

Document Version 2.1

Data Audit: 1 May 2026

ICO REGISTRATION NO: Z 6056416

The Representative Body of the Church in Wales

General Privacy Notice

DATA PROTECTION MANAGEMENT SYSTEM

Compliance Handbook and Governance Framework

DATA PROTECTION ACT 2018

UK GENERAL DATA PROTECTION REGULATIONS (UK GDPR)

PRIVACY & ELECTRONIC COMMUNICATIONS REGULATIONS 2003

DATA (Use & Access) ACT 2025

Contents by Section

PART ONE – GOVERNANCE & OPERATIONAL POLICIES

- Intro. Governance Statement & Regulatory Compliance Mapping

- Section 1. Representative Body Contact Details
- Section 2. Status of key personnel
- Section 3. Overview
- Section 4. Purpose Statement
- Section 5. Definitions
- Section 6. Roles and Responsibilities
- Section 7. Scope of the Policy
- Section 8. General principles of Data Protection and Accountability
- Section 9. Information Management
- Section 10. Lawfulness of Processing
- Section 11. Individuals Data Rights
- Section 12. Data Access Rights
- Section 13. Data Protection Impact Assessments
- Section 14. Practical Data Protection Actions
- Section 15. International Transfers of Personal Data

PART TWO – DATA CONTROL POLICIES

- Section 16. Personal Data under our control
- Section 17. Engaging with us on Social Media
- Section 18. Types and Categories of Personal Data
- Section 19. Sharing your Personal data with others
- Section 20. Data Storage, Transfer and Retention
- Section 21. Website Cookie Policy
- Section 22. Automated Decision Making and profiling
- Section 23. Safeguarding and Children's Personal Data
- Section 24. Data Protection Complaints Policy

PART THREE – STAFF PROCEDURAL POLICIES

- Section 25. Human Resources and Payroll
- Section 26. Home Working Policy
- Section 27. Generative AI Policy
- Section 28. Internet, Email and Communications
- Section 29. Social Media Policy

PART FOUR – DATA RIGHTS & BREACH POLICIES

- Section 30. Data Subject Access Requests
- Section 31. Data Breach Policy

PART FIVE – LEGITIMATE INTEREST & UPDATES POLICIES

- Section 32. Recognised Legitimate Interests
 - Section 33. Marketing
 - Section 34. Video Conferencing
 - Section 35. CCTV
 - Section 36. Dashcams
 - Section 37. Management Gifting
 - Section 38. Review and Updating
-
- ANNEX A. Legitimate Interest Assessments and Register
 - ANNEX B. Provincial Safeguarding Team Privacy Notice

DATA PROTECTION MANAGEMENT SYSTEM

Compliance Handbook and Governance Framework

PART ONE of FIVE

GOVERNANCE & OPERATIONAL POLICIES

Introduction

Governance Statement

This Data Protection Compliance Handbook forms part of the Representative Body of the Church in Wales (“the RB”) formal data protection governance framework and records the policies, procedures and accountability measures implemented to ensure compliance with the UK General Data Protection Regulation, the Data Protection Act 2018, and associated legislation.

The RB’s management has approved this handbook and requires that its policies and procedures are implemented in practice, monitored on an ongoing basis, and reviewed regularly to ensure continued compliance with applicable data protection law and guidance issued by the Information Commissioner’s Office.

How to Use This Handbook

This handbook contains the RB’s data protection governance policies and procedures. It is intended to assist staff in understanding their responsibilities and to provide clear guidance on how personal data must be handled.

The document is divided into five parts:

- **Part One – Governance and Operational Policies**
Provides the overall framework for data protection within the RB.
- **Part Two – Data Control Policies**
Describes the types of personal data processed and how it is managed.
- **Part Three – Procedural Policies**
Provides operational guidance for staff, including home working, communications and AI usage.
- **Part Four – Data Rights and Breach Procedures**
Sets out how to respond to data subject requests and personal data breaches.
- **Part Five – Legitimate Interests and Monitoring Policies**
Describes specific processing activities relying on legitimate interests and the procedures used to review them.

If staff are unsure how to deal with a particular situation they should refer to the relevant section of this handbook or contact the Data Protection Manager.

Regulatory Compliance Mapping

This Data Protection Compliance Handbook has been structured to reflect the key obligations arising under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 and the Data (Use and Access) Act 2025.

The sections of this handbook collectively address the core requirements relating to:

- lawful processing of personal data
- accountability and governance
- data subject rights
- security of processing
- international data transfers
- breach reporting and complaint handling

This document therefore forms part of the RB's internal compliance framework and may be made available to regulators or auditors upon request.

Policy Hierarchy Statement - Relationship Between Policies

The policies contained within this handbook operate together as part of the RBs data protection governance framework.

- **Part One** establishes the governance structure and legal framework for the processing of personal data.
- **Part Two** identifies the categories of personal data processed by the RB and the lawful bases relied upon for that processing.
- **Part Three** provides operational policies designed to ensure that staff and contractors handle personal data securely and in accordance with the RB's obligations.
- **Part Four** sets out the procedures for responding to data subject rights and managing personal data breaches.
- **Part Five** provides specific policies relating to processing activities that rely on legitimate interests and explains how those interests are assessed and monitored.

NB: These policies should be read together and applied consistently across all business activities involving the processing of personal data.

1 The Representative Body of the Church in Wales - 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: 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 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 handbook forms part of the RB's data protection governance framework and outlines the policies, procedures and controls implemented to ensure compliance with applicable data protection legislation.

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.

3.5 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 in accordance with the following data processing principles:

- (a) Lawfulness, fairness and transparency
- (b) Purpose limitation
- (c) Data minimisation
- (d) Accuracy
- (e) Storage limitation
- (f) Integrity and confidentiality
- (g) Accountability

4 The purpose of this policy is to:

- 4.1 protect the confidentiality, integrity and availability of personal data held by the RB;
- 4.2 ensure that the RB's data assets, information systems and IT facilities used to process personal data are protected against unauthorised access, damage, loss or misuse;
- 4.3 support the RB's commitment to compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other applicable data protection legislation;
- 4.4 ensure that all staff understand their responsibilities when handling personal data and comply with the RB's procedures for the lawful and secure processing of personal data;
- 4.5 promote awareness within the RB of the importance of information security and the need to protect the confidentiality and integrity of the data handled in the course of business.

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.
- (l) RB Staff

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 Information security and data protection are the responsibility of all staff. All employees must ensure that personal data is handled securely and in accordance with this policy and applicable data protection legislation.

6.2 The RB's **Data Protection Manager** has particular responsibility for:

- (a) monitoring and implementing this policy;
- (b) monitoring potential and actual data protection or information security breaches and ensuring that appropriate action is taken;
- (c) ensuring that staff are aware of their data protection responsibilities through the provision of appropriate training and guidance;
- (d) promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other relevant legislation and regulatory guidance;
- (e) acting as the primary point of contact within the RB for data protection matters and liaising with regulators where necessary.
- (f) All staff must promptly report any suspected data protection breach, loss of personal data, or security incident to the Data Protection Manager.

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 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 Staff must follow the security arrangements and technical and organisational measures which are appropriate and in place for the type of information they access in the course of their work.
- 8.4 RB information (other than personal data) is owned by the RB and not by any individual or team.
- 8.5 RB information must be used only in connection with work being carried out for the RB and not for other commercial or personal purposes;

Accountability

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

- 8.7 The RB recognises its responsibility under Article 5(2) of the UK General Data Protection Regulation (UK GDPR) to demonstrate compliance with the data protection principles.
- 8.8 In order to meet this accountability obligation, the RB maintains appropriate policies, procedures and records relating to the processing of personal data.
- 8.9 These measures include, where appropriate:
- (a) maintaining records of processing activities in accordance with Article 30 UK GDPR;
 - (b) conducting data protection impact assessments where processing is likely to result in a high risk to individuals;
 - (c) maintaining records of data protection complaints and data protection incidents;
 - (d) implementing appropriate technical and organisational security measures; and
 - (e) providing training and guidance to staff on data protection responsibilities.
- 8.10 The Data Protection Manager is responsible for overseeing these accountability measures and ensuring that the RB is able to demonstrate compliance with applicable data protection legislation.

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;
- 9.4 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 The UK GDPR recognises 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 includes 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 Where we deal with Special Category Data for our employees, our subsidiary legal bases for employees are described in the Human Resources section of this document and the dedicated Staff and Human Resources privacy documentation.

10.14 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 Individuals Data Rights

11.1 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.

11.2 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.

- (a) These rights are protected by design and default in our data protection systems.
- (b) To exercise any of their rights Data Subjects should contact our **Data Protection Manager** using the details given above.
- (c) 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.

11.3 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.

11.4 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.

- 11.5 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.
- 11.6 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.
- 11.7 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.
- 11.8 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.
- 11.9 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.
- 11.10 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.
- 11.11 If our processing is based on Legitimate Interests, the Data Subjects are entitled to know what and whose Legitimate Interests they are.
- 11.12 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.
- 11.13 The Data Subjects are entitled to know the source of the information and whether the source is publicly accessible.
- 11.14 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.
- 11.15 Data Subjects have the right to complain to the Information Commissioners Office on 0303 123 1113 or through their website www.ico.org.uk

12 Data Access Rights

12.1 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.

12.2 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**.

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

13 Data Protection Impact Assessments (DPIAs)

13.1 This section establishes the RB's framework for identifying, assessing, and managing high-risk processing activities in accordance with Article 35 UK GDPR and associated ICO guidance.

13.2 A Data Protection Impact Assessment (DPIA) is a structured process designed to:

- a) identify risks to the rights and freedoms of individuals;
- b) assess the necessity and proportionality of processing; and
- c) define measures to mitigate identified risks.

When a DPIA is Required

- 13.3 A DPIA will be conducted where processing is likely to result in a **high risk** to individuals. A DPIA is mandatory where processing involves:
- a) Systematic and extensive evaluation or profiling of individuals
 - b) Automated decision-making with legal or similarly significant effects
 - c) Large-scale processing of special category data
 - d) Large-scale processing of criminal offence data
 - e) Systematic monitoring of publicly accessible areas (e.g. CCTV)
 - f) Processing involving vulnerable individuals (including children)
 - g) Use of new or emerging technologies
 - h) Matching or combining datasets from multiple sources
 - i) Processing which prevents individuals from exercising their rights or accessing services

Screening Requirement

- 13.4 All new processing activities, systems, or material changes to existing processing must undergo a **DPIA screening assessment** to determine whether a full DPIA is required.
- 13.5 The outcome of screening must be documented and recorded in the RB's DPIA Register.

Relationship with Other Accountability Measures

- 13.6 Each DPIA must be linked to:
- a) The relevant ROPA entry (Record of Processing Activities)
 - b) Any associated Legitimate Interest Assessment (LIA)
 - c) Any relevant Information asset or Data Audit Record
- 13.7 Where a DPIA identifies reliance on Legitimate Interests, the LIA must be reviewed alongside the DPIA

Risk Assessment Approach

- 13.8 Risks will be assessed using a **risk-based methodology**, considering:
- a) Likelihood of harm severity of impact;
 - b) nature of the data;
 - c) context of processing;
 - d) vulnerability of individuals.
- 13.9 Risks include, but are not limited to:
- a) identity theft or fraud
 - b) financial loss
 - c) discrimination
 - d) reputational damage
 - e) loss of confidentiality

- f) distress or psychological harm
- g) loss of control over personal data

Mitigation and Residual Risk

- 13.10 Appropriate **technical and organisational measures** must be identified to mitigate risks, including:
- a) data minimisation
 - b) access controls
 - c) encryption/pseudonymisation
 - d) retention controls
 - e) staff training
 - f) contractual safeguards

- 13.11 A **residual risk assessment** must be completed following mitigation.

