Document Version 1.1

Data Audit: 4 June 2025

ICO REGISTRATION NO: ZB 908513

OWAIN PRITCHARD

Data Protection Manager

The Bangor Diocesan Board of Finance

Bwrdd Cyllid Esgobaeth Bangor

Data Compliance Document and General Privacy Notice 2025/26

=

Esgobaeth Bangor
The Diocese of Bangor

Contents by Section

PART FOUR – DATA RIGHTS & BREACH POLICIES

PART FIVE – OPERATIONAL AND UPDATING POLICIES

Bangor Diocesan Board of Finance
Bwrdd Cyllid Esgobaeth Bangor

Data Protection Compliance Document

PART ONE of FIVE

DBF OPERATIONAL POLICIES

1 The Bangor Diocesan Board of Finance Contact Details

1.1 The Bangor Diocesan Board of Finance hereinafter referred to as 'the DBF', We, Us and Our.

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

1.3 Data Protection queries may be addressed to us for the attention of The Data Protection Manager at The Bangor Diocesan Board of Finance Cathedral Close Bangor LL57 1RL

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: ZB 908513

2 Status of key personnel

2.1 The Archbishop of Wales, the Most Reverend Andrew John, Chair of Trustees.

2.2 We have designated **Mr Owain Pritchard** as **Data Protection Manager** for the DBF.

3 Introduction and Overview

3.1 The DBF is a charitable institution responsible for promoting and assisting the work and purposes of the Church in Wales and in the Province of Wales generally and in particular in the Diocese of Bangor for the time being and to comply with the rules and regulations of the constitution of the Church in Wales. You can find out more information about us at Home - Diocese of Bangor

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

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

3.4 Pursuant to the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) the DBF 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 DBF's data processing activities; and be able to

demonstrate that it has used or implemented such measures and complied with the data protection principles.

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

(i) Fairly, Lawfully and Transparently.

(ii) for limited purposes.

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

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

(v) in accordance with the prescribed rights.

(vi) for no longer than necessary.

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

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

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

4.1 protect against potential breaches of confidentiality;

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

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

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

5 Definitions

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

(a) Members of the Trustees of the DBF
(b) The Staff, Office and Post Holders of the DBF;
(c) Donors;
(d) Individuals who contact us with enquiries or complaints;
(e) Users of our website;
(f) Individuals who feature in our newsletters or articles;
(g) Individuals who we engage to provide services to us; and
(h) Individuals who engage with us on social media.

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

Staff	means staff members of the DBF and anyone holding an office or post under the Church in Wales when acting for the DBF 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 DBF and includes their agents, employees and representatives as appropriate.
The Cohort	means the individuals listed in Section 5.1
DBF information	means DBF-related information other than personal information regarding clients, suppliers and other DBF contacts of the DBF;
DBF information	means personal data relating to staff, customers, clients and suppliers; and Any other DBF information; and Confidential information. (see below).

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

6 Roles and responsibilities

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

(a) monitoring and implementing this policy;

(b) monitoring potential and actual security breaches;

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

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

7 Scope of the Policy

7.1 The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the DBF, 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 DBF 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 DBF information must be treated as commercially valuable and protected from loss, theft, misuse or inappropriate access or disclosure.

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

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

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

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

9 Information management

9.1 Personal data must be processed in accordance with:

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

(b) this data protection policy generally; and

(c) all other relevant DBF policies.

9.2 In addition, all information collected, used and stored by the DBF 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 DBF will take appropriate technical and organisational measures to ensure that personal data is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage, including:

(a) pseudonymisation of personal data where necessary;

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

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

10 Lawfulness of processing

10.1 There are 6 lawful bases for data processing.

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

10.3 The lawful bases for data processing are as follows:

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

(b) **Contract:** The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the direct request of the data subject prior to entering into a contract.

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

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

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

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

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

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

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

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

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

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

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

(b) if the LIA identifies a significant privacy impact, consider whether we also need to conduct a Data Protection Impact Assessment (DPIA);

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

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

Lawful Bases for Processing – Special Note

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

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

10.8 A non-exhaustive list of such arrangements include:

(a) Stipendiary and Non Stipendiary Clerics
(b) Other Ministry licensed by a Bishop (e.g. LLMs)
(c) Voluntary service within the Church
(d) A range of other posts and offices

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

Special Category Data

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

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

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

(a) we have a lawful basis for doing so as set out above; and
(b) one of the special conditions for processing special category data applies:
    (i) the data subject has given explicit consent;
    (ii) the processing is necessary for the purposes of exercising the employment law rights or obligations of the DBF or the data subject;
    (iii) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;
    (iv) processing relates to personal data which are manifestly made public by the data subject;
    (v) the processing is necessary for the establishment, exercise or defence of legal claims; or
    (vi) for reasons of substantial public interest; or
    (vii) for the purposes of preventive or occupational medicine.

