18.1 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.

18.2 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.

18.3 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 which is reproduced below.

18.4 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.

18.5 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.

Computer Monitoring Policy

18.6 The RB uses a comprehensive Computer system and employs a dedicated Information Technology (IT) team to manage it.

18.7 Certain members of the Cohort may be provided with computer equipment for use on the RB's business both in the office and at home where applicable and approved.

18.8 Such members of Cohort are expected to care for the equipment provided and report any deficiencies, breakdowns or failures to the IT management team.

Statutory Basis for Monitoring Activity

18.9 The primary legislative source for data protection matters is the Data Protection Act 2018 which is supplemented by the retained UK General Data Protection Regulations.

18.10 Additionally, the Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018 and the Employer's duty of care to their Employees are applicable in certain circumstances.

18.11 The Church in Wales makes use of the lawful basis of Public Task in its day to day operational management of the Church pursuant to the Welsh Church Act 1914 and the Constitution of the Church in Wales.

Scope of the Policy

18.12 This policy covers monitoring of the RB's computer equipment.

18.13 The items monitored by the software employed by the RB include:

(a) Patterns of Online behaviour and usage, to identify threats.
(b) Emails, including content, destination and source.
(c) Website Access
(d) Timings of computer usage e.g. logging on/off.

18.14 The items which are NOT monitored by the software include:

(a) Recording of Telephone calls is not conducted.
(b) Recording of the Mitel telephone system is not conducted. However, the fact a call was made and between which parties is kept for 30 days.
(c) Recording of Microsoft Teams calls is not onducted except where the user chooses to record the session.

Monitoring

18.15 The IT team has the ability to monitor computer usage through dedicated software.

18.16 It is the policy of the RB that such monitoring will only be reactive in nature. That means monitoring will occur automatically by virtue of the software involved but the results will not be accessed unless there appears to be a reason to do so.

18.17 Such reasons may include allegations of poor work time keeping, lack of satisfactory task completion or a specific allegation of an offence to be investigated.

Management of Data

18.18 Monitoring an individuals computer will inevitably mean processing their personal data.

18.19 The RB has published detailed data protection policies which include policies regarding processing the personal data of employees, retention schedules and access management.

18.20 All computer monitoring requests will be directed to the Head of IT in the first instance who may consult with the Data Protection Officer and the Head of Legal as required.

Hardware Security and Passwords

18.21 Each employee is provided with a username and password during their new starter onboarding process.

18.22 The password will be required to be updated from time to time. This is achieved by automatic prompts from the computer system.

18.23 Passwords should be kept private to the individual and not shared with anyone else.

18.24 Employees must only use their own password.

19 Email Security Policy

19.1 In August 2023 the Information Commissioners Office (ICO) issued new guidance to organisations regarding email security, with particular reference to the sending of emails to multiple recipients.

19.2 The Representative Body of the Church in Wales (The RB) has a legal duty to keep the data under its control secure. [under S.66 DPA 2018 and Art.5(1)f and Art 32 UKGDPR].

19.3 The RB has issued this email security policy and updated the official staff training, to assist staff to understand the requirements of the legislation and prevent unnecessary data breaches.

Data Protection issues

19.4 Emails have the ability to send a large amount of information to multiple addressees at once. Consequently, there always exists the potential for error.

19.5 Sending an email to the wrong addressee, adding an addressee to a 'cc' list in error or sending an email using 'cc' when 'bcc' should have been applied all constitute a Data Breach.

19.6 Whether such a Data Breach should be reported to the Regulator (ICO) will depend on the circumstances of each case.

19.7 If in doubt about a particular situation staff should seek advice from the Data Protection Officer at dataprotection@churchinwales.org.uk

Regulatory advice

19.8 The ICO email security advice states:

(a) "Failure to use BCC correctly in emails is one of the top data breaches reported to us every year – and these breaches can cause real harm, especially where sensitive personal information is involved."

(b) "While BCC can be a useful function, it's not enough on its own to properly protect people's personal information"

Staff and Cohort Actions

19.9 Staff and members of the Cohort should remember:

19.9.1 The use of 'bcc' only protects the recipient's identity not the content of the email.

19.9.2 Emails are not inherently secure and can pass through various systems and servers before reaching their intended recipient.

19.9.3 Staff members should get into the habit of using 'bcc' instead of 'cc' whenever multiple recipients are added to an email.

19.9.4 Staff members **must** use 'bcc' whenever sensitive information, confidential information or Special Category Data is present in the email contents.

19.9.5 The email settings on your computer can be arranged to set an email delay, (usually 1 or 2 minutes) on the dispatch of your emails, so you have the opportunity to stop the sending if an error is discovered.

19.9.6 If you are sending an email to a large number of recipients, such as a Newsletter, consider using a bulk mail provider. E.g. Mailchimp.

19.9.7 Where an email content includes Special Category data or confidential information, consideration should be given to using other types of protection:

(a) For a small number of emails consider sending individual copies.

(b) If documents are attached to the email, encrypt the data or the document itself.

20 Data Storage, transfer and retention

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

Data Transfer

20.2 Personal Data under our control will only be transferred to a third party organisation 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.

20.3 Personal Data sent by email will be encrypted where possible, where it is not possible the email itself should be encrypted**.** Attachments to emails containing Personal Data will always be encrypted.

20.4 Personal data will not be transferred over a wireless network if a hardwired network is available.

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

20.6 Passwords if transferred by email will be sent over a different email system to that of the encrypted email. Where this is not possible another means will be considered E.g. Voice or SMS transfer.

20.7 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.

20.8 Transfer of hard copy documents containing Personal Data will be achieved through personal physical transfer or if using the Royal Mail system by Special Delivery only. We will not use Recorded Delivery/'Signed For' under any circumstances.

20.9 Personal Data contained on removable media must be encrypted and its transfer achieved through personal contact or if using Royal Mail by Special Delivery only.

20.10 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.

Data Storage

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

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

20.13 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.

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

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

20.16 We will retain the data of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

20.17 Details of retention periods for specific data is provided in the data under control analysis chart above.

20.18 Where we have a legal obligation to retain data outside of these periods they will be held securely and reviewed regularly until the obligation no longer exists.

21 International data transfers

21.1 There are stringent legal restrictions on international transfers of personal data and transfers to international organisations.

21.2 Staff may only transfer personal data outside the UK, or to an international organisation, with the prior written authorisation of the **Data Protection Manager**

21.3 We do not generally operate outside of the United Kingdom but we may maintain professional contacts in other countries.

21.4 All Data and information collected in any State will be processed in the UK.

21.5 Due to the operation of the Internet and other computer based applications Personal Data under our control may transit countries outside of the UK.