Consultation Requirements

- 13.12 Where appropriate, consultation will be undertaken with:
- a) Managers and team leaders
 - b) The Data protection Manager
 - c) Affected individuals or their representatives

ICO Consultation

- 13.13 If a DPIA identifies a **high residual risk that cannot be mitigated**, the RB will consult the Information Commissioner's Office prior to commencing processing.

Approval and Sign-Off

- 13.14 The RB maintains a DPIA Register in structured spreadsheet format as part of its accountability framework
- 13.15 All DPIAs must be:
- (a) Reviewed by the Data protection manager
 - (b) Formally approved prior to the commencement of processing

14 Practical Data Protection Actions

- 14.1 Given the internal confidentiality of personnel files, access to such information is limited to the specifically authorised staff and management on a necessity basis. Except as provided in individual roles, other staff are not authorised to access that information.
- 14.2 All staff must keep personnel information strictly confidential.

- 14.3 Staff may ask to see their personnel files and any other personal data in accordance with the UK GDPR and other relevant legislation. For further information, see the RB's data subject access request policy.

Access to premises and information

- 14.4 Office doors, keys and access codes must be kept secure at all times and keys or access codes must not be given or disclosed to any third party at any time.
- 14.5 Documents containing confidential information and equipment displaying confidential information should be positioned in a way to avoid them being viewed by people passing by, e.g. through office windows or during video conference calls.
- 14.6 Visitors must be required to sign in at reception, accompanied at all times and never left alone in areas where they could have access to confidential information.
- 14.7 Wherever possible, visitors should be seen in meeting rooms. If it is necessary for a member of staff to meet with visitors in an office or other room which contains RB information, then steps should be taken to ensure that no confidential information is visible.
- 14.8 At the end of each day, or when desks are unoccupied, all paper documents, backup systems and devices containing confidential information must be securely locked away.

Computers and IT

- 14.9 Password protection and encryption must be used where available on RB computers and systems in order to maintain confidentiality.
- 14.10 Computers and other electronic devices must be password protected and those passwords must be changed on a regular basis. Passwords must not be written down or given to others.
- 14.11 Computers and other electronic devices must be locked when not in use and when you leave your desk, to minimise the risk of accidental loss or disclosure.
- 14.12 Confidential information must not be copied onto removable storage devices without the express permission of a manager.
- 14.13 Data held on any of these temporary devices should be transferred to the RB's computer(s) and/or network as soon as possible in order for it to be backed up and then deleted from the device.
- 14.14 All electronic data must be securely backed up in accordance with the RB approved back up schedule.
- 14.15 Staff must ensure they do not introduce malware or malicious code on to RB systems.

- 14.16 Software must not be installed or downloaded from the internet without it first being virus checked. Staff should contact their line manager for guidance on appropriate steps to be taken to ensure compliance.

Communications and transfer of information

- 14.17 Care must be taken about maintaining confidentiality when speaking in public places, e.g. when speaking on a mobile telephone.
- 14.18 Confidential information must be marked 'confidential' and circulated only to those who need to know the information in the course of their work for the RB.
- 14.19 Confidential information must not be removed from the RB's offices unless required for authorised business purposes.
- 14.20 Where confidential information is permitted to be removed from the RB's offices, all reasonable steps must be taken to ensure that the integrity of the information and confidentiality are maintained.
Staff must ensure that confidential information is:
- (a) stored on an encrypted device with strong password protection, which is encrypted at rest and kept locked when not in use;
 - (b) when in paper copy, not transported in see-through or other unsecured bags or cases;
 - (c) not read in public places (e.g. waiting rooms, cafes, trains); and
 - (d) not left unattended or in any place where it is at risk (e.g. in conference rooms, motor vehicles, public transport or cafes).

Email and cloud storage accounts

- 14.21 Postal and email addresses and numbers should be checked and verified before information is sent to them.
- 14.22 Particular care should be taken with email addresses and attention paid to avoid opportunities for auto-complete features to insert incorrect addresses.
- 14.23 All sensitive or particularly confidential information should be encrypted before being sent by email.
- 14.24 Further details regarding data security and how documents and emails should be protected are set out in the RB's data security, transfer, storage and retention policy.
- 14.25 Staff members must not use a personal email account or cloud storage account for work purposes.

Data Transfer to third parties

- 14.26 Third parties should be used to process RB information only in circumstances where appropriate written agreements are in place ensuring that those service providers offer appropriate confidentiality, information security and data protection undertakings. Consideration must be given to whether the third parties will be processors for the purposes of Article 28, UK GDPR.
- 14.27 Staff involved in setting up new arrangements with third parties or altering existing arrangements should consult the **Data Protection Manager** for advice and more information.

Data Protection Training

- 14.28 All staff will receive training in data protection. New joiners will receive training as part of the induction process. Further training will be provided annually or whenever there is a substantial change in the law or our policy and procedure.
- 14.29 The **Data Protection Manager** will continually monitor training needs but if you feel that you need further training on any aspect of the relevant law or our Information management and security policy or procedures, please contact the **Data Protection Manager**.

Reporting Data Subject Access Requests (DSARs)

- 14.30 All members of staff have an obligation to report actual or suspected Data Subject Access Requests (DSARs). This allows the RB to:
- (a) Respond to the request as required by law; and
 - (b) maintain a register of requests;
- 14.31 Please refer any suspected DSAR to the **Data Protection Manager** for immediate action.

Reporting data breaches

- 14.32 All members of staff have an obligation to report actual or potential data protection compliance failures. This allows the RB to:
- (a) investigate the failure and take remedial steps if necessary;
 - (b) maintain a register of compliance failures; and
 - (c) Where required, the RB will notify the Information Commissioner's Office within 72 hours any applicable notifications.
- 14.33 Refer any suspected data breach to the **Data Protection Manager** for immediate action.

15 International Transfers of Personal Data

Purpose

- 15.1 This policy sets out how We ensure that personal data transferred outside the United Kingdom is protected in accordance with the UK GDPR, the Data Protection Act 2018, and amendments introduced by the Data (Use and Access) Act (DUAA).
- 15.2 We recognise that transferring personal data internationally can present increased risks and is committed to ensuring that appropriate safeguards are in place.

Scope

- 15.3 This policy applies to all international transfers of personal data carried out by us, including transfers relating to:
- (a) The Cohort
 - (b) Employees, workers, contractors, and job applicants
 - (c) Data Processors and other external individuals
 - (d) Electronic and paper-based data
 - (e) Transfers to companies, service providers, and other third parties
- 15.4 A transfer includes making personal data accessible from outside the UK, even where data is hosted in the UK.

Legal Framework

- 15.5 All international transfers are recorded in the ROPA, including the safeguard relied upon and any transfer risk assessment.
- 15.6 Under UK data protection law, personal data may only be transferred outside the UK where one of the following applies:
- (a) The destination country or organisation is subject to a **UK adequacy regulation**; or
 - (b) Appropriate safeguards are in place;
 - (c) UK International data Transfer agreement (IDTA)
 - (d) Addendum to UK SCCs; or
 - (e) A limited statutory exception applies.
- 15.7 The Data Use and Access Act 2025 (DUAA) clarifies and updates the UK's approach to assessing adequacy and transfer risk, allowing a more proportionate, outcomes-based assessment of protections in the destination country.
- 15.8 The Main Establishment for all of our Data Processing is the UK.
- 15.9 The competent supervisory authority is the UK Information Commissioner's Office (ICO), whose address is Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

- 15.10 We have considered the requirements of Article 27 UK GDPR and decided that we do not need to appoint an EU Representative because
- (a) We are not a public authority; and
 - (b) our international processing is only occasional, of low risk to the data protection rights of individuals; and
 - (c) does not involve the large-scale use of special category or criminal offence data.

Transfers Based on UK Adequacy Regulations

- 15.11 We may transfer personal data to countries, territories, or international organisations that are subject to a **UK adequacy regulation**, as determined by the UK Government.
- 15.12 Where adequacy applies:
- (a) No additional transfer safeguards are required; and
 - (b) Transfers may proceed subject to compliance with all other UK GDPR principles.
- 15.13 We keep adequacy decisions under review and monitor for changes that may affect ongoing transfers.

Transfers Subject to Appropriate Safeguards

- 15.14 Where no UK adequacy regulation applies, We will only transfer personal data where **appropriate safeguards** are in place, such as:
- (a) The UK International Data Transfer Agreement (IDTA);
 - (b) The UK Addendum to the EU Standard Contractual Clauses; or
 - (c) Other safeguards recognised under UK data protection law.
- 15.15 Contracts incorporating these safeguards must be approved in accordance with internal governance procedures.

Transfer Risk Assessment

- 15.16 In line with the DUAA's revised approach, We will assess whether the safeguards in place provide **protection that is not materially lower than the standard of protection in the UK**.
- 15.17 This assessment will be:
- (a) Proportionate to the nature, volume, and sensitivity of the data;
 - (b) Focused on practical and foreseeable risks to individuals; and
 - (c) Documented as part of our accountability records.
- 15.18 Where risks are identified, We will implement additional technical, contractual, or organisational measures as appropriate.

Restricted and Exceptional Transfers

- 15.19 Where neither adequacy nor appropriate safeguards apply, We will only rely on a **statutory exception** (such as explicit consent or necessity for contract performance) where:
- (a) The conditions for the exception are clearly met;
 - (b) The transfer is occasional and limited; and
 - (c) The risks to individuals have been assessed and documented.
- 15.20 Statutory exceptions are not used for routine or large-scale transfers.

Security and Data Minimisation

- 15.21 For all international transfers, We ensure that:
- (a) Only the minimum personal data necessary is transferred;
 - (b) Appropriate technical and organisational security measures are in place; and
 - (c) Access to personal data is restricted to authorised recipients.

Transparency

- 15.22 Where required, individuals will be informed about international transfers of their personal data through our privacy notices, including:
- (a) The destination country or region; and
 - (b) The safeguards relied upon.

Responsibilities

- 15.23 Staff may only transfer personal data outside the UK, or to an international organisation, with the prior written authorisation of the **Data Protection Manager**
- 15.24 We do not generally operate outside of the United Kingdom but we may maintain professional contacts in other countries.
- 15.25 All Data and information collected in any State will be processed in the UK.
- 15.26 Due to the operation of the Internet and other computer based applications Personal Data under our control may transit countries outside of the UK.
- 15.27 All staff involved in procuring services or sharing personal data internationally must ensure compliance with this policy.
- 15.28 Our **Data Protection Manager** is responsible for approving international transfer mechanisms and maintaining related records.

Record Keeping and Accountability

- 15.29 Pursuant to Article 30 UK-GDPR a Record of Processing Activity (ROPA) is maintained as an internal record of:

- (a) International data transfers;
- (b) Transfer mechanisms and safeguards relied upon;
- (c) Transfer risk assessments conducted; and
- (d) Any supplementary measures implemented.