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

11 Data Access Rights

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

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

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

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

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

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

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

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

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

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

12 Data Protection Impact Assessments (DPIAs)

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

12.1.1 whether the processing is necessary and proportionate in relation to its purpose;

12.1.2 the risks to individuals; and

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

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

13 Practical Data Protection Actions

13.1 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.

13.2 All staff must keep personnel information strictly confidential.

13.3 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 DBF's data subject access request policy.

Access to premises and information

13.4 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.

13.5 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.

13.6 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.

13.7 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 DBF information, then steps should be taken to ensure that no confidential information is visible.

13.8 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

13.9 Password protection and encryption must be used where available on DBF computers and systems in order to maintain confidentiality.

13.10 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.

13.11 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.

13.12 Confidential information must not be copied onto floppy disk, removable hard drive, CD or DVD or memory stick/ thumb drive without the express permission of a manager.

13.13 Data held on any of these temporary devices should be transferred to the DBF's computer(s) and/or network as soon as possible in order for it to be backed up and then deleted from the device.

13.14 All electronic data must be securely backed up in accordance with the DBF approved back up schedule.

13.15 Staff must ensure they do not introduce viruses or malicious code on to DBF systems.

13.16 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

13.17 Care must be taken about maintaining confidentiality when speaking in public places, e.g. when speaking on a mobile telephone.

13.18 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 DBF.

13.19 Confidential information must not be removed from the DBF's offices unless required for authorised DBF purposes.

13.20 Where confidential information is permitted to be removed from the DBF'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

13.21 Postal and email addresses and numbers should be checked and verified before information is sent to them.

13.22 Particular care should be taken with email addresses and attention paid to avoid opportunities for auto-complete features to insert incorrect addresses.

13.23 All sensitive or particularly confidential information should be encrypted before being sent by email.

13.24 Further details regarding data security and how documents and emails should be protected are set out in the DBF's data security, transfer, storage and retention policy.

13.25 Staff members must not use a personal email account or cloud storage account for work purposes.

Data Transfer to third parties

13.26 Third parties should be used to process DBF 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.

13.27 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

13.28 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.

13.29 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)

13.30 All members of staff have an obligation to report actual or suspected Data Subject Access Requests (DSARs). This allows the DBF to:

(a) Respond to the request as required by law; and

(b) maintain a register of requests;

13.31 Please refer any suspected DSAR to the **Data Protection Manager** for immediate action.

Reporting data breaches

13.32 All members of staff have an obligation to report actual or potential data protection compliance failures. This allows the DBF to:

(a) investigate the failure and take remedial steps if necessary;

(b) maintain a register of compliance failures; and

(c) make any applicable notifications.

13.33 Please refer any suspected data breach to the **Data Protection Manager** for immediate action.

14 International data transfers

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

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

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

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

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

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

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

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

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

14.9.1 We are not a public authority; and

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

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

Bangor Diocesan Board of Finance
Bwrdd Cyllid Esgobaeth Bangor

Data Protection Compliance Document

PART TWO of FIVE

DATA CONTROL POLICIES

15 Personal Data under our control

TRUSTEES OF THE BANGOR DIOCESAN BOARD OF FINANCE

15.1 Data under control analysis chart:

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

Consequences of not providing your data

15.1.1 If your name and contact details are not provided you will be unable to act as a Trustee of the DBF 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