21.6 We will only transfer data outside the UK if adequate safeguards are in place in the destination country.

21.7 The Main Establishment for all of our Data Processing is the UK.

21.8 The lead supervisory authority is UK Law and the UK Information Commissioners Office whose address is Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

21.9 We have considered the requirements of Article 27 UK GDPR and decided that we do not need to appoint an EU Representative because

21.9.1 We are not a public authority; and

21.9.2 our international processing is only occasional, of low risk to the data protection rights of individuals; and

21.9.3 does not involve the large-scale use of special category or criminal offence data.

22 Children's Personal Data

22.1 We do not currently employ or engage anyone under the age of 18 years. If this situation changes we will update this policy as necessary.

22.2 Our Website is not directed at children.

22.3 We will not knowingly collect information from persons under 13 years of age without their parent's or guardian's consent.

22.4 We have considered the provisions of the Age Appropriate Design Code (AADC) and concluded we are not a relevant ISS likely to be accessed by children pursuant to Section 123 Data Protection Act 2018.

22.5 If a Parent or Guardian of a person under 13 years of age discovers their child has engaged with our Website without their consent, please inform us immediately using the contact email address provided above.

22.6 There is nothing on our Website which could be damaging to children who view the pages or the pictures.

23 Human Resources and Payroll

23.1 As a core activity within our business activity We process data for the purposes of our Human Resources function and Payroll function.

23.2 The lawful authority we rely on for processing this personal data is article 6(1)(b) of the UK GDPR, which relates to processing necessary to perform a contract or to take steps as requested, before entering a contract.

23.3 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.

23.4 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.

23.5 We recognise that staff are entitled to the same data access rights listed above and should follow the procedure laid out in the Subject Access Requests section of this policy document.

Recruitment

23.6 We use the information provided during the recruitment process to progress employment applications with a view to offering an employment contract.

23.7 We use contact details provided to contact applicants to progress their application and the other information provided to assess suitability for the role.

23.8 We do not collect more information than we need to fulfil our stated purposes and will not keep it longer than necessary.

23.9 If an individual is invited for interview we may ask for additional information such as personal referees and health information to establish fitness to work.

23.10 If we make a conditional offer of employment, we will ask for information so that we can carry out pre-employment checks. An individual must successfully complete pre-employment checks to progress to a final offer.

23.11 We must confirm the identity of our staff and their right to work in the United Kingdom and seek assurance as to their trustworthiness, integrity and reliability.

Payroll Matters

23.12 To manage our Payroll function we use information provided by employees to ensure accurate and timely payment of wages and emoluments.

23.13 The lawful authority for this function is our contractual relationship with employees and the legal obligation we have under HMRC and other legislation.

23.14 We collect no more information than is necessary to perform the function.

23.15 We may complete the Payroll function ourselves or contract with a Data Processor to perform the function on our behalf, in which case the information transmission between ourselves and the Data Processor will be subject to strict security measures, contractual terms and encrypted where necessary and appropriate.

24 Home Working Policy

Introduction

24.1 This policy covers processing of Personal data and the use of electronic devices which could be used to access the RB's systems and store information, alongside employees' own personal data. Such devices include, but are not limited to, smart phones, tablets, laptops and similar technologies.

24.2 The RB is the Data Controller of any Personal Data processed on its behalf and remains in control of the data regardless of the ownership of the device, or the location in which the data is processed.

24.3 All employees or approved contractors of the RB are required to keep any RB information and data securely and comply with Data Protection law.

24.4 All employees or approved contractors are required to assist and support the RB in carrying out its legal and operational obligations, including co-operating with the management team should it be necessary to access or inspect RB data stored on your personal device or equipment at your home.

24.5 The RB reserves the right to refuse, prevent or withdraw access or permissions for users to work from their homes and/or particular devices or software where it considers there are unacceptable security, or other risks, to its employees, business, reputation, systems or infrastructure.

Security and Confidentiality of Materials

24.6 All employees or approved contractors must follow The RB policies and procedures in relation to working with personal data as if they are present in the office.

24.7 There are also additional risks relating to working remotely. All employees or approved contractors must adhere to these instructions and follow both the spirit and the letter of this policy as this list of potential risks is not an exhaustive one.

24.8 The data protection principles still apply and need to be adhered to, i.e. you should only access as much personal data as you need for the task at hand.

24.9 You must consider "appropriate security", both at home and in transit. Additionally, you must be able to provide evidence you are complying with these principles on request.

24.10 Do not leave a computer with personal confidential information on screen. An unauthorised person reading personal data is a data breach.

24.11 Do not leave your computer 'logged on' when unattended. Think about who may access the device when you are not around – whether deliberately or accidentally.

24.12 Make sure rooms containing computers and other equipment, are secure when unattended, with windows closed and locked and blinds or curtains closed.

24.13 When making a business phone or online conference call remember that it is confidential and consider who is around who might overhear.

24.14 Levels of Home Security and access to Personal Data should be the same as at work.

24.15 Work should only be completed on RB approved systems and applications.

24.16 Do not hold Personal Data on personally owned electronic devices. (i.e. Devices not provided by the RB) unless approved in writing by the RB.

24.17 Any RB Personal Data downloaded to a personal device must be deleted as soon as possible.

24.18 If using a personally owned device, check for automatic uploads to Cloud storage systems. E.g. If subscribed to iCloud or Dropbox, you may inadvertently be uploading RB documents to your personal account in these applications. These uploads should be disabled whilst you are working.

24.19 Any paper files or documents taken from the office to work at home must be protected in transit and in your home. Ideally transported in a secure form such as a briefcase or encrypted memory stick and never left unattended in a vehicle.

24.20 Keep paperwork secure at home and out of sight of members of your family, visitors to the premises and others.

Loss or Theft

24.21 In the event that a device, whether personal or RB owned, is lost, stolen or its security is compromised, you MUST immediately, or if out of hours within an hour of the business reopening the next working day, report this to the **Data Protection Manager**, in order for them to assist in changing passwords to all RB services, considering the extent of the loss and reporting as a data breach if appropriate.

24.22 You must also cooperate with the management team in wiping the device remotely where possible and necessary, even if such a wipe results in the loss of your own data, such as photos, contacts etc.

24.23 The RB will not normally monitor the content of your personal devices. However, the RB reserves the right to monitor and log data traffic transferred between your device and RB systems, both over internal networks and via the Internet.

24.24 In exceptional circumstances, for instance where the RB requires access in order to comply with its legal obligations or requirements from a lawful authority such as the Information commissioner or the Police. The RB will require access to RB data and information stored on a personal device. Under these circumstances, all reasonable efforts are made to ensure that there is no access to an employee's private information.

Privacy Notice 2024/25

Part Three of Four

Data Protection Rights

And Responsibilities

Data Subject Access Requests

25 The RB holds personal data (or information) about job applicants, employees, clients, customers, suppliers, business contacts and other individuals for a variety of business purposes.