15.30 The RB maintains its Article 30 Record of Processing Activities in structured spreadsheet format, which is the authoritative and version-controlled record

15.31 These records form part of our UK GDPR accountability obligations.

Review

15.32 This policy will be reviewed periodically and updated to reflect:

- (a) Changes in legislation or UK adequacy regulations;
- (b) Guidance issued by the Information Commissioner's Office (ICO); or
- (c) Changes to our processing activities.

DATA PROTECTION MANAGEMENT SYSTEM

Compliance Handbook and Governance Framework

PART TWO of FIVE

DATA CONTROL POLICIES

16 Personal Data under our control

16.1 Each data processing activity described in this section is recorded in the RB's ROPA and assigned a unique reference.

MEMBERS OF THE GOVERNING BODY – ROPA REF – RB06

16.2 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
<p>Your name;</p> <p>Your contact details (such as your postal address, telephone number and/or email address);</p> <p>Your Date of Birth;</p> <p>Your Bank Account Details;</p> <p>Your connection with the Church in Wales (which will reveal your religious beliefs).</p>	<p>Public Task</p> <p>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.</p> <p>Special Category Data</p> <p>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.</p> <p>Archiving</p> <p>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.</p>	<p>Your contact details will be retained for the duration of your membership of the Governing Body and Seven years thereafter.</p> <p>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.</p>	<p>Your Personal Data is provided to us by the relevant Diocese.</p> <p>Personal Data is shared with our authorised staff and Data Processors.</p> <p>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.</p> <p>Names of Governing Body Members are listed on our Website.</p> <p>Names and periods of office will be shared with interested parties only for historical research purposes.</p>

Consequences of not providing your data

- (a) 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

- (b) 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.
- (c) We will only transfer your Personal Data in such circumstances where we have your explicit consent to do so.

CLERGY AND FORMER CLERGY– ROPA REF – RB07

16.3 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
<p>Your name;</p> <p>Your contact details (such as your postal address, telephone number and/or email address);</p> <p>Your Date of Birth;</p> <p>Your National Insurance number and tax code</p> <p>Your bank details, payroll details and tax status information</p> <p>Your salary, honorarium, pension and benefits details</p> <p>Your Bank Account Details;</p> <p>Your Date of Ordination;</p> <p>Information relevant to the provision of a house for duty;</p> <p>Details of any disciplinary matter;</p> <p>Health information;</p>	<p>Public Task</p> <p>We will use your name and contact details to correspond with you in relation to Church in Wales relevant business;</p> <p>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;</p> <p>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;</p> <p>We will use your Personal Data to assist the Bishop with making and managing your appointment;</p> <p>We will use your Personal Data to provide you with a house for duty and for administrative purposes in relation to such house;</p> <p>We will collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.</p>	<p>We 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.</p> <p>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.</p> <p>For these purposes you remain engaged by the us if you are a member of a Church in Wales pension scheme.</p> <p>DBS disclosure results will ordinarily be destroyed within six months of receipt.</p> <p>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.</p> <p>In the event that the disclosure result highlights concerns relating (in the view of our Safeguarding Manager) to safeguarding of children and/or adults at risk, a record of the disclosure results will be retained securely by our Safeguarding Team indefinitely.</p>	<p>His Majesty's Revenue and Customs (HMRC) in connection with your pay and benefits</p> <p>Banks and other financial institutions in connection with your pay and benefits</p> <p>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</p> <p>Payroll provider to enable us to pay you</p> <p>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.</p> <p>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.</p> <p>Further biographical information and contact details will only be included with your consent.</p> <p>We will publish some Personal data of Clerics so the public can contact them for pastoral support and to promote their Ministry.</p>

<p>Any other information recorded on the Infonet;</p> <p>Your connection with the Church in Wales (which will reveal your religious beliefs);</p> <p>Information about criminal convictions.</p>	<p style="text-align: center;">Legal Obligation</p> <p>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.</p> <p>This is because the Church in Wales has a Legal Obligation to take all reasonable precautions to ensure that the Church is a safe place for all.</p> <p>We will only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary for reasons of substantial public interest, namely, safeguarding, preventing or detecting unlawful acts, protecting the public against dishonesty, preventing fraud or suspicion of terrorism or money laundering.</p> <p>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.</p> <p style="text-align: center;">Special Category Data</p> <p>If and to the</p>	<p>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.</p> <p>Our policy in respect of Clergy personal files, including a retention schedule policy, is available separately on our website.</p>	<p>Such data will be published on the Church in Wales Website and will include:</p> <ol style="list-style-type: none"> 1. Name and 2. Church in Wales Email Address. <p>Other Personal Data such as Postal Address and Telephone number may be published after discussions with the individual Cleric.</p>
--	---	--	--

	<p>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.</p> <p style="text-align: center;">Archiving</p> <p>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.</p>		
--	---	--	--

Consequences of not providing your data

- (a) 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.
- (b) 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.
- (c) 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

- (d) 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.
- (e) We will only transfer your Personal Data in such circumstances where we have your explicit consent to do so.

Circumstances in which we receive your Personal Data from outside of the UK

- (f) We may receive information about Clerics and ex-Clerics from the various provinces of the Anglican Communion globally.

- (g) We will retain such Personal Data in our files for the purposes of identifying the Cleric and corroborating any information provided to us during any future application for Permission to Officiate or other post or office within the Church in Wales.
- (h) Such information will be retained in accordance with our Clergy Files policy regarding retention of Personal Data as laid out above.

OFFICE HOLDERS AND POST HOLDERS– ROPA REF – RB08

16.4 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
<p>Your name;</p> <p>Your contact details (such as your postal address, telephone number and/or email address);</p> <p>Your Bank Account details (if in a paid post);</p> <p>Your connection with the Church in Wales (which will reveal your religious beliefs);</p>	<p>Public Task</p> <p>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.</p> <p>Listing your name on the provincial website as an office/post holder will be done pursuant to your role.</p> <p>Special Category Data</p> <p>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.</p> <p>Where DBS Checks are conducted they are part of an automated decision making process pursuant to Article 22 UK GDPR.</p> <p>The information provided by the DBS service is used to assess suitability for appointment to a post.</p> <p>Legal Obligation</p> <p>We will only use information relating to</p>	<p>Your contact details will be retained for the duration of your office and for 7 years thereafter.</p> <p>Your name and your period of office will be retained indefinitely for historical research purposes.</p> <p>DBS disclosure results will ordinarily be destroyed within six months of receipt.</p> <p>In the event that the disclosure result highlights concerns relating (in the view of our Safeguarding Manager) to safeguarding of children and/or adults at risk, a record of the disclosure results will be retained securely by our Safeguarding Team indefinitely.</p>	<p>Your personal data will be provided to us either by you directly or by the relevant Diocese and or Bishop.</p> <p>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.</p> <p>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.</p> <p>We will use your bank account details to pay you any expenses due;</p> <p>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.</p> <p>We will collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.</p> <p>We carry out DBS checks on behalf of other parts of the Church in Wales, such as on behalf of the Bishops or Diocese.</p> <p>The information obtained will be used by us in conjunction</p>

	<p>criminal convictions where the law allows us to do so. This will usually be where such processing is necessary for reasons of substantial public interest, namely, safeguarding, preventing or detecting unlawful acts, protecting the public against dishonesty, preventing fraud or suspicion of terrorism or money laundering.</p> <p>This is because the Church in Wales has a Legal Obligation to take all reasonable precautions to ensure that the Church is a safe place for all</p> <p style="text-align: center;">Archiving</p> <p>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.</p>		<p>with other parts of the Church in Wales to determine whether to engage you.</p> <p>Information about criminal convictions will be obtained from the Disclosure and Barring Service ("DBS") if you have agreed to undertake a DBS check through the Church in Wales.</p>
--	---	--	--

Consequences of not providing your data

- (a) 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

- (b) 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.
- (c) 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 – ROPA REF – RB09

16.5 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
<p>Tenant and/or guarantor name;</p> <p>Tenant and/or guarantor contact details (such as postal address, telephone number and/or email address, together with alternative contact details for deposit scheme);</p> <p>Tenant and/or guarantor Bank Account Details;</p> <p>Information provided from referees/previous landlords of tenant;</p> <p>Information from credit reference agencies;</p> <p>Tenant and/or guarantor salary details;</p>	<p>Contract</p> <p>The use of the tenant's Personal Data to enter into a tenancy agreement;</p> <p>for correspondence in relation to the tenancy and associated matters;</p> <p>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.</p> <p>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.</p> <p>Credit Checks are part of an automated decision making and profiling process pursuant to Article 22 UK GDPR.</p> <p>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.</p> <p>Legal Obligation</p> <p>We may be required to report details of our Tenants to HMRC or other statutory bodies.</p>	<p>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.</p>	<p>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.</p> <p>We use this information to assess reliability as a tenant or guarantor and the ability to pay the rent;</p> <p>to enter into a tenancy agreement;</p> <p>to correspond with the tenant and/or guarantor in relation to the tenancy and associated matters;</p> <p>for tenancy administrative purposes;</p> <p>to obtain rent and deposit payment from tenant and/or guarantor and to return any deposit payment.</p> <p>We will share your name and address with:</p> <p>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;</p> <p>our tenancy managing agents for property management and maintenance purposes;</p> <p>people and organisations we use to carry out repairs and maintenance.</p>

Consequences of not providing your data

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

DONORS– ROPA REF – RB10

16.6 Data under control analysis chart for Donors

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

Consequences of not providing your data

- (a) 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.

PURCHASERS OF OUR BUILDINGS– ROPA REF – RB11

16.7 Data under control analysis chart for **Purchasers of our buildings.**

Personal Data	Lawful Base(s)	Retention Period	Source of Data Use of Data & Data Sharing
<p>Purchasers name;</p> <p>contact details (such as postal address, telephone number and/or email address);</p> <p>Bank Account Details;</p>	<p>Contract</p> <p>The use of the purchaser's Personal Data to enter into an agreement;</p> <p>for correspondence in relation to the property sale and associated matters;</p> <p>to collect payment and any deposit including all matters which will be necessary for the purposes of taking steps prior to entering into a contract with the purchaser and for the performance of the contract between us.</p> <p>Legal Obligation</p> <p>We may be required to report details of the transaction to HMRC or other statutory bodies.</p> <p>Public Task</p> <p>Disposal of Church owned building is part of the day to day management of the Church in Wales which is authorised under the Welsh Church Act and the Constitution.</p> <p>Sharing your data with relevant bodies such as utility companies local councils and others falls under this lawful basis.</p>	<p>Your Personal Data will be retained for the duration of the sale process and for 15 years thereafter due to the limitation period on property disputes.</p>	<p>Your personal data will be provided to us by yourselves or your agent or other professional advisers.</p> <p>We use this information to correspond with you, your agent or your professional advisers in relation to the sale and associated matters for administrative purposes; in relation to the sale.</p> <p>We may share your Personal Data with some or any of the following where applicable and relevant:</p> <p>Our professional advisers</p> <p>In house property team</p> <p>Utility Companies</p> <p>Councils or other public bodies.</p> <p>Statutory bodies</p> <p>HMRC</p>

Consequences of not providing your data

- (a) Failure to provide us with your Personal Data as requested will mean that we cannot enter into an agreement with you to purchase any of our properties.