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

CLERGY AND FORMER CLERGY INCLUDING LLMs

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

Personal Data	Lawful Base(s)	Retention Period	Source of Data Use of Data & Data Sharing
Your name; Your contact details (such as your postal address, telephone number and/or email address); Your Date of Birth; Your National Insurance number and tax code Your bank details, payroll details and tax status information Your salary, honorarium, pension and benefits details Your Bank Account Details; Your Date of Ordination; Information relevant to the provision of a house for duty; Details of any disciplinary matter; Health information; Any other information recorded on the Infonet;	**Public Task** We will use your name and contact details to correspond with you in relation to Church in Wales relevant DBF; We will use your National Insurance number, tax code, bank details, payroll details and tax status information to pay you any salary or honorarium and for benefit and pension purposes; We will use your Personal Data to deal with any disciplinary and/or grievance issues which may arise relating to you or in respect of which you may be able to provide relevant information; We will use your Personal Data to assist the Bishop with making and managing your appointment; We will use your Personal Data to provide you with a house for duty and for administrative purposes in relation to such house; We will collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.	We will keep your Personal Data for as long as you are engaged by us and for a period of up to 70 years after your death. The reasons for keeping your personal data for this length of time include to comply with HMRC requirements and because some claims can be brought up to 6 years after your engagement ends. For these purposes you remain engaged by the us if you are a member of a Church in Wales pension scheme. DBS disclosure results will ordinarily be destroyed within six months of receipt. Your personal file will contain a pro-forma that will indicate the date of receipt of the DBS disclosure information and whether results were acceptable. In the event that the disclosure result highlights concerns relating (in the view of our Safeguarding Manager) to safeguarding of children and/or adults at risk, a record of the disclosure results will be retained securely by our Safeguarding Team indefinitely.	His Majesty's Revenue and Customs (HMRC) in connection with your pay and benefits Banks and other financial institutions in connection with your pay and benefits Payroll provider to enable us to pay your expenses, grants etc. 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. Further biographical information and contact details will only be included with your consent. We will publish some Personal data of Clerics so the public can contact them for pastoral support and to promote their Ministry. Such data will be published on the Church in Wales Website and will include: 1. Name and 2. Church in Wales Email Address. Other Personal Data such as Postal Address and Telephone number may be published after discussions with the individual Cleric.

Your connection with the Church in Wales (which will reveal your religious beliefs); Information about criminal convictions.	**Legal Obligation** We carry out DBS checks on behalf of other parts of the Church in Wales, such as on behalf of the Bishops or Diocese. The information obtained will be used by us in conjunction with other parts of the Church in Wales to determine whether to engage you. This is because the Church in Wales has a Legal Obligation to take all reasonable precautions to ensure that the Church is a safe place for all. We will only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary for reasons of substantial public interest, namely, safeguarding, preventing or detecting unlawful acts, protecting the public against dishonesty, preventing fraud or suspicion of terrorism or money laundering. DBS Checks are part of an automated decision making process pursuant to Article 22 UK GDPR. The information provided by the DBA service is used to assess suitability for employment or appointment to a post. **Special Category Data** If and to the Extent our processing of your Personal Data reveals your religious beliefs, our processing of that Special	Information on your clergy personal file pertaining to your ministry is kept until 70 years after your death for your assistance, to comply with the Church's safeguarding requirements, and for historical purposes. Our policy in respect of Clergy personal files, including a retention schedule policy, is available separately on our website.	

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

Consequences of not providing your data

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

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

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

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

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

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

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

15.2.6 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.

15.2.7 Such information will be retained in accordance with the Church in Wales Clergy Files policy regarding retention of Personal Data.

FULL & PART TIME STAFF MEMBERS OF THE DBF

15.3 Data under control analysis chart for **Staff Members**.

Personal Data	Lawful Base(s) and Statutory authority	Retention Period	Source of Data Use of Data & Data Sharing
Your name; Your contact details (such as your postal address, telephone number and/or email address); Next of kin/Family data for contact in an emergency Your Bank Account details (if in a paid post); Your role with the Church in Wales (which may reveal your religious beliefs); Access to your data via the Computer Monitoring Policies. See below	**Consent** We may process data with your consent such as in the early stages of applying for a role. **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. **Public Task** Use of your Personal Data for administrative purposes, to ensure the smooth and proper running of the Church. **Special Category Data** 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. Where DBS Checks are conducted they are part of an automated decision making process pursuant to Article 22 UK GDPR. The information provided by the DBS service is used to assess suitability for appointment to a post.	Your contact details will be retained for the duration of your employment and for 7 years thereafter. DBS disclosure results will ordinarily be destroyed within six months of receipt. In the event that the disclosure result highlights concerns relating (in the view of our Safeguarding Manager) to safeguarding of children and/or adults at risk, a record of the disclosure results will be retained securely by our Safeguarding Team indefinitely.	Your personal data will usually be provided to us by you directly We will share your contact details with other departments within the RB for specific admin matters including training. We will use your bank account details to pay your wages and any expenses due; 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. The information obtained will be used by us in conjunction with other parts of the Church in Wales to determine whether to engage you. Information about criminal convictions will be obtained from the Disclosure and Barring Service ("DBS") if you have agreed to undertake a DBS check through the Church in Wales. 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. A list of these third parties is available on request.