25.1 The individuals (known as 'data subjects') have a general right to find out whether we hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access, or the right to make a data subject access request. The purpose of the right is to enable the individual to be aware of, and verify, the lawfulness of the processing of personal data that we are undertaking.

25.2 The **Data Protection Manager** is responsible for ensuring:

25.2.1 that all data subject access requests are dealt with in accordance with UK GDPR and other relevant legislation and guidance; and

25.2.2 that all staff have an understanding of UK GDPR and other relevant legislation and guidance in relation to data subject access requests and their personal responsibilities in complying with the relevant aspects of UK GDPR and other relevant legislation and guidance.

25.3 This policy provides guidance on handling data subject access requests and is intended for internal use. It is not a privacy policy or statement, and is not to be made routinely available to third parties.

25.4 This policy provides guidance on:

25.4.1 what to do if you receive a data subject access request; and

25.4.2 how to decide whether a request for information is a data subject access request.

25.5 Failure to comply with the right of access under UK GDPR puts both staff and the RB at a potentially significant risk. The RB takes compliance with this policy very seriously.

25.6 We will review and update this policy annually in accordance with our data protection obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy to staff when it is adopted.

25.7 If you have any questions regarding this policy, please contact the **Data Protection Manager**.

How to recognise a data subject access request (DSAR)

25.8 A data subject access request is a request from an individual or from someone acting with their authority, e.g. a relative or solicitor for the information the individual is entitled to ask for under UK GDPR, namely:

25.8.1 for confirmation as to whether we process personal data about the individual and, if so:

25.8.2 for access to that personal data

25.8.3 and certain other supplementary information

25.9 Such a request will typically be made in writing but may be made orally (e.g. during a telephone conversation). The request may refer to 'UK GDPR', 'GDPR' and/or to 'data protection' and/or to 'personal data' **but does not need to do so** in order to be a valid request. For example, a letter which states 'please provide me with a copy of all the information that you have about me' will be a data subject access request and should be treated as such.

25.10 All data subject access requests should be immediately directed to the **Data Protection Manager** for immediate attention.

What to do when you receive a data subject access request

25.11 If you receive a data subject access request, you must immediately take the steps to alert the **Data Protection Manager**.

25.12 There are limited timescales within which we must respond to a request and any delay could result in our failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual.

25.13 The timescales referred to in this policy must be calculated from the day we receive a request (whether it is a working day or not) until the corresponding calendar date in the next month, for example if a request is received on 1 September, the information must be provided by 1 October.

25.14 If you are in any way unsure as to whether a request for information is a data subject access request, please contact the **Data Protection Manager**.

25.15 If you receive a data subject access request by email, you must immediately forward the request to the **Data Protection Manager**.

25.16 If you receive a data subject access request orally, you must:

(a) take the name and contact details of the individual;

(b) inform the individual orally that you will notify the **Data Protection Manager** that the individual has made an oral request and say the **Data Protection Manager** will contact them in relation to the request;

(c) immediately inform the **Data Protection Manager** and provide the individual's contact details and details of the oral request and the date on which it was received.

25.17 You will receive confirmation when the request has been received by the **Data Protection Manager**. If you do not receive such confirmation within **two** working days of sending it, you should contact the **Data Protection Manager** to confirm safe receipt.

25.18 You must not take any other action in relation to the data subject access request unless the **Data Protection Manager** has authorised you to do so in advance and in writing.

Advice for responding to a valid request by the Data Protection Manager.

25.19 Where we process a large quantity of information about an individual, we may need to ask the individual to specify the information or processing activities to which the request relates.

25.20 While it is not a requirement under UK GDPR that an individual must make a DSAR in writing, it is helpful for the RB if they do so. Individuals should therefore be encouraged to use the email address provided in this document.

25.21 We will not usually charge a fee for responding to a data subject access request. We may, however, charge a reasonable fee (based on the administrative cost of providing the information) for responding to a request:

(a) that is manifestly unfounded or excessive, e.g. repetitive; or

(b) for further copies of the same information.

Identifying the data subject

25.22 Before responding to a data subject access request, the **Data Protection Manager** will take reasonable steps to verify the identity of the person making the request.

25.23 We will not retain personal data, e.g. relating to former employees for the sole purpose of being able to react to potential data subject access requests in the future.

25.24 If we have doubts as to the identity of the person making the data subject access request, we may ask for additional information to confirm their identity.

25.25 Typically we will request a copy of the individual's driving licence or passport to enable us to establish their identity and signature (which should be compared to the signature on the data subject access request and any signature we already hold for the individual). We may also ask for a recent utility bill (or equivalent) to verify the individual's identity and address.

25.26 If, having requested additional information, we are still not in a position to identify the data subject, we may refuse to act on a data subject access request.

Refusing to respond to a request

25.27 We may refuse to act on a data subject access request where:

(a) even after requesting additional information, we are not in a position to identify the individual making the data subject access request;

(b) requests from an individual are manifestly unfounded or excessive, e.g. because of their repetitive character.

25.28 If we intend to refuse to act on a data subject access request, we will inform the individual, within one month of receiving the individual's request:

(a) of the reason(s) why we are not taking action; and

(b) that they have the right to complain to the ICO and seek a judicial remedy.

Time limit for responding to a request

25.29 Once a data subject access request is received, the RB must provide the information requested without delay and at the latest within one month of receiving the request.

25.30 Therefore a note of when request was received and when the time limit will end must be kept by the **Data Protection Manager** and recorded in the data protection register.

25.31 If a data subject access request is complex or the data subject has made numerous requests, the RB:

(a) may extend the period of compliance by a further two months; and

(b) must inform the individual of the extension within one month of the receipt of the request and explain why the extension is necessary.

Information to be provided in response to a request

25.32 The individual is entitled to receive access to the personal data we process about the individual and the following information:

(a) the purposes for which we process the data;

(b) the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations;

(c) where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;

(d) the fact that the individual has the right:

(i) to request that the RB rectifies, erases or restricts the processing of the individual's personal data; or

(ii) to object to its processing;

(iii) to lodge a complaint with the ICO;

(e) where the personal data has not been collected from the individual, any information available regarding the source of the data;

(f) any automated decision we have taken about the individual, together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual.

25.33 The information referred to above should be provided:

(a) in a way that is concise, transparent, easy to understand and easy to access;

(b) using clear and plain language, with any technical terms, abbreviations or codes explained;

(c) in writing;

(d) in a commonly-used electronic format, if the data subject access request was made electronically, unless otherwise requested by the individual.