INDIVIDUALS WHO CONTACT US WITH ENQUIRIES/COMPLAINTS– ROPA REF – RB12

16.8 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
<p>Your name;</p> <p>Your contact details (such as your telephone number or email address);</p> <p>Details of your enquiry;</p> <p>Your connection with the Church in Wales (which may reveal your religious beliefs), if relevant.</p>	<p style="text-align: center;">Consent</p> <p>Use of your Personal Data for the purpose dealing with your enquiry or complaint is based on your Consent.</p> <p>Keeping a record of your enquiry or complaint in order to deal with it, is based on your Consent.</p> <p style="text-align: center;">Special Category Data</p> <p>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.</p> <p style="text-align: center;">Legal Obligation</p> <p>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.</p> <p>This is because the Church in Wales has a Legal Obligation to take all reasonable precautions to ensure that the Church is a safe place for all.</p>	<p>Records of your enquiry or complaint are retained until 12 months after the matter is resolved or your Consent is withdrawn, which ever comes first.</p> <p>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.</p>	<p>Your Personal Data is provided by you when you contact us. (e.g. by making a phone call or emailing us).</p> <p>We will use the Personal Data to deal with your enquiry or complaint;</p> <p>We will make a record of your enquiry /complaint for internal admin purposes.</p>

Consequences of not providing your data

- (a) Failure to provide us with your details will mean that we cannot contact you to deal with your enquiry.
- (b) 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– ROPA REF – RB13

16.9 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
<p>Your name;</p> <p>Your contact details including, email address and (if a member of the Church in Wales) details of your parish/Diocese.</p> <p>For online training, we may collect technical information, including the internet protocol address used to connect your computer to the internet;</p> <p>the browser type and version;</p> <p>time zone settings;</p> <p>browser plug-in types and versions, operating system and platform;</p> <p>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;</p> <p>length of visit to certain pages and methods used to browse away from the page.</p> <p>Your attendance record of courses (whether online or in person), dates of completion and marks of any assessments.</p>	<p>Public Task</p> <p>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.</p> <p>Contract</p> <p>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.</p> <p>Legal Obligation</p> <p>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.</p> <p>Special Category Data</p> <p>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.</p>	<p>We keep records of all completed training for a period of six years from the date of completion.</p> <p>This is so that refresher or updated training can be offered to the appropriate persons at the appropriate time.</p> <p>Certain training information will be contained in Clergy files and retention periods are dealt with in our Clergy Files Policy available on our Website.</p>	<p>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/</p> <p>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).</p> <p>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.</p> <p>Training courses may be arranged and booked by the relevant Diocese.</p>

Consequences of not providing your data

- (a) If you disable our Cookies, you will be unable to use certain parts of/functions on our website.
- (b) 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.
- (c) 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 FEATURED IN OUR NEWSLETTERS OR ARTICLES– ROPA REF – RB14

16.10 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
<p>Your name;</p> <p>Your geographical location;</p> <p>Your association with the Church in Wales, which is likely to reveal your religious beliefs;</p> <p>Any other personal details you provide to us as part of your story.</p>	<p style="text-align: center;">Consent</p> <p>Use of your Personal Data for the purpose of writing the newsletter or article is based on your Consent.</p> <p style="text-align: center;">Special Category Data</p> <p>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.</p> <p style="text-align: center;">Archiving</p> <p>Newsletters are a valuable source of historical information and as such once published are retained indefinitely in the public interest for historical research purposes.</p>	<p>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.</p>	<p>Your Personal Data is provided by you when you agree to feature in a newsletter or article.</p> <p>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.</p>

Consequences of not providing your data

- (a) Failure to provide us with your details will mean that we cannot contact you to deal with your enquiry.
- (b) In certain limited circumstances we may be able to deal with allegations of misconduct amounting to safeguarding issues anonymously.

INDIVIDUALS AND ORGANISATIONS WHO PROVIDE US WITH SERVICES – ROPA REF – RB15

16.11 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
<p>Your name and contact details;</p> <p>Your bank account details.</p>	<p>Contract</p> <p>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.</p> <p>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.</p> <p>Special Category Data</p> <p>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.</p>	<p>We will retain your Personal Data for the duration of the provision of services and for seven years thereafter in case there should be any contractual dispute.</p> <p>We use Jotform.com as data processor. Your data will remain on their servers in Europe for up to 2 months while being transferred to our in house X-Ledger system where it will be kept for the duration of the contract plus seven years.</p>	<p>Your Personal Data is provided by you when you agree to provide us with services.</p> <p>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.</p> <p>We use Jotform.com as data processor, we will share your data with them under a data processor agreement.</p>

Consequences of not providing your data

- (a) 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.

RB STAFF MEMBERS FULL AND PART TIME – ROPA REF – RB16

16.12 Data under control analysis chart for **RB Staff Full & Part Time**.

Personal Data	Lawful Base(s) and Statutory authority	Retention Period	Source of Data Use of Data & Data Sharing	Types of Personal Data we may use
<p>Your name;</p> <p>Your contact details (such as your postal address, telephone number and/or email address);</p> <p>Next of kin/Family data for contact in an emergency</p> <p>Your Bank Account details (if in a paid post);</p> <p>Your role with the Church in Wales (which may reveal your religious beliefs);</p> <p>Access to your data via the Computer Monitoring Policy. (See section 3.1 below)</p>	<p>Consent</p> <p>We may process data with your consent such as in the early stages of applying for a role.</p> <p>Contract</p> <p>The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the direct request of the data subject prior to entering into a contract.</p> <p>Public Task</p> <p>Use of your Personal Data for administrative purposes, to ensure the smooth and proper running of the Church.</p> <p>Special Category Data</p> <p>The lawful authority we rely on to process any information provided as part of an employment</p>	<p>Your contact details will be retained for the duration of your employment and for 7 years thereafter.</p> <p>DBS disclosure results will ordinarily be destroyed within six months of receipt.</p> <p>In the event that the disclosure result highlights concerns relating (in the view of our Safeguarding Manager) to safeguarding of children and/or adults at risk, a record of the disclosure results will be retained securely by our Safeguarding Team indefinitely.</p>	<p>Your personal data will usually be provided to us by you directly</p> <p>We will share your contact details with other departments within the RB for specific admin matters including training.</p> <p>We will use your bank account details to pay your wages and any expenses due;</p> <p>We will collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.</p> <p>We carry out DBS checks on behalf of other parts of the Church in Wales, such as on behalf of the Bishops or Diocese.</p>	<p>We may process the following types of data about you</p> <p>Identity</p> <p>Financial</p> <p>Transaction</p> <p>Technical</p> <p>Profile</p> <p>Usage</p> <p>Marketing</p> <p>If your name and contact details are not provided you will be unable to be appointed as a staff member or receive salary payments, pension rights or other related financial matters.</p> <p>Further details regarding this in section 17 below.</p>

	<p>application which is special category data, such as health, religious or ethnic information is Article 9(2)(b) of the UK GDPR, which also relates to our obligations in employment and the safeguarding of the employee's fundamental rights and article 9(2)(h) for assessing an individual's work capacity as an employee.</p> <p>Where DBS Checks are conducted they are part of an automated decision making process pursuant to Article 22 UK GDPR.</p> <p>The information provided by the DBS service is used to assess suitability for appointment to a post.</p> <p>Legal Obligation</p> <p>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</p>		<p>The information obtained will be used by us in conjunction with other parts of the Church in Wales to determine whether to engage you.</p> <p>Information about criminal convictions will be obtained from the Disclosure and Barring Service ("DBS") if you have agreed to undertake a DBS check through the Church in Wales.</p> <p>We will share your data with certain third party organisations who provide services to assist us with certain matters such as external Human Resources policy providers and software companies.</p> <p>A list of these third parties is available on request.</p>	
--	--	--	--	--

	<p>substantial public interest, namely, safeguarding, preventing or detecting unlawful acts, protecting the public against dishonesty, preventing fraud or suspicion of terrorism or money laundering.</p> <p>This is because the Church in Wales has a Legal Obligation to take all reasonable precautions to ensure that the Church is a safe place for all.</p> <p>Also, Schedule 1 part 1(1) and (2)(a) and (b) of the Data Protection Act 2018 which relates to processing for employment, the assessment of working capacity and preventative or occupational medicine.</p> <p>Legitimate Interest</p> <p>This lawful basis is used for our CCTV systems and when staff members use Video conferencing software. (see separate</p>			
--	---	--	--	--

	<p>legitimate interest assessments)</p> <p>Your data may be shared with your line manager under our Management Gifting policy to provide you with a gift.</p>			
--	---	--	--	--

17 Engaging with us on Social Media

- 17.1 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.
- 17.2 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.
- 17.3 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.

18 Types and Categories of Personal Data

- 18.1 **Identity data:** name, username, title, date of birth. Contact data: billing and delivery address, email address, phone number.
- 18.2 **Financial data:** payment card details (processed by a third-party payment services provider and not stored by us).
- 18.3 **Transaction data:** details of products purchased, amounts, dates etc.
- 18.4 **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.
- 18.5 **Profile data:** username and password, purchases or orders made by users.
- 18.6 **Usage data:** information about how users use our website, products and services.
- 18.7 **Marketing and communications data:** record of Website users preferences in receiving marketing from us about the products we sell.

19 Sharing Your Personal Data with others

19.1 SERVICE PARTNERS– [ROPA REF – RB15](#)

Information about our service partners	<p>Our service partners are other businesses that we enter into contracts with. They include:</p> <p>Suppliers and sub-contractors;</p> <p>Suppliers of IT products and services;</p> <p>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.</p> <p>However, if you would like further information about any of our current service providers, please contact us on 029 2034 8200</p>
Why we need to share your Personal Data	<p>We use suppliers and sub-contractors to perform certain aspects of our contracts with our tenants. For example, providing maintenance services;</p> <p>We use suppliers of IT products and services in connection with the supply, maintenance and/or improvement of our IT network.</p>

<p>The legal grounds we rely upon</p>	<p>The sharing of your personal data with suppliers and sub-contractors is necessary for the performance of our Contract with them;</p> <p>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.</p>
--	--

19.2 OTHER PARTS OF THE CHURCH IN WALES – ROPA REF – RB17

<p>Information about the different parts of the Church</p>	<p>Information about the structure of the Church in Wales can be found at www.churchinwales.org.uk .</p>
<p>Why we need to share your Personal Data</p>	<p>where it is necessary in the course of the work and activities of the Church in Wales, for example:</p> <p>sharing details of a complaint with the applicable Parish or Diocese;</p> <p>sharing details about donations received being shared with the applicable Parish or Diocese;</p> <p>sharing details of disciplinary issues relating to clergy with the applicable Bishop.</p>
<p>The legal grounds we rely upon</p>	<p>We will share Personal data with other parts of the Church in Wales when:</p> <p>We have a legal Obligation to do so.</p> <p>It is necessary for the performance of a Contract</p> <p>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.</p> <p>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</p>
<p>What precautions do we take?</p>	<p>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.</p> <p>To this end the Church in Wales aims to ensure;</p> <p>that only personal data that needs to be shared in connection with the operations and activities of the Church is shared;</p> <p>that personal data is only shared when it is necessary and appropriate to do so;</p> <p>that personal data is shared on a ‘need to know’ basis and is not shared more widely than is necessary; and</p> <p>that personal data is shared securely.</p>

19.3 OTHER THIRD PARTIES (Regulatory) – ROPA REF – RB18

<p>Legal or regulatory requirements</p>	<p>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.</p>
--	--

	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	<p>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.</p> <p>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</p>
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.	<p>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.</p> <p>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.</p> <p>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.</p>
Use of Legitimate Interests	<p>We use the Lawful Base of Legitimate interest sparingly and only when no other basis exists for processing the Personal Data in question.</p> <p>The Legitimate Interest Assessments are reproduced in full in this document.</p> <p>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.</p> <p>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.</p> <p>To support the primary objectives of Representative body of the Church in Wales.</p>
When do we apply the Lawful basis of Legitimate Interest?	