	Legal Obligation We will only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary for reasons of substantial public interest, namely, safeguarding, preventing or detecting unlawful acts, protecting the public against dishonesty, preventing fraud or suspicion of terrorism or money laundering. This is because the Church in Wales has a Legal Obligation to take all reasonable precautions to ensure that the Church is a safe place for all. 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. **Legitimate Interest** This lawful basis is used for our CCTV systems and when staff members use Video conferencing software. (see separate legitimate interest assessments)		

Consequences of not providing your data

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

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

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

OFFICE HOLDERS AND POST HOLDERS

15.4 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
Your name; Your contact details (such as your postal address, telephone number and/or email address); Your Bank Account details (if in a paid post); Your connection with the Church in Wales (which will reveal your religious beliefs);	**Public Task** Use of your Personal Data for administrative Purposes, to provide you with relevant papers and documents and to share with other members of various committees is part of the proper running of the Church in Wales. Listing your name on the provincial website as an office/post holder will be done pursuant to your role. **Special Category Data** If and to the extent processing your Personal data reveals your religious beliefs, our processing of that information will be carried out because you have manifestly made the information public in accepting the role within the Church in Wales. Where DBS Checks are conducted they are part of an automated decision making process pursuant to Article 22 UK GDPR. The information provided by the DBS service is used to assess suitability for appointment to a post. **Legal Obligation** We will only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary for reasons of substantial public interest, namely, safeguarding, preventing or detecting	Your contact details will be retained for the duration of your office and for 7 years thereafter. Your name and your period of office will be retained indefinitely for historical research purposes. DBS disclosure results will ordinarily be destroyed within six months of receipt. In the event that the disclosure result highlights concerns relating (in the view of our Safeguarding Manager) to safeguarding of children and/or adults at risk, a record of the disclosure results will be retained securely by our Safeguarding Team indefinitely.	Your personal data will be provided to us either by you directly or by the relevant Diocese and or Bishop. We will share your contact details with other members of the committee or body you are an office holder of to enable members to contact each other to discuss Church in Wales DBF. We will record your name and the fact that you were an Office/Post Holder of the Church in Wales and the dates of your period of office for historical research purposes. We will use your bank account details to pay you any expenses due; We will use your Personal Data to provide you with information relevant to your office, such as meeting papers and issues for discussion at committee meetings. We will collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. We carry out DBS checks on behalf of other parts of the Church in Wales, such as on behalf of the Bishops or Diocese. The information obtained will be used by us in conjunction with other parts of the Church in Wales to determine whether to engage you. Information about criminal convictions will be obtained from the Disclosure and Barring Service (“DBS”) if you

	unlawful acts, protecting the public against dishonesty, preventing fraud or suspicion of terrorism or money laundering. This is because the Church in Wales has a Legal Obligation to take all reasonable precautions to ensure that the Church is a safe place for all **Archiving** Keeping a record of your name and the dates you held an office or post in the Church in Wales is necessary for historical research purposes and is in the public interest.		have agreed to undertake a DBS check through the Church in Wales.

Consequences of not providing your data

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

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

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

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

DONORS INCLUDING GIFT AID

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

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

Consequences of not providing your data

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

INDIVIDUALS WHO CONTACT US WITH ENQUIRIES/COMPLAINTS

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

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

Consequences of not providing your data

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

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

INDIVIDUALS WHO FEATURE IN OUR NEWSLETTERS OR ARTICLES

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

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

Consequences of not providing your data

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

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

INDIVIDUALS WHO WE ENGAGE TO PROVIDE SERVICES TO US

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

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

Consequences of not providing your data

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

ADDITIONAL PROCESSING AND LAWFUL BASES

15.9 Data Processing under Legitimate Interests.

15.10 We use the Lawful Base of Legitimate interest sparingly and only when no other basis exists for processing the Personal Data in question.

Personal Data	Lawful Base(s)	Retention Period	Data Sharing
People identified via proprietary Video Conference software	**Legitimate Interests**	Until Legitimate Interest no longer exists or 3 months if recorded	Data is only shared with our authorised Data Processors
People identified through our CCTV systems.	**Legitimate Interests**	Until Legitimate Interest no longer exists or 3 months Max.	Data is only shared with our authorised Data Processors
People identified through our Dashcam Equipment	**Legitimate Interests**	Until Legitimate Interest no longer exists or 3 months Max.	Data is only shared with our authorised Data Processors.

16 Sharing Your Personal Data with others

16.1 SERVICE PARTNERS

Information about our service partners	Suppliers and sub-contractors; Suppliers of IT products and services; We haven't included the names of our service partners in this privacy notice because we will deal with different providers from time to time. However, if you would like further information about any of our current service providers, please contact us using the contact details provided above.
Why we need to share your Personal Data	We use suppliers and sub-contractors to perform certain aspects of our contracts. For example, providing maintenance services; We use suppliers of IT products and services in connection with the supply, maintenance and/or improvement of our IT network.
The legal grounds we rely upon	The sharing of your personal data with suppliers and sub-contractors is necessary for the performance of our **Contract** with them; The sharing of your personal data 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.