Automated decision-making

25.34 If the data subject access request specifically asks for information about the logic behind any automated decision that we have taken in relation to important matters relating to the individual (e.g. performance at work, creditworthiness, reliability or conduct), we must provide a description of the logic involved in that automated decision, subject to the following conditions:

(a) the automated decision must have constituted the sole basis for the decision. For example, an application for credit which is conducted without any human intervention, other than to complete the application form, could be a decision which is taken solely by automatic means. However, if there is any element of human discretion as to whether or not to grant the credit, the decision would cease to be wholly automated and the individual would not be entitled to a description of the logic;

(b) in providing a description of the logic we are not required to reveal any information which constitutes a trade secret.

25.35 If the RB carries out automated decision-making in relation to an individual, the data subject access request may include a request:

(a) for information relating to the automated decision;

(b) for human intervention on the part of the RB, i.e. to ask that an individual with the authority and competence to change the decision should review the automated decision, considering all the available data;

(c) to express their point of view on the automated decision; and/or

(d) to contest the automated decision.

If such a request is received, the **Data Protection Manager** will ensure that it is dealt with in accordance with UK GDPR and other relevant legislation and guidance.

How to locate information

25.36 The personal data we need to provide in response to a data subject access request may be located in several electronic and manual filing systems or on those of data processors or other third parties. Consequently, it is important to identify at the outset the type of information requested so that the search can be focused.

25.37 Depending on the type of information requested, a search may be needed in all or some of the following media:

(a) electronic systems, e.g. databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV;

(b) manual filing systems in which personal data are accessible according to specific criteria, e.g. chronologically ordered sets of manual records containing personal data;

(c) data systems held externally by our data processors e.g. external payroll service providers;

(d) private devices used by employees and others;

(e) occupational health records;

(f) pensions data;

(g) share scheme information;

(h) insurance benefit information;

The above systems should be searched using the individual's name, employee number, customer account number or other personal identifier as a search determinant as applicable.

What is personal data?

25.38 Once you have carried out the search and gathered the results, you will need to select the information to be supplied in response to the data subject access request. The individual is only entitled to access to information which constitutes the individual's personal data.

25.39 Personal data is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, eg their name, identification number, location data or online identifier. It may also include personal data that has been pseudonymised (eg key-coded), depending on how difficult it is to attribute the pseudonym to a particular individual.

Requests made by third parties on behalf of the individual

25.40 Occasionally we may receive a request for data subject access by a third party (an 'agent') acting on behalf of an individual.

25.41 Such agents may include parents, guardians, legal representatives and those acting under a power of attorney or other legal authority. The agent must provide sufficient evidence that the agent is authorised to act on behalf of the individual.

Exemptions to the right of subject access

25.42 In certain circumstances we may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention:

25.43 We do not have to disclose any personal data which we are processing for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

25.44 This is not an absolute exemption. It only applies to the extent to which the giving of subject access would be likely to prejudice any of these purposes. We are still required to provide as much of the personal data as we able to. For example, if the disclosure of the personal data could alert the individual to the fact that they are being investigated for an illegal activity (ie by us or by the police) then we do not have to disclose the data since the disclosure would be likely to prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders.

Protection of rights of others:

25.45 We do not have to disclose personal data to the extent that doing so would involve disclosing information which identifies another individual, unless:

(a) that other individual has consented to the disclosure of the information to the individual making the request; or

(b) it is reasonable to disclose the information to the individual making the request without the other individual's consent, having regard to:

(i) the type of information that would be disclosed;

(ii) any duty of confidentiality owed to the other individual;

(iii) any steps taken by the controller with a view to seeking the consent of the other individual;

(iv) whether the other individual is capable of giving consent; and

(v) any express refusal of consent by the other individual.

Confidential references:

25.46 We do not have to disclose any confidential references that we have given to third parties for the purpose of actual or prospective:

(a) education, training or employment of the individual;

(b) appointment of the individual to any office; or

(c) provision by the individual of any service

NB: This exemption does not apply to confidential references that we receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (ie the person giving the reference), which means you must consider the rules regarding disclosure of third-party data before disclosing the reference.

Legal professional privilege:

25.47 We do not have to disclose any personal data which are subject to legal professional privilege. There are two types of legal professional privilege:

(a) 'legal advice privilege', which covers confidential communications between the RB and its professional legal advisers for the purpose of seeking or obtaining legal advice;

(b) 'litigation privilege', which covers confidential communications between the RB and its professional legal advisers or a third party where litigation is contemplated or in progress.

If you think the legal professional privilege exemption could apply to the personal data that have been requested, or are in any way uncertain as to whether it might apply, you should refer the matter to our legal advisers for further advice.

Corporate finance:

25.48 We do not have to disclose any personal data which we process for the purposes of, or in connection with, a corporate finance service if:

(a) disclosing the personal data would be likely to affect the price of an instrument; or

(b) disclosing the personal data would have a prejudicial effect on the orderly functioning of financial markets or the efficient allocation of capital within the economy and we believe that it could affect a person's decision:

(i) whether to deal in, subscribe for or issue an instrument;

(ii) whether to act in a way likely to have an effect on a business activity, eg on the industrial strategy of a person, the capital structure of an undertaking or the legal or beneficial ownership of a business or asset.

Management forecasting:

25.49 We do not have to disclose any personal data which we process for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity. Examples of management forecasting and planning activities include staff relocations, redundancies, succession planning, promotions and demotions.

(a) This exemption must be considered on a case-by-case basis and must only be applied to the extent to which disclosing the personal data would be likely to prejudice the conduct of that business or activity.

Negotiations:

25.50 We do not have to disclose any personal data consisting of records of our intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations. For example, if the HR department is negotiating with an employee in order to agree the terms of a redundancy package and the employee makes a data subject access request, the HR department can legitimately withhold giving access to information which would prejudice those redundancy negotiations.

(a) We must, however, disclose all other personal data relating to the individual unless those other personal data are also exempt from disclosure.

Deleting personal data in the normal course of business

25.51 The information that we are required to supply in response to a data subject access request must be supplied by reference to the data in question at the time the request was received.

25.52 However, as we have one month in which to respond and we are generally unlikely to respond on the same day as we receive the request, we are allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data are supplied if such amendment or deletion would have been made regardless of the receipt of the data subject access request.

25.53 We are, therefore, allowed to carry out regular housekeeping activities even if this means that we delete or amend personal data after the receipt of a data subject access request. What we are not allowed to do is amend or delete data because we do not want to supply the data.

Consequences of failing to comply with this policy

25.54 The RB takes compliance with this policy very seriously. If we fail to comply with a subject access request or fail to provide access to all the personal data requested or fail to respond within the one-month time period, we will be in breach of GDPR and other relevant legislation. This may have several consequences:

(a) it may put at risk the individual(s) whose personal information is being processed;

(b) the individual may complain to the ICO and this may lead the ICO to investigate the complaint. If we are found to be in breach, enforcement action could follow, which carries the risk of significant civil and criminal sanctions for the RB and, in some circumstances, for the individual responsible for the breach;

(c) if an individual has suffered damage, or damage and distress, as a result of our breach of UK GDPR or other relevant legislation, the individual may take us to court and claim damages from us; and

(d) a court may order us to comply with the subject access request if we are found not to have complied with our obligations under UK GDPR and other relevant legislation.