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 Website Cookies Policy – ROPA REF – RB20

Purpose

- 21.1 This Cookie Policy explains how we use cookies and similar technologies on its website, in accordance with the UK Privacy and Electronic Communications Regulations (PECR), the UK GDPR, and amendments introduced by the Data (Use and Access) Act (DUAA).

What Are Cookies

- 21.2 Cookies are small text files that are placed on a user's device when they visit a website. They are widely used to make websites work efficiently, improve user experience, and provide information to website operators.
- 21.3 Cookies may be:
 - a) Session cookies, which expire when the browser is closed; or
 - b) Persistent cookies, which remain on the device for a set period or until deleted.

How We Use Cookies

- 21.4 We use cookies to:
 - a) Ensure the website functions correctly
 - b) Maintain security and prevent fraud
 - c) Remember user preferences
 - d) Understand how the website is used, in order to improve performance and content
- 21.5 Cookies may be set by us ("first-party cookies") or by third parties providing services on our behalf ("third-party cookies").

Cookies That Do Not Require Consent

21.6 Under UK law, as clarified by the DUAA, certain cookies may be used **without user consent** where they are strictly necessary for the website to function or for limited, low-risk purposes. These include cookies used:

- a) To enable core website functionality (e.g. page navigation, form submission)
- b) For security purposes, including fraud prevention and system integrity
- c) To remember user preferences essential to the service requested
- d) For **anonymous, low-risk statistical measurement** aimed at understanding website usage and performance, where:
 - i. Data is aggregated or anonymised;
 - ii. It is not used to track users across websites; and
 - iii. It does not significantly impact user privacy

These cookies are enabled by default and cannot be switched off, as the website would not function properly without them.

Cookies That Require Consent

21.7 Where cookies are used for purposes that are **not strictly necessary**, such as:

- a) Marketing or advertising
- b) Tracking users across websites
- c) Personalised content or profiling

We will obtain the user's **prior consent** before placing those cookies on their device.

21.8 Users will be presented with clear information and genuine choice through a cookie banner or preference tool.

Managing Cookie Preferences

21.9 Users can manage or withdraw their cookie preferences at any time by:

- a) Using the cookie settings tool available on the website; and/or
- b) Adjusting browser settings to block or delete cookies

Please note that blocking certain cookies may affect website functionality.

Third-Party Cookies

21.10 Some cookies may be set by third-party service providers, such as analytics or embedded content providers. These third parties are responsible for their own compliance with applicable data protection and e-privacy laws.

21.11 Where third-party cookies require consent, they will not be activated unless and until consent is provided.

Personal Data and Cookies

21.12 Where cookies involve the processing of personal data, that processing is carried out in accordance with our Privacy Policy, which explains:

- a) What personal data we collect
- b) The lawful bases relied upon

- c) How long data is retained
- d) Individuals' rights under UK data protection law

22 Automated Decision-Making and Profiling

Policy Statement: Purpose

- 22.1 This policy statement documents our assessment of the use of automated decision-making and profiling and confirms the outcome of that assessment in accordance with the UK GDPR and the Data Protection Act 2018.

Definition

- 22.2 Under Article 22 of the UK GDPR, automated decision-making refers to decisions made solely by automated means, without meaningful human involvement, which produce legal effects concerning an individual or similarly significant effects. This includes certain forms of automated profiling.

Assessment Scope

- 22.3 We have assessed our processing activities across all business functions, including:
- a) Employment and workforce management
 - b) Recruitment and selection
 - c) Performance management and disciplinary processes
 - d) Customer, client, and public-facing services
 - e) Operational, financial, and administrative decision-making

Assessment Outcome

- 22.4 Following this assessment, We have concluded that:
- a) We do not carry out any decision-making that is based solely on automated processing;
 - b) No automated processing produces legal effects or similarly significant effects on individuals;
 - c) Any systems or tools used to support decision-making involve meaningful human review and discretion; and
 - d) We do not engage in automated decision-making or profiling in relation to:
 - o Staff members, workers, or job applicants; or
 - o Members of the public, customers, or other external individuals.
- 22.5 Accordingly, Article 22 of the UK GDPR does not apply to our current processing activities.

Safeguards and Controls

- 22.6 Where technology is used to assist decision-making, We ensure that:
- a) Decisions are reviewed and approved by appropriately trained individuals;
 - b) Individuals are not subject to decisions made solely by automated means; and
 - c) Processing complies with the principles of lawfulness, fairness, transparency, and accountability.
- 22.7 In recruitment processes, including where Disclosure and Barring Service (DBS) information is considered, all decisions are subject to meaningful human review.

22.8 DBS results are assessed on a case-by-case basis, taking into account the nature of the role, relevance of any information disclosed, safeguarding considerations, and any representations made by the individual. No applicant is rejected solely by automated means.

Transparency

22.9 As we do not conduct automated decision-making within the meaning of Article 22 UK GDPR, specific disclosures relating to such processing are not currently required. However, we provide general transparency regarding our use of technology in decision-making where relevant.

22.10 We prohibit the use of any system or rule that would result in the automatic rejection of candidates based solely on predefined criteria without human assessment

Ongoing Review

22.11 This position will be kept under review and reassessed if there are material changes to:

- a) Business processes or services
- b) Use of artificial intelligence or automated tools
- c) Employment practices
- d) Applicable legislation or ICO guidance

Accountability

22.12 This statement forms part of our UK GDPR accountability framework and may be made available to regulators or other relevant stakeholders upon request.

23 Safeguarding and Children's Personal Data – [ROPA REF - RB-05](#)

23.1 The RB recognises that personal data relating to children and safeguarding matters requires a higher level of protection.

23.2 In safeguarding contexts, the protection of individuals from harm may take precedence over certain data protection rights where permitted by law.

23.3 We process personal data relating to children in connection with our activities, including worship, events, pastoral care, safeguarding, and community engagement.

23.4 We also process safeguarding information, which may include sensitive personal data relating to children, vulnerable individuals, and those connected with safeguarding concerns.

23.5 Such data may include:

- a) identity and contact details
- b) participation in activities or events
- c) safeguarding records, concerns, and case information
- d) information relating to health, wellbeing, or risk

23.6 Safeguarding data is processed for purposes including:

- a) protecting children and vulnerable individuals from harm
 - b) responding to safeguarding concerns and allegations
 - c) risk assessment and management
 - d) compliance with safeguarding policies and legal obligations
- 23.7 Due to the sensitive nature of safeguarding processing:
- a) access is restricted to authorised individuals
 - b) information is handled confidentially
 - c) additional security measures are applied
- 23.8 Personal data relating to children and safeguarding is processed under appropriate lawful bases, including:
- a) legal obligations
 - b) Public Task
 - c) legitimate interests (including safeguarding functions)
 - d) substantial public interest under applicable legislation
- 23.9 Where appropriate, consent will be obtained from a parent or guardian, particularly in relation to:
- a) Images or recordings
 - b) Participation in certain activities
- 23.10 We will not use children’s personal data for marketing purposes without appropriate consent.
- 23.11 Our website is not specifically directed at children. We do not knowingly collect personal data from children through our website without appropriate consent.
- 23.12 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.
- 23.13 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.
- 23.14 There is nothing on our Website which could be damaging to children who view the pages or the pictures.
- 23.15 Further information about safeguarding-related data processing is provided in this document at Annex B - Safeguarding Privacy Notice.

24 Data Protection Complaints Policy

- 24.1 How to Make a Complaint – An individual can make a complaint to our Data Protection Manager by using our contact details provided above or by using the Online form on our website.

- 24.2 Purpose of the Policy - This policy outlines how we handle complaints related to personal data under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Data (Use and Access) Act 2025. It ensures individuals can raise concerns regarding the collection, processing, sharing, or access to their personal data and be assured of a fair, timely, and lawful response.
- 24.3 Scope of the Policy - This policy covers all personal data held in physical and electronic formats and applies to:
- (a) Employees
 - (b) Website Users
 - (c) Third-party contractors
 - (d) Any individual whose personal data is processed by us
- 24.4 Legal Framework - This policy is guided by the following UK legislation:
- (a) UK General Data Protection Regulation (UK GDPR)
 - (b) Data Protection Act 2018
 - (c) Data (Use and Access) Act 2025
 - (d) Privacy and Electronic Communications Regulations (PECR)
- 24.5 Grounds for Complaint – An individual may submit a complaint if you believe we:
- (a) Processed your personal data unlawfully or without your consent or a lawful basis.
 - (b) Denied your data subject rights, including:
 - (c) Information/ Access
 - (d) Rectification
 - (e) Erasure ("Right to be Forgotten")
 - (f) Data portability
 - (g) Restriction or objection to processing
 - (h) Failed to provide transparency in data use or profiling.
 - (i) Shared or accessed your data outside of approved legal parameters.
 - (j) Did not notify you of a data breach within the required timeframe.
 - (k) Breached our obligations set out in the data legislation and Regulations.
- 24.6 Complaints Procedure - Once a complaint is received it will receive:
- (a) Acknowledgement - We will acknowledge receipt of the complaint promptly and in any event within 30 days (our internal target is within 5 working days)
 - (b) Initial assessment by the Data Protection Manager to determine validity and scope
 - (c) Investigation within **30 calendar days** (complex matters may take longer, with notice)
 - (d) A written response outlining:
 - (i) Findings
 - (ii) Any remedial actions taken
 - (iii) Your rights and next steps
- 24.7 Remedies and Corrective Action - If the investigation identifies a failure or breach, we may take one or more of the following actions or others as appropriate:

- (a) Amending or deleting incorrect data
- (b) Changing internal processes
- (c) Training or disciplining staff
- (d) Reporting incidents to the Information Commissioner's Office (ICO) where required
- (e) Offering a formal apology (if applicable)

24.8 Complaints Register and Record Keeping

24.9 The RB will maintain a record of all data protection complaints received. The complaints register will record:

- (a) the date the complaint was received;
- (b) the nature of the complaint;
- (c) the outcome of the investigation;
- (d) any corrective action taken; and
- (e) whether the matter was referred to the Information Commissioner's Office.

24.10 These records are maintained as part of the RB's accountability obligations under the UK GDPR and may be used to monitor compliance, identify trends, and improve internal data protection practices.

24.11 Escalation and Data Rights - If the complainant is not satisfied with our handling of their complaint or the outcome, once we have investigated the complaint and replied, they may escalate the matter to the: Information Commissioner's Office (ICO). Their contact details are below.

ICO Website: <https://ico.org.uk/make-a-complaint/>

Phone: 0303 123 1113

Post: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

DATA PROTECTION MANAGEMENT SYSTEM

Compliance Handbook and Governance Framework

PART THREE of FIVE

STAFF PROCEDURAL POLICIES

25 Human Resources and Payroll – ROPA REF – RB16

- 25.1 As a core activity within the RB We process data for the purposes of our Human Resources function and Payroll function.
- 25.2 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.
- 25.3 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.
- 25.4 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.
- 25.5 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.
- 25.6 **NB:** A dedicated staff member privacy notice with an extended versions of clauses 25 to 29 are available on the staff intranet/Portal.