16.2 OTHER PARTS OF THE CHURCH IN WALES

Information about the different parts of the Church in Wales	Information about the structure of the Church in Wales can be found at www.churchinwales.org.uk .
Why we need to share your Personal Data	where it is necessary in the course of the work and activities of the Church in Wales, for example: sharing details of an inquiry or complaint with the applicable Parish or Diocese;
The legal grounds we rely upon	We will share Personal data with other parts of the Church in Wales when: We have a **legal Obligation** to do so. It is necessary for the performance of a **Contract** It is carried out in the course of the proper running and management of the Church in Wales under the lawful basis of **Public Task**. Where the other part of the Church in Wales is a legal entity in its own right and our data sharing with them is not based on the proper running of the Church under **Public Task** then we will share details with them based on their data protection compliance and our Data Controller/Processer agreements with them as applicable
What precautions do we take?	Personal data is only shared within the Church in Wales where this can be done fairly and lawfully, in accordance with the data protection principles and data protection laws. A Data Sharing agreement has been agreed between the Dioceses. To this end the Church in Wales aims to ensure; that only personal data that needs to be shared in connection with the operations and activities of the Church is shared; that personal data is only shared when it is necessary and appropriate to do so; that personal data is shared on a 'need to know' basis and is not shared more widely than is necessary; and that personal data is shared securely.

16.3 OTHER THIRD PARTIES

Legal or regulatory requirements	On occasion, we may be required to disclose your Personal Data to organisations such as regulatory bodies, the courts and the police to comply with legal obligations we are subject to and/or to prevent fraud or crime. Also to other organisations such as the courts, the police, regulatory bodies, credit reference agencies and/or debt collection and tracing agents;
Protecting our interests	We may need to disclose your Personal Data in connection with steps we need to take to protect our interests or property. For example, a default with payment, we may disclose your Personal Data to credit reference agencies or debt collection or tracing agents.

Professional advice and legal action	We may need to disclose your Personal Data to our professional advisers (for example, our lawyers and accountants) in connection with the provision by them of professional advice.
Use of Proprietary Software and Online Services. **Eg. Survey Monkey, Mailchimp or similar services.**	From time to time we may use proprietary software/Services for operational purposes to assist in future planning for Church activities. Such software may be used to gather opinions for the assessment of future proposals; to manage our response to developing technology; evaluate the viewpoint of individuals both within the Church and with the Public to various proposals related to Church matters. The software/service used may generate electronic surveys to be distributed to interested parties under the lawful basis of Public Task. This type of software/service will not be used as marketing activity on behalf of the DBF. There is no commercial element to their use, so they do not activate the restrictions on marketing pursuant to the Privacy & Electronic Communications Regs 2003. The communications in these cases may be sent via email/post or text messaging. The retention of this data is likely to be relatively short lived. Generally, the data collected, once evaluated will be kept for no longer than 12 months.

16.4 Below is a chart showing all the organisations and individuals with whom we may share data.

Processor	Processor
Representative Body of the Church in Wales	**Bright HR (Peninsula)**
Bangor Cathedral	**Fresh Desk**
Microsoft Teams	**GoDaddy**
Social Media: Linkedin/WhatsApp FB/Tik Tok/Twitter/Snapchat/Instagram	**G-suite**
Mailchimp	**AI – ChatGPT**

Engaging with us on Social Media

16.5 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.

16.6 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.

16.7 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.

17 Types and Categories of Personal Data

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

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

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

17.4 **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.

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

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

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

18 Children's Personal Data

18.1 We do not contract with children to provide products or services.

18.2 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.

18.3 We may record details of children if relevant and appropriate to our Church based activity or for the purposes of giving advice and we may subsequently reference the children in our records.

18.4 In all cases where a child is under 13 years, we will obtain parental consent to record the child's details in our records, unless there is some other lawful basis prevailing upon the circumstances, such as legal obligation in Safeguarding matters.

18.5 There is nothing on our Website which could be damaging to children who view the pages or the pictures. Our Products and Services are not made available to children under 18 years.

Bangor Diocesan Board of Finance
Bwrdd Cyllid Esgobaeth Bangor

Data Protection Compliance Document

PART THREE of FIVE

PROCEDURAL POLICIES

19 Human Resources and Payroll

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

19.1.1 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.

19.1.2 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.

19.1.3 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.

19.1.4 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.