25.55 Any questions regarding this Policy should be addressed to the **Data Protection Manager**.

26 The RB Data Breach Policy

26.1 We accept the Information Commissioners Office definition of a data breach as follows:

26.2 "A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals."

26.3 We have determined a policy to comply with Data Breaches in the RB as follows:

26.4 A data breach may take many different forms, for example:

(a) loss or theft of data or equipment on which personal data is stored;

(b) unauthorised access to or use of personal data either by a member of staff or third party;

(c) loss of data resulting from an equipment or systems (including hardware and software) failure;

(d) human error, such as accidental deletion or alteration of data;

(e) unforeseen circumstances, such as a fire or flood;

(f) deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

(g) 'blagging' offences, where data is obtained by deceiving the organisation which holds it.

26.5 Details of the breach will be notified to or come to the notice of our **Data Protection Manager** who will begin an investigation into the breach to determine:-

(a) Its existence – has there in fact been a breach.

(b) Its extent – how much data has been breached.

(c) Its consequences – the consequences dictate the next actions as described below.

26.6 The **Data Protection Manager** will inform the ICO as soon as practicable and in any event within 72 hours if the breach is likely to result in a risk to the rights and freedoms of individuals or could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

26.7 In addition to the provisions above the **Data Protection Manager** is responsible for notifying each of the data subjects concerned directly, if a breach is likely to result in a high risk to the rights and freedoms of individuals.

26.8 If a minor data breach has occurred which does not require notification to the Regulator the **Data Protection Manager** will record the incident in Data Protection Register along with the justification for not reporting it.

26.9 All data breaches whether reportable or not will be recorded in our records to:

(a) Demonstrate our response to the incident.

(b) Comply with our record keeping responsibilities under UK GDPR.

(c) Maintain a satisfactory record of our actions for future reference.

Privacy Notice 2024/25

Part Four of Four

Policies Requiring Legitimate Interests Assessment

Policies requiring a Legitimate Interest Assessment

27 Marketing

27.1 We do not engage in Direct Marketing activity for the business.

27.2 We do not make use of Automated calling systems, Unsolicited live calls or Electronic Communications including Emails, Text messages, Telephone Calls, MMS or Faxes.

27.3 We may conduct Marketing activity through the use of non directed advertising in newspapers, periodicals, leaflets and similar.

27.4 We are familiar with the provisions of the Privacy & Electronic Communications Regulations (PECR).

27.5 The PECR Regulations apply to our Marketing effort in the respect of contacting prospective clients whose details have been passed to us by third parties.

27.6 We maintain our own 'do not call' list of people who may not be on any official list but have informed us they do not wish to receive marketing calls from ourselves.

28 Video Conferencing Policy

General

28.1 We use 3rd party proprietary video conferencing facilities within our business activity, which are able to record the conversations and presentations which occur during their use.

28.2 We understand that the participants of these conversations should be made aware that we are processing their Personal Data.

28.3 Where Video conferencing conversations are recorded and kept by us this data may be subject of a Data Subject Access Request. (DSAR)

28.4 We do not generally record and keep the conversations but when we do so the data and its security will be in dealt with in accordance with this Privacy policy.

28.5 A Legitimate Interests Assessment was conducted regarding video conferencing and is reproduced in this document.

28.6 This Policy has been established in accordance with the determinations of our Data Audit and the published guidance of the UK National Cyber Security Centre. (NCSC) on Video Conferencing and Cloud security.

28.7 We will only use the Video Conferencing Application Platforms (the Platform) which are from time to time approved by the Management.

28.8 The Security and Privacy settings on the Platform will be checked and adjusted to ensure the safety of participants to the call.

28.9 The choice of platform will be reviewed at least annually during the Privacy review or sooner if issues are reported to the **Data Protection Manager**.

Phishing

28.10 We are aware of the practice of Phishing during video conference calls. Phishing may be defined as follows: 'Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.'

28.11 Caution will be used when engaged in video conference calling especially in the use of any 'Live Chat' features to reduce the opportunities for Phishing.

28.12 Participants will not be allowed to share external links during the call without the express permission of the Moderator.

28.13 All Participants will be warned regarding the dangers of Phishing, clicking unknown links etc at the commencement of a call.

The Platform

28.14 The Video Conference Platform will be approved by the Management before use.

28.15 The latest software version must be checked for and downloaded prior to each use of the platform.

28.16 Consideration will be given to any 'paid for' version of the Platform if such a version exists and if it provides greater security and Privacy for the participants.

Passwords

28.17 Every use of the Platform will be controlled by the use of a Password to access any individual Video Conference call.

28.18 To reduce the risk of phishing and or deliberate interference or corruption of the process, when the call is either open to the public or has more than 5 separate participants, consideration will be given to using individual passwords for each participant.

Storage and Uploading of Video Conferencing

28.19 Video Conference recording facilities are available on most platforms.

28.20 We understand the image of a participant on a Video Conference call is Personal Data and can be subject to a Data Access request.

28.21 Where we intend to keep recordings of Video Conference calls this will be notified to participants at the start of the call to provide an opportunity for them to 'Opt out' by

closing their video link and remaining on the call using audio only or by leaving the call altogether.

Video Conferencing Applications – Legitimate Interest Assessment

28.22 We use 3rd party proprietary video conferencing facilities within our business activity, which are able to record the conversations and presentations which occur during their use.

28.23 We understand that the participants of these conversations should be made aware that we are processing their Personal Data.

28.24 Where Video conferencing conversations are recorded and kept by us this data may be subject of a Data Subject Access Request. (DSAR)

28.25 We do not generally record and keep the conversations but when we do so the data and its security will be in dealt with in accordance with this Privacy policy.

28.26 A Legitimate Interests Assessment was conducted by Us and is reproduced below:

28.27 In the course of our primary business activity we will gather Personal Data due to the use of Video Conferencing applications.

28.28 We wish to use Video Conferencing applications to facilitate efficient and speedy communications between interested parties engaged upon or connected to our business activity. These parties are often in disparate locations which makes direct communication without using technology virtually impossible.

28.29 We derive a substantial benefit in terms of a reduction in time spent travelling using a video conferencing platform.

28.30 The video conferencing platform is a 3rd party proprietary application which is publicly available and confirms to the prevailing Privacy regulations in and of itself.

28.31 Our use of the Platform will be within the manufacturer's suggested operating procedures.

(a) If we did not process the data by video conferencing the alternative would be to use traditional telecommunications which has fewer features and is not satisfactory in terms of content delivery when visual images are required.