26 Home Working Policy – See Intranet – Staff Portal

27 Generative Ai Policy – See Intranet – Staff Portal

28 Internet, Email and Communications Policy– See Intranet – Staff Portal

29 Social Media Policy– See Intranet – Staff Portal

DATA PROTECTION MANAGEMENT SYSTEM
Compliance Handbook and Governance Framework

PART FOUR of FIVE

DATA RIGHTS & BREACH POLICIES

30 **Data Subject Access Requests – ROPA REF – RB19**

- 30.1 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.
- 30.2 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.
- 30.3 The RB will handle all data subject access requests in a manner that is reasonable and proportionate, taking into account:
- a) the nature and scope of the request;
 - b) the systems in which personal data is held;
 - c) the likelihood of locating relevant personal data; and
 - d) the burden and cost of retrieval.
- 30.3.1 The RB is not required to conduct unlimited or speculative searches but must be able to justify the scope of any searches undertaken and any limitations applied.
- 30.3.2 that all data subject access requests are supported by appropriate records, including search records and decision logs, to demonstrate compliance.
- 30.4 The **Data Protection Manager** is responsible for ensuring:
- (a) that all data subject access requests are dealt with in accordance with UK GDPR and other relevant legislation and guidance; and
 - (b) 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.
- 30.5 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.
- 30.6 This policy provides guidance on:
- 30.6.1 what to do if you receive a data subject access request; and
 - 30.6.2 how to decide whether a request for information is a data subject access request.

- 30.7 Failure to comply with the right of access under UK GDPR puts both staff and the RB at a potentially significant risk.
- 30.8 The RB takes compliance with this policy very seriously and requires that all data subject access requests are handled in a consistent, documented and auditable manner.
- 30.9 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.
- 30.10 If you have any questions regarding this policy, please contact the **Data Protection Manager**.

How to recognise a data subject access request (DSAR)

- 30.11 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:
- 30.11.1 for confirmation as to whether we process personal data about the individual and, if so:
 - 30.11.2 for access to that personal data
 - 30.11.3 and certain other supplementary information
- 30.12 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.
- 30.13 All data subject access requests must be recorded by the Data Protection Manager in a central register, including the date of receipt, scope of the request, and applicable response deadline.
- 30.14 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

- 30.15 If you receive a data subject access request, you must immediately take the steps to alert the **Data Protection Manager**.
- 30.16 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.

- 30.17 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.
- 30.18 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**.
- 30.19 If you receive a data subject access request by email, you must immediately forward the request to the **Data Protection Manager**.
- 30.20 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.
- 30.21 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.
- 30.22 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.

- 30.23 Where we process a large quantity of information about an individual, we may ask the individual to specify the information or processing activities to which the request relates in order to enable the RB to conduct searches in a targeted and proportionate manner.
- 30.24 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.
- 30.25 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

- 30.26 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.
- 30.27 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.
- 30.28 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.
- 30.29 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.
- 30.30 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

- 30.31 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, including where the effort required to comply would be disproportionate when balanced against the value of the information likely to be obtained.
- 30.32 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

- 30.33 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.
- 30.34 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.
- 30.35 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

30.36 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.

30.37 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

30.38 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.

30.39 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

30.40 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. It is therefore necessary to define an appropriate and proportionate search strategy at the outset.

30.41 Depending on the type of information requested and applying a reasonable and proportionate approach 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;

30.42 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.

- 30.43 The RB is not required to search every possible system or location where personal data may be held. Searches will be limited to those systems and locations where it is reasonable to expect that relevant personal data will be found.
- 30.44 The scope of the search, including any systems or locations excluded, must be determined on a case-by-case basis and documented by the Data Protection Manager.
- 30.45 In determining the scope of any search, the RB will take into account:
- (a) the relevance of the system to the request;
 - (b) the likelihood of retrieving meaningful personal data;
 - (c) the time and cost involved in conducting the search; and
 - (d) whether the data can be obtained from alternative sources more efficiently.
- 30.46 A record of the searches undertaken must be maintained for each data subject access request, including:
- (a) the systems and locations searched;
 - (b) the search parameters used;
 - (c) any systems or locations not searched and the reasons for exclusion.

What is personal data?

- 30.47 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.
- 30.48 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

- 30.49 Occasionally we may receive a request for data subject access by a third party (an 'agent') acting on behalf of an individual.
- 30.50 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

- 30.51 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.

30.52 In applying any exemption, the RB will ensure that the decision is necessary, proportionate and documented.

Crime detection and prevention:

30.53 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.

30.54 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:

30.55 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:

30.56 We do not have to disclose any confidential references that we have given to or received from 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

Legal professional privilege:

30.57 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:

30.58 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:

30.59 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:

30.60 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

- 30.61 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.
- 30.62 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.
- 30.63 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.

Audit Trail

- 30.64 The RB will retain an audit file for each data subject access request, including the request, correspondence, search records, decisions on scope and exemptions, and the final response.

Consequences of failing to comply with this policy

- 30.65 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.
- 30.66 Any questions regarding this Policy should be addressed to the **Data Protection Manager**.

31 Data Breach Policy

- 31.1 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.
- 31.2 This policy sets out how the RB identifies, manages, investigates, and responds to personal data breaches.
- (a) in accordance with the UK GDPR, the Data Protection Act 2018, and amendments introduced by the Data (Use and Access) Act (DUAA).
 - (b) Following our commitment to protecting personal data and ensuring that any personal data breach is handled promptly, effectively, and transparently.

Scope

- 31.3 This policy applies to:
- a) All employees, workers, contractors, and temporary staff
 - b) All personal data processed by us, in any format
 - c) Breaches involving data relating to staff, customers, clients, suppliers, or members of the public

What Is a Personal Data Breach

- 31.4 A personal data breach is a security incident that leads to:
- a) Loss of confidentiality (e.g. unauthorised disclosure or access);
 - b) Loss of integrity (e.g. unauthorised alteration); or
 - c) Loss of availability (e.g. accidental loss or destruction).
- 31.5 Not all incidents will meet the threshold of a reportable personal data breach, but all suspected incidents must be reported internally.
- 31.6 A personal data breach may occur through accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
- 31.7 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.

Reporting a Data Breach

31.8 Internal Reporting

31.9 All staff must report any suspected or actual personal data breach immediately.

- (a) to the Data Protection Manager or, if unavailable, their line manager.
- (b) All suspected or confirmed personal data breaches must be recorded in a central breach register immediately upon identification.

31.10 Reports should include, where possible:

- a) A description of what happened
- b) The type of personal data involved
- c) The individuals affected
- d) When the incident occurred or was discovered

31.11 Failure to report a breach promptly may increase risk to individuals and the RB.

Breach Assessment

31.12 Upon receipt of a report, the Data Protection Manager will carry out an initial triage to:

- (a) confirm whether the incident constitutes a personal data breach;
- (b) determine whether immediate containment action is required; and
- (c) assign responsibility for investigation.

31.13 Breaches may be classified according to severity (e.g. low, medium, high) based on:

- (a) the sensitivity of the data involved;
- (b) the number of individuals affected; and
- (c) the potential impact on individuals.

31.14 This classification will inform the urgency of response and level of oversight required.

31.15 For the purposes of this policy, a breach is considered to be "identified" when the RB has a reasonable degree of certainty that a personal data breach has occurred.

31.16 Once a breach is identified, **the Data Protection Manager** will promptly assess it to determine:

- a) The nature, scope, and cause of the breach
- b) The categories and volume of personal data affected
- c) Whether special category or criminal offence data is involved
- d) The likely impact on the rights and freedoms of individuals

Risk-Based Assessment (DUAA Approach)

- 31.17 In line with the DUAA, we assess breaches using a **risk-based and proportionate approach**, considering whether the breach is likely to result in a risk to the rights and freedoms of individuals.
- 31.18 Breach investigations will be conducted in a manner that is reasonable and proportionate, taking into account the severity of the incident, the sensitivity of the data involved, and the likely impact on individuals.
- 31.19 This assessment focuses on practical and foreseeable harm, such as:
- a) Identity theft or fraud
 - b) Financial loss
 - c) Discrimination
 - d) Loss of confidentiality or distress
- 31.20 Incidents involving safeguarding data, special category data, or large volumes of personal data must be escalated to the Data Protection Manager immediately and prioritised for assessment.

Notification to the ICO

- 31.21 We will notify the Information Commissioner's Office (ICO) without undue delay and, where required, within 72 hours of becoming aware of a personal data breach that is likely to result in a risk to individuals' rights and freedoms.
- 31.22 Where notification is not required, we will document:
- a) the reasons for the decision;
 - b) the assessment carried out; and
 - c) the factors considered in determining that the breach is unlikely to result in a risk to individuals.

Notification to Affected Individuals

- 31.23 We will notify affected individuals **without undue delay** where a personal data breach is likely to result in a **high risk** to their rights and freedoms.
- 31.24 Notifications will be clear and plain-language and will include:
- a) The nature of the breach
 - b) The likely consequences
 - c) The steps we have taken or propose to take
 - d) Advice on how individuals can protect themselves
- 31.25 Notification to individuals may not be required where permitted by law, for example where appropriate technical or organisational measures render the data unintelligible.

Containment and Remediation

- 31.26 We will take immediate and appropriate steps to contain and limit the breach as soon as it is identified.
- 31.27 Following resolution of a breach, the RB will assess the root cause and implement appropriate corrective actions to prevent recurrence.

Record Keeping and Accountability

- 31.28 In accordance with Article 33(5) of the UK GDPR, the RB maintains an internal record of all personal data breaches, including:
- a) The facts relating to the breach
 - b) Its effects
 - c) The remedial action taken
 - d) Decisions on notification
- 31.29 An audit file will be maintained for each personal data breach, including the incident report, investigation findings, risk assessment, decisions on notification, and remedial actions taken.
- 31.30 This record forms part of our UK GDPR accountability obligations.

Roles and Responsibilities

- 31.31 **All staff** are responsible for reporting suspected breaches immediately.
- 31.32 **Managers** must escalate incidents and support investigations.
- 31.33 The **Data Protection Manager** is responsible for breach assessment, notification decisions, and regulatory engagement.

Training and Awareness

- 31.34 We provide regular training and guidance to ensure staff understand:
- a) How to recognise a personal data breach
 - b) How to report incidents
 - c) Their responsibilities under this policy

Review

- 31.35 This policy will be reviewed periodically and updated to reflect:
- a) Changes in legislation or ICO guidance
 - b) Lessons learned from data breach incidents
 - c) Changes to our processing activities or systems

DATA PROTECTION MANAGEMENT SYSTEM

Compliance Handbook and Governance Framework

PART FIVE of FIVE

LEGITIMATE INTEREST & UPDATES POLICIES

32 Policy Statement: Assessment of DUAA Recognised Legitimate Interests

Purpose

- 32.1 This policy statement records our assessment of the “recognised legitimate interests” introduced under the UK Data (Use and Access) Act 2025 (DUAA) and confirms the outcome of that assessment.
- 32.2 The DUAA amends the UK GDPR by introducing a limited set of **recognised legitimate interests** for which organisations may process personal data without undertaking a Legitimate Interests Assessment (LIA), provided the processing strictly falls within the categories defined in the legislation.