19.2 Recruitment

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

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

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

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

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

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

19.3 Payroll Matters

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

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

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

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

20 Staff Home Working Policy

Introduction

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

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

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

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

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

Security and Confidentiality of Materials

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

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

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

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

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

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

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

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

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

20.15 Work should only be completed on DBF approved systems and applications.

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

20.17 Any DBF Personal Data downloaded to a personal device must be deleted as soon as possible.

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

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

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

Loss or Theft

20.21 In the event that a device, whether personal or DBF owned, is lost, stolen or its security is compromised, you MUST immediately, or if out of hours within an hour of the DBF reopening the next working day, report this to the **Data Protection Manager**, in order

for them to assist in changing passwords to all DBF services, considering the extent of the loss and reporting as a data breach if appropriate.

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

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

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

Approval for Working remotely

20.25 Home and/or Remote working must not begin until authorised by the DBF.

20.26 Applications to begin Home/Remote working should be made in writing to your line manager who will consider requests for home working in consultation with Human Resources.

21 Generative AI Policy

21.1 The DBF recognises the potential of artificial intelligence (AI) to transform the way we work, improve the services we provide and our competitiveness.

21.2 We are committed to ensuring we use AI tools in a secure and responsible way, respecting confidentiality and third party rights. This includes any AI tools used by third parties on our behalf.

21.3 This policy provides guidance to staff on using and deploying generative AI tools in the course of your work, the circumstances in which we will monitor use of generative AI, and the action we will take if this policy is breached. It should be read in conjunction with other policies that are relevant to the use of AI in the workplace, eg:

21.3.1 data protection policy

21.3.2 information security policy

21.3.3 Internet Email and Communications policy

21.4 This policy applies to all individuals, including employees, workers, temporary and agency workers, contractors, interns, volunteers and apprentices (referred to as 'staff' in this policy).

21.5 We will review and update this AI policy regularly to take account of changes in technology, legal obligations and best practice. We will circulate any new or modified policy to staff when it is adopted.

21.6 The Data Protection Manager is responsible for monitoring and implementing this policy. If you have any questions or comments on this policy, please contact the Data Protection Manager.

What is meant by Generative AI?

21.7 There is no single definition of artificial intelligence (AI). Broadly speaking it is the simulation of human intelligence in machines, generally computer systems.

21.8 AI tools can learn, problem-solve, make decisions, and understand language. This can be contrasted with non-AI pre-programmed tools, which generally apply the same set of rules each time unless a human intervenes to update the rules. An AI tool can learn and adapt without human intervention.

21.9 There are several types of AI, including generative, predictive and extractive:

Generative AI	An AI tool that *generates* new, realistic content in the form of text, audio, computer code, data or images etc For example, using an AI tool to: —generate a marketing blog post —improve an email you have already written —write a product description or a job description —write a script or slides for a presentation —check, amend and improve your grammar, spelling and writing style —summarise a report or large block of text —power sophisticated chatbots, or —write software code or find common bugs in code
Predictive AI	An AI tool that analyses data to make *predictions*, eg about: —customers' buying behaviour, or —how busy the office will be at any particular time
Extractive AI	An AI tool that *extracts* data from the dataset it has been trained on (but can't create data)

21.10 This policy focuses on generative AI but it also applies more broadly to all forms of AI used for DBF purposes. *eg ChatGPT and Microsoft Copilot* are examples of generative AI providers.

AI guiding principles

21.11 Our responsible AI approach means that we:

(a) consider the real-world impact of any AI that we may use or develop;

(b) take action to avoid the creation or reinforcement of bias;

(c) can explain how the AI we use works;

(d) create accountability through audit, governance and human oversight; and

(e) respect privacy and champion robust data governance.

Potential benefits of using AI in the workplace

21.12 Generative AI can be an efficient tool for producing text, images or code quickly and to a specification.

21.13 Generative AI provides opportunities for efficiencies, eg *when used in brainstorming ideas or creating a first draft.*

21.14 AI has the potential to improve productivity, personalise the customer experience and accelerate product/service developments. It may be capable of completing repetitive, manual high-volume tasks, freeing up our staff for more interesting value-added work.

Potential risks of using generative AI in the workplace

21.15 To understand the potential risks of using AI in the workplace it is helpful to understand how generative AI tools are trained and how they work.

21.16 Generative AI tools are trained on colossal banks of existing content from various sources, called datasets. They learn to identify patterns in those datasets. The more advanced generative AI tools are able to identify those patterns without human intervention or supervision. Some generative AI tools will then use additional input or prompt data and feedback from users to continue to self-train (a prompt is a question or request you write for the AI tool to answer or solve).Text-generating AI tools often work by selecting the most-likely next word in a sentence and the one after that (to create text), whereas image-generating AI tools often work by selecting the next pixel.

21.17 This raises several questions including:

(a) can the generative AI tool reuse, recycle or republish information we input—and make that information available for other users, directly or indirectly?

(b) do we have the right or permission to put information that belongs to someone else into the AI tool, eg confidential information, personal data or copyright material belonging to someone else?