(b) The software we use is compliant with the UK Government's National Cyber Security Centre (NCSC) guidelines for Video Conferencing.

(c) We maintain a high level of data privacy standards including Data Processing agreements where necessary with our primary business partners.

(d) We will not always record the video conference call but if we do, any Personal Data processed will not be of the kind to cause any ethical

issues and will be dealt with in line with our robust and fully operational UK GDPR privacy policies and systems.

28.28 Video Conferencing and the use of images both of the participants and with reference to non Personal Data information such as charts, graphs, photographs etc is the only way to achieve the purpose and transmit the information necessary for the successful completion of the agenda of the call.

28.29 The use of Video Conference calling is a proportionate methodology to fulfil our communication needs.

28.30 Mulltiple location communication is not possible without some form of technology and the transmission of information, especially graphical and photographic information is not possible using traditional telecommunications.

28.31 Receiving and processing Personal Data during Video Conference calling is a well established medium for the transference of data.

28.32 All participants on the call will have received notification that we will be processing their data.

28.33 All participants in the call will have opted in to the 3rd party application provider's Terms and Conditions.

28.34 All participants in the call will be adults.

28.35 Video conferencing is not an unusual method of processing and We do not expect anyone to object to the processing of their data in this way.

28.36 We recognise that any data we retain from the video conference can form the basis of a Subject Access Request which can be made to us under our Policy in this document should a data subject have any concerns.

28.37 The Legitimate Interest Assessment Test determined the following:

28.38 Following the assessment, it was decided that there was no infringement of the UK GDPR or the rights of the individual participants in our use of a Video Conferencing Application.

28.39 The legal basis for the processing was established as being in our Legitimate Interests for the following purposes:

28.40 To facilitate efficient business video and telecommunications.

28.41 To protect the safety of our employees and participants on the call from unnecessary real world travelling.

28.42 To support our primary business objectives.

29 CCTV

29.1 We use closed circuit television (CCTV) to provide a safe and secure environment for staff, visitors and customers, and to protect RB property. This policy relates to our use and management of CCTV at the premises used for the St Padarns Institute.

29.2 This policy sets out the accepted use of the CCTV equipment and images to ensure compliance with relevant data protection and privacy laws including: Retained Regulation (EU) 2016/679, the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) (together referred to as the 'Data Protection Legislation'), and related laws including but not limited to the Human Rights Act 1998 (all referred to collectively in this policy as the CCTV Laws).

29.3 This policy has been produced in line with the law and guidance provided by the Information Commissioner's Office.

Your responsibility to comply with this policy

29.4 Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred to the **Data Protection Manager.**

29.5 All staff must comply with this policy. We take compliance with this policy very seriously. Failure to comply with the policy puts at risk the individuals whose personal information is being processed, carries the risk of significant civil and criminal sanctions for the individual and for us, and may, in some circumstances, amount to a criminal offence by the individual.

29.6 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. Non-employees. such as contract staff and consultants may have their contract terminated with immediate effect.

Data transfer

29.7 We do not allow personal data collected by our CCTV equipment to be transferred to a person or entity without the prior written approval of the **Data Protection Manager**.

Why we use CCTV

29.8 CCTV systems are deployed at our premises for the following purposes and on the legal basis set of Legitimate Interests. We have installed CCTV systems to:

29.8.1 deter crime and assist in the prevention and detection of crime and/or serious breaches of policies and procedures;

29.8.2 assist with the identification, apprehension and prosecution of offenders; and

29.8.3 monitor security and health and safety at our premises.

29.9 We have carried out a legitimate interest assessment and consider that these purposes are legitimate, reasonable, appropriate and proportionate.

29.10 The CCTV system will NOT be used:

(a) In a manner likely to create any ethical issues such as public decency.

(b) for any automated decision making; or

(c) to monitor private areas of the premises.

29.11 Before installing and using CCTV systems on our premises, we have:

(a) assessed and documented the appropriateness of and reasons for using CCTV;

(b) established and documented who is responsible for day-to-day compliance with this policy; and

(c) ensured signage is displayed to inform individuals that CCTV is in operation.

29.12 We keep a record of the CCTV installed and used.

29.13 Once installed, reviews will be regularly undertaken to ensure that the use of the CCTV systems and the processing of the personal data obtained through it remains justified.

Covert recording and monitoring of staff

29.14 Covert monitoring means monitoring carried out in a manner calculated to ensure those subject to it are unaware that it is taking place.

29.15 We, do not undertake covert recording with our CCTV equipment.

Positioning cameras

29.16 We will make every effort to position cameras to ensure they only cover our premises.

29.17 Cameras will not be routinely monitored and the recordings will be used in a passive recording manner.

29.18 Cameras will not be hidden from view and must be sited in such a way as to ensure that they only monitor spaces intended to be covered.

29.19 The installation of cameras in areas in which individuals would have an expectation of privacy, e.g. showers and toilets, will not be authorised under this policy.

29.20 We will clearly display signs in the vicinity of the cameras so that staff, visitors and customers/clients are aware they are entering an area covered by CCTV.

29.21 The cameras do not focus only on one sector of employees or visitors and are used in the manner that would, objectively be expected.

29.22 The recordings are held digitally, password protected, accessible only by trained and approved staff members and kept for no longer than 3 months.

29.23 We do not expect anyone to object to the processing of their data in this way and we recognise that CCTV data can form the basis of a Subject Access Request which can be made to us under our Data Subject Access Request Policy, should a data subject have any concerns.

Image quality

29.24 Images produced by the equipment must be as clear as possible so that they are effective. To achieve this, we will ensure that:

(a) the equipment is properly installed, serviced, checked and maintained (and maintenance logs maintained) to ensure it works properly;

(b) any recording media, if needed, will be of good quality and will be replaced if the quality of the images has begun to deteriorate;

(c) where time/date of images are recordable, the equipment will be set accurately and this will be regularly checked and documented;

(d) cameras will be correctly positioned;

(e) assessments will be made as to whether constant real-time recording is necessary, or if recording can be limited to those times when suspect activity is likely to occur;

(f) cameras will be protected from vandalism so far as is possible; and

(g) if cameras break down or are damaged, the **Head of IT** is responsible for arranging timely repair.

Data and image retention

29.25 Images and recording logs must be retained and disposed of in accordance with the law. Images stored on removable media will similarly be erased or destroyed once the purpose of the recording is no longer relevant. Data will only be retained for legal and/or compliance reasons in accordance with the relevant retention and disposal of data policies.

29.26 For digital recording systems, CCTV images held on the hard drive of a PC or server will be overwritten on a recycling basis once the drive is full, and unless authorised by the **Data Protection Manager** will not be held for more than 90 days. If images are retained longer than this, the reason(s) will be recorded in the data protection register.