Assessment Outcome

- 32.3 We have reviewed the recognised legitimate interests set out in the DUAA, including (but not limited to):
- (a) National security, public security, and defence
 - (b) Emergency response
 - (c) Safeguarding vulnerable individuals
 - (d) Crime prevention, detection, and investigation
 - (e) Other narrowly defined public interest purposes

Following this review, We have concluded that:

- 32.4 the RB does not currently rely on any of the recognised legitimate interests introduced under the DUAA as a primary lawful basis for its processing activities.
- 32.5 While certain activities (such as safeguarding or cooperation with law enforcement) may align with recognised legitimate interests, the RB has elected to continue to rely on established lawful bases under Article 6 UK GDPR to ensure consistency, clarity, and appropriate safeguards.

Lawful Basis for Processing

- 32.6 As a result, We do **not** rely on DUAA recognised legitimate interests as a lawful basis for processing personal data. Instead, all processing activities continue to rely on one or more of the established lawful bases under UK GDPR Article 6:
- 32.7 Where legitimate interests are relied upon as a lawful basis, they will be supported by a documented Legitimate Interests Assessment (LIA).

Ongoing Review

- 32.8 This assessment will be kept under review and revisited if there are material changes to our business activities, the nature of its data processing, or further regulatory guidance is issued by the Information Commissioner’s Office (ICO).

- 32.9 Where a new processing activity is proposed that may fall within a recognised legitimate interest, this must be assessed and approved by the Data Protection Manager before reliance is placed on that basis.

Accountability

- 32.10 This statement forms part of our accountability records under the UK GDPR and is available for inspection by relevant stakeholders and regulators upon request.

33 Marketing

- 33.1 The RB does not engage in commercial direct marketing activities. Any communications with individuals are limited to pastoral, administrative, or charitable purposes and are conducted in accordance with applicable data protection and PECR requirements.

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

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

34 Video Conferencing Policy – [ROPA REF – RB01](#)

General

- 34.1 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.

- 34.2 Where recordings are made, participants will be clearly informed at the outset. Where appropriate, alternative means of participation (such as audio-only) will be made available.

- 34.3 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.

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

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

- 34.6 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

- 34.7 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.'
- 34.8 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.
- 34.9 Participants will not be allowed to share external links during the call without the express permission of the Moderator.
- 34.10 All Participants will be warned regarding the dangers of Phishing, clicking unknown links etc at the commencement of a call.

The Platform

- 34.11 The Video Conference Platform will be approved by the RB Management before use.
- 34.12 The latest software version must be checked for and downloaded prior to each use of the platform.
- 34.13 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

- 34.14 Every use of the Platform will be controlled by the use of a Password to access any individual Video Conference call.
- 34.15 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

- 34.16 Video Conference recording facilities are available on most platforms.
- 34.17 We understand the image of a participant on a Video Conference call is Personal Data and can be subject to a Data Access request.
- 34.18 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.

34.19 The use of video conferencing platforms has been assessed under a Legitimate Interests Assessment (LIA-01), which is set out in Annex A to this policy.

35 CCTV MONITORING – ROPA REF – RB02

35.1 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.

35.2 This policy sets out the accepted use of the CCTV equipment and images to ensure compliance with relevant data protection and privacy laws including: UK General Data Protection Regulation (UK GDPR) as supplemented by the Data Protection Act 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).

35.3 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

35.4 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**.

35.5 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.

35.6 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

35.7 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

35.8 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:

- (a) deter crime and assist in the prevention and detection of crime and/or serious breaches of policies and procedures;
- (b) assist with the identification, apprehension and prosecution of offenders; and
- (c) monitor security and health and safety at our premises.

- 35.9 The use of CCTV is subject to ongoing review to ensure that it remains necessary, proportionate, and justified in light of its impact on individuals.
- 35.10 We have carried out a data protection impact assessment and consider that these purposes are legitimate, reasonable, appropriate and proportionate.
- 35.11 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.
- 35.12 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.
- 35.13 We keep a record of the CCTV installed and used.
- 35.14 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

- 35.15 Covert monitoring means monitoring carried out in a manner calculated to ensure those subject to it are unaware that it is taking place.
- 35.16 We do not undertake covert recording with our CCTV equipment.

Positioning cameras

- 35.17 We will make every effort to position cameras to ensure they only cover our premises.
- 35.18 Cameras will not be routinely monitored and the recordings will be used in a passive recording manner.
- 35.19 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.
- 35.20 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.
- 35.21 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.
- 35.22 The cameras do not focus only on one sector of employees or visitors and are used in the manner that would, objectively be expected.

- 35.23 The recordings are held digitally, password protected, accessible only by trained and approved staff members and kept for no longer than 3 months.
- 35.24 Individuals retain the right to object to this processing; however, the RB has determined that the processing is reasonable, proportionate and within the expectations of individuals in the circumstances.
- 35.25 It is recognised that CCTV data can form the basis of a Subject Access Request which can be made to the RB under the Data Subject Access Request Policy, should a data subject have any concerns.

Image quality

- 35.26 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 **Data Protection Manager** is responsible for arranging timely repair.

Data and image retention

- 35.27 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.
- 35.28 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.
- 35.29 Where a request to retain information is authorised, reasonable steps will be taken to safeguard any footage which may otherwise be deleted.
- 35.30 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

35.31 Staff images

- (a) 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.
- (b) Access to recorded images will be restricted to authorised staff only and will not be made more widely available.
- (c) 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.
- (d) 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:
 - (e) the date and time they were removed;
 - (f) the name of the person removing the media;
 - (g) 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);
 - (h) the reason for viewing the images; and
 - (i) the date and time the media were returned to the system, destroyed or sent to secure storage, as applicable.
- (j) 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

- (k) 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.
- (l) 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.
- (m) 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:
 - (i) 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;
 - (ii) prosecution agencies (such as the Crown Prosecution Service);
 - (iii) relevant legal representatives of people whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings);

- (iv) individuals who have been caught on our CCTV in accordance with a data subject access request;
- (v) 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
- (vi) staff involved with our disciplinary processes.

35.32 If a police officer requests images from our CCTV system in relation to an investigation that has not been initially reported by the RB, 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

35.33 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.

35.34 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

35.35 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.

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

35.37 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.

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

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

35.40 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

35.41 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.

35.42 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

35.43 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.

35.44 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.

35.45 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.

Enforcement and compliance

35.46 All authorised users of our surveillance technology and its underlying data are required to adhere to the controls around the use of CCTV as set out in this policy and as may be advised separately from time to time. The use of the CCTV system for any purpose other than those specifically authorised will be subject to a full investigation and could lead to disciplinary action up to and including dismissal without notice.

35.47 The misuse of our surveillance systems and unauthorised use of images and CCTV footage may constitute a criminal offence.

35.48 Any concerns regarding the use of CCTV should be shared with your line manager or the Data Protection Manager.

35.49 The use of CCTV has been subject to a Legitimate Interests Assessment (LIA-02), as set out in Annex A.

36 Dashcams – ROPA REF – RB03

36.1 We intend to use dashcam recording equipment within the operation of the RB in church vehicles and where staff members private vehicles used for business purposes.

36.2 The use of dashcams has been subject to a Legitimate Interests Assessment (LIA-03), as set out in Annex A.

37 Management Gifting Policy – ROPA REF – RB04

37.1 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.

37.2 This policy is governed by the lawful basis of Legitimate Interests.

37.3 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:

- (a) The staff member's line manager will be approached to approve the proposal.
- (b) The gift will be sanctioned based on suitability and price.
- (c) The price will not exceed £50 (fifty pounds)
- (d) The line manager will supervise the dispatch of the gift to the home address of the relevant staff member.

37.4 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.

37.5 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 below.

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.

- 37.6 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.
- 37.7 The Management Gifting Policy has been subject to a Legitimate Interests Assessment (LIA-04), as set out in Annex A.

38 Review and Updating

- 38.1 The RB acknowledges the developing nature of data protection legislation and implements procedures to ensure ongoing compliance.
- 38.2 The RB has established a regular system for review and updating as required.
- 38.3 The **Data Protection Manager** is responsible for arranging reviews of our systems and staff training in line with our established training schedule.
- 38.4 We intend to create a robust system of Data protection by design and by default. We will conduct a Data/Information Audit on a regular basis as required by the regulations and record any updates to these policies.
- 38.5 A Data Audit will be conducted:
- 38.5.1 Regularly and in any event at least annually.
 - 38.5.2 When changes to procedures or processes warrant a Data Processing Impact Assessment (DPIA)
 - 38.5.3 When any other relevant changes are required
 - 38.5.4 The Data Protection staff training schedule is established as follows:
 - (a) Induction – On appointment or re-appointment.
 - (b) Ongoing - On a rolling six monthly basis of knowledge checks and reminders.
 - (c) Updating – As required consequent to changing and developing rules and procedures.
 - (d) Following any personal data breach or regulatory investigation.
- 38.6 Our Data Protection Manager has been authorised to make enquiries of our Legal advisors, if required, in the event of any queries beyond their existing understanding and knowledge.

ANNEX A – LEGITIMATE INTERESTS ASSESSMENTS (LIAs)

This Annex forms part of the Representative Body’s Data Protection Management System (DPMS) and contains all current Legitimate Interests Assessments relied upon by the RB.

This document is maintained as part of the RB’s accountability records and is subject to version control and periodic review.

Each LIA is approved by the Data Protection Manager and is reviewed annually.

LIA REGISTER

Ref	Activity	Lawful Basis	Owner	Ropa Ref.
LIA-01	Video Conferencing	Legitimate Interests	DPM	RB-01
LIA-02	CCTV	Legitimate Interests	DPM	RB-02
LIA-03	Dashcams	Legitimate Interests	DPM	RB-03
LIA-04	Management Gifting	Legitimate Interests	HR	RB-04

LIA-01 – VIDEO CONFERENCING

1. Processing Description

The RB uses third-party video conferencing platforms to facilitate communication between staff, clergy, and stakeholders. In some cases, meetings may be recorded.

2. Purpose Test

Processing is necessary to:

- facilitate efficient communication across geographically dispersed participants;
- support operational and administrative activities;
- reduce the need for travel.

These are legitimate organisational interests.

3. Necessity Test

The RB considers that:

- video conferencing is the only practical method for real-time multi-party communication with visual content;
- alternative methods (e.g. telephone) are insufficient where visual information is required;
- use of such platforms is standard and expected in modern organisational operations.

4. Balancing Test

Nature of Data

Audio, video, and limited identifying information.

Reasonable Expectations

Participants would reasonably expect data processing when joining video calls.

Impact

Limited, as:

- recording is not routine;
- participants are informed where recording occurs;
- alternative participation (e.g. audio-only) may be offered where appropriate.

Risks to individuals

The following potential risks to individuals have been identified

- loss of confidentiality;
- unauthorised access to personal data;
- misuse of personal data;
- distress or loss of privacy.

Safeguards

The RB applies the following safeguards to mitigate identified risks:

- platform security settings configured;
- access controls applied;
- recordings retained only where necessary;
- data handled in accordance with RB policies.
- Access to data is restricted to authorised personnel;
- data is stored securely and protected by appropriate technical measures;
- retention periods are limited;
- staff are trained in data protection requirements;
- policies and procedures govern the use of the data.