(c) who owns the intellectual property (eg the copyright) in the text (or image/code) produced by the AI tool?

(d) can we rely on the accuracy of the text or results generated by the AI tool?

(e) are there any other risks, eg biases in the data that the AI tool was trained on that might cause it to discriminate?

21.18 Some of these AI risks are overlapping and the following sections expand on the main themes.

Privacy and confidentiality risks

(a) Generative AI tools can exacerbate data and privacy risks.

(b) Data protection law requires that we must have a lawful ground for collecting and using personal data. However, the lawful ground on which we originally collected personal data may not cover us for using that data in a generative AI tool. Unless additional consent is obtained, entering that personal data into a publicly-accessible generative AI tool (which can store the information indefinitely, recycle and reuse it) is likely to constitute a data protection breach.

(c) Likewise, using publicly-accessible generative AI tools runs the risk of exposing DBF-owned (proprietary) information.

Intellectual property (IP) and trade secrets

(d) AI tools can increase the risk that our IP and trade secrets will be improperly disclosed. Most publicly-accessible AI tools don’t guarantee the information you input into the tool will not be used to train the AI model. This means our IP could be reproduced or made available to other users in some form.

(e) AI-generated content may also infringe IP owned by third parties, particularly copyrights. This is effectively the same risk as above, but in reverse, ie we put third party information into an AI tool without proper licence, thereby breaching the third party's IP. This could be information belonging to a customer, supplier or party completely unconnected to the DBF.

(f) There is also an indirect risk where our IP is shared with third-party suppliers, eg marketing agents. While we must take care to avoid inputting our valuable IP into an AI tool, we must also ensure that our third-party providers do not do exactly that with our IP, eg to produce marketing collateral.

Accuracy

21.19 Where generative AI does not have the information to provide the information you have requested, it may still attempt to provide you with an output. It could do this by simply making things up (or 'hallucinating').

(a) Relying on a response or text produced from an AI tool without checking could have a range of negative outcomes including damage to our reputation.

(b) As well as the risk of hallucinations, the output of an AI tool may not be guaranteed to be 100% accurate. Generally speaking, accuracy in AI refers to how often the AI system guesses the correct answer, measured against correctly labelled test data. This is known as statistical accuracy.

(c) In many cases, the outputs of an AI system are not intended to be treated as factual information, eg about an individual, but rather a statistically informed guess as to something which may be true about the individual now or in the future. Where this is the case, it is important that we do not misinterpret the AI as being factually or statistically accurate.

Bias

(d) Another concern with generative AI (and other forms of AI) is the potential for bias to be embedded within the AI tool. This bias can then be perpetuated as the AI tool operates and develops, inadvertently leading to the creation of discriminatory content or decisions. This is not necessarily deliberate, the AI tool may simply be reflecting the unconscious bias of its creators or other users.

(e) There are two main potential sources of bias—the data itself and the algorithm applied to the data by the AI tool:

(i) if the data used to train a generative AI tool is biased (eg towards a particular race or gender), the AI tool is likely to produce biased content; whereas

(ii) if bias is embedded into the AI algorithm (the coded instructions that tells the AI tool how to function), the output is likely to be biased even if the data itself is not biased.

Who may use generative AI for work purposes and when?

21.20 Access to internal and publicly-accessible AI tools, platforms or related systems is restricted to authorised staff only..

21.21 You must not download and/or use third party add-ins without approval from your line manager.

Guidelines for staff on using generative AI tools and platforms

21.22 If you wish to use another generative AI tool, you should contact the Data Protection Manager to ask whether you can be given authority to use it.

21.23 You must not share your access credentials or allow others to use generative AI tools on your behalf.

21.24 You must not use generative AI in any way that could be considered discriminatory, or could give rise to defamation, harassment, intimidation or bullying or in any way that could harm the reputation of another.

21.25 You must not use generative AI to create illegal content or for illegal purposes.

21.26 You must not use offensive, obscene or abusive language, graphics or imagery when inputting content into generative AI and must not attempt to create content which is offensive, obscene or abusive through your use of generative AI tools.

21.27 Unless specifically authorised to do so, you must not input into a publicly-accessible generative AI tool:

(a) the DBF's trademarks, brands, logos or any other identifying material;

(b) the DBF's name, email or other contact details (other than where required to input your work email address);

(c) proprietary DBF information;

(d) customer or supplier materials, information or data;

(e) trade secrets, confidential or valuable information;

(f) usernames, passwords (other than for the AI tool itself), and security tokens; or

(g) personal data, ie information or data from which any living individual can be identified—including personal data relating to employees, customers, suppliers and unconnected third parties.