29.27 Where a request to retain information is authorised, reasonable steps will be taken to safeguard any footage which may otherwise be deleted.

29.28 All digital recordings will be password-protected and available only to authorised staff, to maintain security. Recording media no longer in use will be securely destroyed.

Access to images

29.29 Staff images

Staff images will only be accessed if a serious event occurs, such as criminal activity, fraud, gross misconduct, or behaviour that puts others at risk.

(a) Access to recorded images will be restricted to authorised staff only and will not be made more widely available.

(b) The request, date, time and the reason for authorisation for release of images and CCTV footage will have to be recorded by the **Data Protection Manager** for audit purposes in the data protection register.

(c) The following information must be kept on the data protection register maintained for that purpose and held by the **Data Protection Manager** when media are removed for viewing:

(i) the date and time they were removed;

(ii) the name of the person removing the media;

(iii) the name(s) of the person(s) viewing the images including the department to which the person viewing the images belongs or, if they are from an outside organisation, the organisation's name (eg the police);

(iv) the reason for viewing the images; and

(v) the date and time the media were returned to the system, destroyed or sent to secure storage, as applicable.

(d) Viewing of recorded images will take place in a restricted area to which other members of staff will not have access while viewing is occurring. Images retained for evidence will be securely stored with limited access for authorised staff only.

Access to and disclosure of images to third parties

Access to and disclosure of images recorded on CCTV will be restricted and carefully controlled. This will ensure that the rights of individuals are protected, and also ensure that the images can be used as evidence if required.

(e) Images may only be disclosed in accordance with the purposes for which they were originally collected. Our data protection policies should also be consulted in relation to the capture, storage, access to and disposal of personal data, in this case images of an identifiable individual.

(f) Disclosures to third parties will only be made in accordance with the purpose(s) for which the system is used and will be limited to:

(g) police and other law enforcement agencies, where the images recorded could assist in a specific criminal enquiry and/or the prevention of terrorism and disorder;

(h) prosecution agencies (such as the Crown Prosecution Service);

(i) relevant legal representatives of people whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings);

(j) individuals who have been caught on our CCTV in accordance with a data subject access request;

(k) in exceptional cases, for others (such as insurers) to assist in identification of a victim, witness or perpetrator in relation to a criminal incident; and

(l) staff involved with our disciplinary processes.

29.30 If a police officer requests images from our CCTV system in relation to an investigation that has not been initially reported by ourselves, then please refer them to the **Data Protection Manager**. It may be that we are required to disclose the images or we have a discretion whether to do so.

Disclosure of information

29.31 The **Data Protection Manager** is the only person who can authorise disclosure of information to the police or other law enforcement agencies. All requests for disclosure should be documented for audit purposes. If disclosure is denied, the reason should also be recorded.

29.32 Before any images are disclosed the following must be recorded in the data protection register:

(a) if the images are being removed from the CCTV system or secure storage to another area, the location to which they are being transferred;

(b) any crime incident number, if applicable; and

(c) the signature of the person to whom the images have been transferred.

Subject access rights to individuals' own data

29.33 The UK GDPR gives an individuals the right to access personal data about themselves, including CCTV images and footage. All requests for access to images by any individual (when they are asking for access to images of themselves) should be addressed to the **Data Protection Manager** in a written format, such as email or letter.

29.34 Please refer to our Data Subject Access Request Policy for further details.

29.35 Requests for access to CCTV images/footage must be made in writing and must include:

(a) the full name and address of the person making the request (the 'data subject');

(b) a description of the data subject and/or details of what they were wearing to ensure we can locate the individual, and only relevant images are disclosed;

(c) the approximate date and time when the images were recorded to allow for searching;

(d) the location where the images were recorded.

29.36 Requests from an individual for CCTV images or footage must be handled, and responded to, in accordance with our Data Subject Access Request Policy.

29.37 The **Data Protection Manager** will record and respond to such requests.

29.38 If we cannot comply with the request, the reasons for not being able to comply will be documented and the data subject will be advised of these in writing.

29.39 Particular care should be exercised when images of other people are included in the materials for disclosure. Images of other individuals will, if possible, be redacted unless there would be an expectation that their images would be released in such circumstances. Non-disclosure will be appropriate in most circumstances.

Requests to restrict processing and objections to processing

29.40 The UK GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data. The UK GDPR also gives individuals the right to object to the processing of their personal data in certain circumstances.

29.41 All such requests should be addressed in the first instance to the **Data Protection Manager**, who will provide a written response within one month of receiving the request, setting out their decision on the request. A copy of the request and response will be retained for an appropriate period determined on a case-by-case basis. Further information is given in the Data Subject Access Request Policy.

Complaints

29.42 Enquiries relating to the DPA 2018, UK GDPR or CCTV Laws should be addressed to the **Data Protection Manager** at the RB's contact details given at the start of this policy document.

29.43 If a member of staff believes that there has been a breach of the DPA 2018, UK GDPR or any CCTV Laws they must contact the **Data Protection Manager** as a matter of urgency**.**

29.44 If a complainant or enquirer is not satisfied with the response received, they can write to the Data Regulator, the ICO whose address is Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. More information can be found on the ICO website at www.ico.org.uk.

29.45 All Data Subjects have the right to complain about us to the Data Regulator at the Information Commissioners Office on 0303 123 1113 or through their website www.ico.org.uk.

29.46 A complete list of Data Subject's rights is provided in the section titled: Individuals Data Rights

CCTV – Legitimate Interest Assessment

29.47 We wish to use CCTV cameras in our business premises to passively record the activity therein.

29.48 Use of CCTV will enable photographic evidence of activity within the premises to be available should an incident occur.

29.49 Lawful authorities such as the Police and Health & Safety investigators would benefit from the recordings in the event of an incident.

29.50 The CCTV system will be operated in line with the industry guidelines set out in the CCTV code of practice promulgated by the ICO.

29.51 The CCTV cameras are clearly visible.

29.52 The operation of the CCTV cameras is Signposted.

29.53 The CCTV cameras will not be used in a way which could create any ethical issues such as public decency.

29.54 Video recording in the workplace is generally considered a useful and necessary activity.

29.55 Video recording in the workplace can only be achieved using a CCTV system.

29.56 Using a Digital CCTV system is a proportionate and unobtrusive response to the situation.

29.57 The CCTV cameras will only be used in operational areas of the business.

29.58 The cameras do not focus only on one sector of employees or visitors and are used in the manner that would, objectively be expected.

29.59 The CCTV data is not constantly monitored by personnel and is only used in a reactive manner should an incident occur.

29.60 The recordings are held digitally, password protected, accessible only by trained and approved staff members and kept for no longer than 3 months.