These measures reduce the likelihood and impact of identified risks.

5. Proportionality (DUAA)

Processing is targeted, limited, and proportionate to its purpose. No less intrusive method would achieve equivalent outcomes.

6. Conclusion

The RB has determined that processing is necessary, proportionate, and does not override the rights of individuals. Legitimate Interests is therefore an appropriate lawful basis.

7. Approval and Review

Approved by: Data Protection Manager

Date: May 2026

Review Date: May 2028

This assessment will be reviewed periodically and where there is a material change to the processing activity.

LIA-02 – CCTV MONITORING

1. Processing Description

The RB operates Closed Circuit Television (CCTV) systems at its premises to capture visual images of individuals within defined areas.

The system operates on a **passive recording basis**, with footage accessed only where required.

2. Purpose of Processing (Purpose Test)

The purposes of the processing are:

- to ensure the safety and security of staff, visitors, and property;
- to prevent and detect crime;
- to assist in the investigation of incidents;
- to support compliance with health and safety obligations.

These purposes are legitimate organisational interests and align with the RB's duty of care and safeguarding responsibilities.

3. Lawful Basis

The lawful basis for this processing is **Legitimate Interests** under Article 6(1)(f) UK GDPR.

4. Necessity Test

The use of CCTV is considered necessary because:

- visual recording is the only effective means of capturing real-time incidents;
- alternative measures (e.g. manual supervision or written records) would not provide equivalent evidential value;
- the system operates in a targeted manner, covering only relevant areas;
- recording is limited to what is required to achieve the stated purposes.

The RB has determined that the processing is a **proportionate and effective means** of achieving these purposes.

5. Balancing Test

(a) Nature of the Data

The data consists of visual images of individuals. No special category data is intentionally processed.

(b) Reasonable Expectations

Individuals would reasonably expect CCTV monitoring in locations such as workplaces and public-facing premises, particularly where signage is clearly displayed.

(c) Impact on Individuals

The impact on individuals is limited because:

- monitoring is not continuous in a live sense (passive recording);
- cameras are visible and signposted;
- private areas (e.g. toilets, changing areas) are excluded;
- access to footage is restricted and controlled.

(d) Safeguards Implemented

The RB applies the following safeguards:

- clear and visible signage informing individuals of CCTV use;
- restricted access to footage (authorised personnel only);
- retention limits (maximum 90 days unless required for investigation);
- secure storage and password protection;
- audit logging of access and disclosures;
- prohibition on covert monitoring.

(e) Vulnerable Individuals / Safeguarding Context

Where CCTV may capture vulnerable individuals, footage is handled with heightened sensitivity and access is further restricted.

6. Proportionality Assessment (DUAA-Aligned)

The RB has assessed that:

- the processing is **targeted and limited to relevant areas**;
- the benefits of the processing (safety, crime prevention) outweigh the limited intrusion;
- no less intrusive alternative would achieve the same outcomes;
- the processing is **reasonable and proportionate in the circumstances**.

7. Conclusion

The RB has concluded that:

- the processing is necessary for legitimate organisational purposes;
- it does not override the rights and freedoms of individuals;
- appropriate safeguards are in place.

Accordingly, reliance on **Legitimate Interests** is justified.

8. Review and Monitoring

This assessment will be reviewed:

- annually;
- following any significant change to CCTV use;
- following any relevant incident or complaint.

9. Approval

Approved by: Data Protection Manager

Date: May 2026

Review Date: May 2028

LIA-03 – DASHCAMS

1. Processing Description

Dashcams are used in vehicles for the purpose of recording road incidents.

2. Purpose Test

- to ensure accurate recording of incidents;
- to support insurance and legal processes;
- to promote safety and accountability.

3. Necessity Test

- real-time visual recording cannot be achieved without camera technology;
- alternative methods would not provide reliable evidence.

4. Balancing Test

Nature of Data

Video footage in public spaces.

Reasonable Expectations

Individuals in public spaces have a reduced expectation of privacy.

Impact

Low, as:

- footage is not actively monitored;
- retention is limited;
- access is restricted.

Risks to individuals

The following potential risks to individuals have been identified

- loss of confidentiality;
- unauthorised access to personal data;
- misuse of personal data;
- distress or loss of privacy.

Safeguards

- limited retention;
- secure storage;
- controlled access.

5. Proportionality (DUAA)

Processing is limited to what is necessary and is proportionate to safety and evidential purposes.

6. Conclusion

The processing is justified under Legitimate Interests.

7. Approval and Review

Approved by: Data Protection Manager

Date: May 2026

Review Date: May 2028

This assessment will be reviewed periodically and where there is a material change to the processing activity.

LIA-04 – STAFF GIFTING

1. Processing Description

Limited personal data (e.g. home address) may be used to send small goodwill gifts to staff members.

2. Purpose Test

- to support staff wellbeing;
- to maintain positive workplace relationships.

3. Necessity Test

- sending a physical gift requires use of address data;
- access is restricted to line managers via HR.

4. Balancing Test

Nature of Data

Basic contact details.

Reasonable Expectations

Staff may reasonably expect limited use of their data for welfare-related purposes.

Impact

Minimal, as:

- processing is occasional;
- data is not retained beyond use;
- individuals may opt out.

Risks to individuals

The following potential risks to individuals have been identified

- loss of confidentiality;
- unauthorised access to personal data;
- misuse of personal data;
- distress or loss of privacy.

Safeguards

- HR-controlled disclosure;
- deletion after use;

- clear restrictions on use.
- Access to data is restricted to authorised personnel;
- data is stored securely and protected by appropriate technical measures;
- retention periods are limited;
- staff are trained in data protection requirements;
- policies and procedures govern the use of the data.

5. Proportionality (DUAA)

Processing is minimal, controlled, and proportionate to a low-impact purpose.

6. Conclusion

The processing is justified under Legitimate Interests.

7. Approval and Review

Approved by: Data Protection Manager

Date: May 2026

Review Date: May 2028

This assessment will be reviewed periodically and where there is a material change to the processing activity.

ANNEX B – PROVINCIAL SAFEGUARDING TEAM PRIVACY NOTICE

This document is prepared pursuant to Section 39 Schedule 1 Part 4 Data Protection Act 2018.

The Church in Wales committed to maintaining your trust by protecting your personal data. Personal data is any information relating to an identified or identifiable person. The Church in Wales Safeguarding Team, which is part of the Representative Body of the Church in Wales, will process your personal data in a transparent and lawful way.

1. Data controller(s)

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

2. Why we collect and use your personal data

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

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

3. The categories of personal data we collect:

3.1 The types of information we process include:

- personal details
- contact information
- family details
- lifestyle and social circumstances
- employment and education details
- housing needs

We also process “special categories” of information that may include:

- race;
- ethnic origin;

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

We process personal information about:

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

4. The lawful basis for using your information

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

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

4.3 Personal data

- Public task – we may need to process your information where it is necessary to undertake a duty or task in the public interest. In particular, this includes making sure that the provision of services and activities by the Church in Wales is safe for all members of the public and so far as possible assists in upholding the law and preventing the commission of any offences.
- Public task – we may need to process your information in order to undertake tasks and duties which relate to the operational aspects of the Church in Wales and includes sharing and receiving data with and processed by the various bodies and officials which make up the Church in Wales. This includes doing all that we reasonably can to ensure that no member of the public, members of the Church in Wales or anybody who works for or is employed by a legal entity which is part of the Church in Wales, including contractors and office holders, is at risk of harm in connection with the activities of the Church in Wales. See in that regard, the

Church in Wales Safeguarding Policy:

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

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

4.4 Special categories & criminal information

- Substantial public interest (protecting the public against dishonesty etc.) – we may need to process your information for a reason of substantial public interest. In particular, this condition is met where it is necessary for the exercise of a “protective function”, as defined in Schedule 1, Paragraph 11(2) Data Protection Act 2018, including the protection of members of the public generally against seriously improper conduct and from any failures in connection with the Church in Wales’s activities, or for safeguarding purposes.
- Legal claims – we may need to process your information where it necessary to do so for the establishment, exercise or defence of legal claims or in connection with judicial process.
- Archiving - we may process your information for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes including the organisation, preservation of, and controlled access to, segments of the Church’s history.

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

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

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

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

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

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

5.1 Where necessary or required to meet the purposes listed, we may collect from or share information with a number of organisations including:

- parishes, dioceses, bishops and cathedrals
- candidates, prospective employees, employees or other staff members.
- legal representatives, parties and individuals involved in or connected with legal claims, inquiries, reviews and dispute resolution (including mediation and arbitration)

- healthcare, social and welfare organisations, educational institutions and committees
- local and central government, regulatory and statutory bodies, • law enforcement authorities
- courts and tribunals and providers of legal services
- statutory, public, regulatory or other legal or independent reviews or inquiries, including any “lessons learned” reviews

6. How long do we keep your information?

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

7. Complaints or concerns

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

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

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

Appendix: Safeguarding Records - Retention Policy Summary

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

For the purpose of this guidance safeguarding records includes:

- **Allegations/Concerns:** Any information that relates to allegations of abuse by clergy, office holders or members of the Church in Wales or any information that relates to a concern around a risk of potential harm to a child or adult e.g. referral information, advice and guidance offered to parishes, case files and records.
- **Risk Assessments:** Any information that relates to risk assessments and managing risk in church settings.
- **Employment:** Any information that relates to the recruitment, support and training of clergy, office holders and employees in line with good practice in safer recruitment (including information from the Disclosure and Barring Service).

- **Discipline:** Any information that relates to disciplinary action in relation to a member of the clergy, office holder, employee or member of the Church in Wales e.g. clergy personal files, supervision files, personnel files, disciplinary tribunal files, provincial court files.

- **Governance:** Any information that relates to the safeguarding leadership and governance and safeguarding practices and policy e.g. minutes of provincial safeguarding panel, safeguarding advisory group, policy development, training delivery records, Quality Assurance processes and outcomes etc.

This policy covers:

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

Independent Inquiry into Child Sexual Abuse (IICSA)

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

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

1 <https://www.iicsa.org.uk/key-documents/115/download/2018-07-25-guidance-note-retention-instructions-data-protection-requirements-version-2.pdf> This request supersedes any existing retention schedules and policies. All records which may be relevant to the Inquiry should **NOT BE DESTROYED** but must be retained and then should be reviewed after the Inquiry is complete.

Relevant material will include:

- Case work related files
- Case work related referral/enquiries/support and advice
- Risk assessments and agreements
- Quality Assurance information e.g. audits, data returns, action and improvement plans
- Files relating to Education establishments, recruitment and safeguarding
- HR Staff files non clergy: current and leavers
- HR Staff files: Employment tribunal cases
- HR Staffing reviews; HR Staffing reviews (Diocesan Bishop's Staff)
- Clergy Personal files: current and leavers

- Clergy discipline: Discipline case files
- Files on appointments to councils, committees and other bodies
- Files and papers relating to Subject Access Requests
- Safeguarding leadership and governance e.g. Governing Body, Representative Body, Provincial Safeguarding Panel e.g. meeting agenda and minutes
- Details of blemished DBS checks, referrals , update schedules and risk assessments
- Any separate records of allegations/concerns in relation to Church Officers.

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

Retention Schedule – Categories and Retention Periods

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

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

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

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