29.61 The use of the CCTV system does not impact the Data Subject or their rights and freedoms in a negative way.

29.62 We do not expect anyone to object to the processing of their data in this way and we recognise that CCTV data can form the basis of a Subject Access Request which can be made to us under our Policy in Section 9 of this document should a data subject have any concerns.

29.63 The legitimate Interest Assessment Test determined the following:

29.64 There was no infringement of the UK GDPR for the use of the CCTV equipment and the legal basis for their use was established as being in our Legitimate Interests for the following purposes:

29.65 To protect our business premises.

29.66 To protect the safety of our employees and visitors to the premises.

29.67 To assist lawful authorities in the prevention and detection of crime.

30 Management Gifting Policy

30.1 The Representative Body of the Church in Wales ("the RB") has established a data protection policy for the acceptable use of Staff Personal Data by Managers for sending gifts to individual staff members.

30.2 This policy is governed by the lawful basis of Legitimate Interests. A Legitimate Interest Assessment (LIA) was conducted and is reproduced below.

30.3 The LIA determined that in the event a staff member is not at work due to illness or for another reason such that their colleagues determine there is reason to consider sending the staff member a gift, such as a bunch of flowers or other small gift the procedure to adopt is as follows:

30.3.1 The staff member's line manager will be approached to approve the proposal.

30.3.2 The gift will be sanctioned based on suitability and price.

30.3.3 The price will not exceed £50 (fifty pounds)

30.3.4 The line manager will supervise the dispatch of the gift to the home address of the relevant staff member.

30.4 If the home address of the staff member is not known to their colleagues, their line manager will send a request for the address to the HR department by email.

30.5 The HR department are authorised to release the address (which is the staff members personal data) ONLY to their line manager by return of email, for the gifting purposes pursuant to the LIA in Appendix 1 below.

30.5.1 NB. This process will not be used to contact the staff member for any other purposes. Specifically, this process WILL NOT be used to discuss or encourage

any likely timings for the staff members return to work or any related matter of the RB's business , which may form part of the staff member's usual working duties.

30.6 The staff members line manager will ensure that once the gift has been dispatched the email containing the home address is deleted and the information is not retained in any other form.

Management gifting. Legitimate Interests Assessment –

Purpose Test

(a) The Representative Body of the Church in Wales (The RB) acting as Employer, wishes to describe a policy for Employees Personal Data to be processed to their line manager outside of the regular provisions and use of personal data related to their employment, when they are off work for sickness or other reasons, in order to provide them with a gift. E.g. a bunch of flowers or a card.

(b) The purpose of the gift is to cheer the Employees spirits and let them know they are being thought about in a positive way by their colleagues at work.

(c) In order to achieve this situation, it will be necessary to process a certain amount of the Employees personal data, usually their home address to their line manager to arrange the gift.

(d) The RB does not expect to derive any material benefit from the processing but considers that authorising the use of the Employees personal data in this way, is a proportional and pleasant use of the data under their control and one to which the Employee would not object.

(e) Since 2016 the HMRC has provided a statutory exemption on gifts of a trivial nature with a value under £50 including VAT. However, this exemption will not be activated, if the gift is not purchased by the RB but by the Employee's relevant manager (or departmental team) themselves.

(f) The Data Protection rules regarding the data to be processed are that the RB holds the personal data as Employer. The data were provided by the Employee during their onboarding activity for their employment and are required to be kept up to date. However, the use of the data in this context is not notified to the employee as part of their employment contract.

(g) It is the RB's general responsibility to protect the data under their control and it does so using various technical and organisational measures.

(h) The RB does not believe there are any ethical issues with the proposed processing.

Necessity Test

(i) Processing the personal data of employees to their line manager as described will achieve the proposed purpose.

(j) The personal data being processed will be kept to a minimum to ensure only the necessary data is released to the relevant line manager.

(k) The RB considers that the processing of the personal data as described is the most proportionate way to achieve the purpose.

(l) The data processed will be kept to a minimum. However, to send a parcel/gift to the employee requires access to their home address.

(m) Clear instructions will be given to line managers as to when they can access the personal data in question and such data will only be available by request to the HR department.

Balancing Test

(n) No Special Category data or criminal offence data will be processed. No children's data or that of vulnerable people will be processed.

(o) The personal data is not considered particularly 'private' information.

(p) All members of staff involved will be adults.

(q) It is not considered that the staff members right to privacy is being overridden by the use of their data in this manner.

(r) It is not considered that the staff members right to a family life (ECHR) is being overridden by the use of their data in this manner.

Reasonable expectations

(s) The RB considers that the use of the data in this manner falls under the reasonable expectations test. Staff may be pleasantly surprised but not disturbed by the use of their data in this manner.

(t) There is no other purpose in the processing than to provide a pleasant experience for the staff member who at the time may be unwell.

(u) Any staff member could ask for their data not to be shared in this way and such requests would be adhered to.

Likely Impact

(v) The RB does not believe that people are likely to object to the processing or find it intrusive.

(w) There is no loss of control over the data subject's personal data.

(x) The data is held securely in the RB's systems in the normal way and only released to a relevant line manager upon written request (email) to the HR department.

(y) The RB recognises the issues relating to contacting employees when ill or on leave and generally operates to a good standard of work/life balance.

(z) In these circumstances the line manager will not discuss an employees illness or include any statement or encouragement to return to work or any other business related matter.

(aa) Any communications sent with the gift will be restricted only to good will and get well messages.

Conclusions

(bb) The conclusions of this assessment will be reviewed regularly. The RB believes having taken advice and completed this assessment that the use of their Employee's personal data in the above described circumstances is both warranted and justified.

(cc) Any employee who is unhappy about receiving a gift can opt out of future instances of gift giving.

31 Dashcams

31.1 We do not make use of Dashcam equipment within our activities.

32 Review and Updating

32.1 We recognise the developing nature of Data Processing legislation and procedures.

32.2 We have established a regular system for review and updating as required.

32.3 Our **Data Protection Manager** is responsible for arranging reviews of our systems and staff training in line with our established training schedule.

32.4 We intend to create a robust system of Data Protection by design. We will conduct a Data/Information Audit on a regular basis as required by the regulations and record any updates to these policies.

32.5 A Data Audit will be conducted:

32.5.1 Regularly and in any event at least Annually.

32.5.2 When changes to procedures or processes warrant a Data Processing Impact Assessment (DPIA)

32.5.3 When any other relevant changes are required

32.5.4 The Data Protection staff training schedule is established as follows:

(a) Induction – On appointment or re-appointment.

(b) Ongoing - On a rolling basis of knowledge checks and reminders.

(c) Updating – As required consequent to changing and developing rules and procedures.

32.6 Our Data Processing contact has been authorised to make enquiries of our Legal advisors, if required, in the event of any queries beyond their existing understanding and knowledge.

Policy Currency

32.7 Policy Active from: 1 July 2024

Update required by: 31 July 2025