This includes inputting data as training data to a generative AI technology or in any instruction or prompt (a question or request that you write for the generative AI tool to answer or solve).

21.28 When using generative AI in the workplace, you must always use your Church in Wales email address to create and log in to any generative AI account (do not use your personal email address or login credentials).

21.29 You must not in any way provide or suggest any endorsement or recommendation by the DBF of any third party generative AI technology.

21.30 You must protect your login credentials and ensure any generative AI accounts that you hold are not accessible to unauthorised third parties. The use of multi-factor authentication is advised in respect of any generative AI tools and technologies used.

21.31 Your use of generative AI in the workplace must be limited to DBF-related purposes and should, at all times, be in accordance with all applicable laws (including data protection and privacy laws).

21.32 You are responsible for ensuring the generated content aligns with our values, ethics and quality standards. Before using any AI generated content, you must carefully review it and ensure you do not use content that:

(a) discloses confidential or proprietary DBF information without approval from your line manager;

(b) reveals personal data about any individual, without approval from your line manager;

(c) has the potential to breach the intellectual property rights of a third-party;

(d) is misleading and/or cannot be verified;

(e) is discriminatory, otherwise biased or offensive.

21.33 You must comply with the terms and conditions of the generative AI technology that you use, unless such terms and conditions are in conflict with or contradict our policies or your terms of employment, in which case you should seek advice from your line manager.

Personal use of generative AI

21.34 You may make reasonable use of generative AI tools for personal use using the DBF's computers, networks and/or systems (including via smartphones or tablets), provided use is minimal and takes place substantially out of normal working hours (ie during your lunch break or before or after work), it does not interfere with your duties and DBF and office commitments and is strictly in accordance with this policy.

21.35 Any unauthorised use of generative AI is strictly prohibited. Permission to use the DBF's systems to access generative AI tools for personal use may be withdrawn at any time at the DBF's discretion.

Monitoring

21.36 Our internet, email and communications policy applies to the use of generative AI technologies via the DBF's systems or network, in particular in relation to the DBF's right to monitor, intercept and read communications.

21.37 We will also monitor how our supplier's and customers use generative AI generally and any use of DBF information or information concerning the DBF by them or by our competitors.

Responsibility for compliance

21.38 All employees are responsible for ensuring their own use of generative AI is in accordance with this policy, and must, in particular, make themselves aware of, and

comply with, their responsibilities, as outlined in this policy, to protect confidential and sensitive information when using generative AI.

21.39 Managers and supervisors are responsible for ensuring their teams are aware of and comply with this policy and they must report any breach of this policy to the Data Protection Manager.

21.40 The Data Protection Manager is responsible for handling any complaints concerning violation of or non-compliance with this policy, including any allegations of harassment, discrimination, or bias that may be raised by employees, customers, suppliers or other third parties.

Breaches of this policy

21.41 Because of the importance of this policy, failure to comply with any requirement of it may lead to disciplinary action and this action may lead to dismissal for gross misconduct. If you are not an employee, breach of this policy may result in termination of your contract with immediate effect.

21.42 You should note in particular that inputting DBF materials, data or information, including commercially sensitive or confidential information, to generative AI tools may amount to misconduct even if it takes place:

(a) on a personal account with appropriate privacy settings;

(b) outside normal working hours; and/or

(c) without using the DBF's computers, systems and networks.

21.43 If, in the course of your employment, you become aware of any misconduct or wrongdoing by any employee, officer, worker or agent of the DBF in breach of this or related policies, you must report it to your line manager.

21.44 You must also make a report to your line manager if you become aware that:

(a) a customer or supplier has input confidential or proprietary DBF information or personal data relating to any of our staff into a publicly-accessible AI tool; or

(b) a publicly-accessible AI tool has otherwise produced output that includes confidential or proprietary DBF information or personal data relating to any of our staff;

(c) we may have used an AI tool in a way that infringes IP owned by third parties or infringes the data protection rights of a third-party, whether deliberately or inadvertently.

21.45 Staff who feel that they have been harassed, bullied or defamed because of material created or generated through the use of generative AI by a colleague should inform their line manager.

22 Internet, Email and Communications Policy

22.1 The DBF recognises that the use of email and the internet can save time and expense, and is an important part of the way we work. However, it brings with it certain risks, some of which may involve potential legal and financial liabilities for both the DBF and the individual, eg:

(a) inadvertently entering into contracts or commitments on behalf of the DBF;

(b) introducing viruses into the DBF's systems;

(c) breaching copyright or licensing rights;

(d) breaching data protection rights;

(e) breaching confidentiality and security;

(f) defamation; and/or

(g) bullying, harassment and discriminatory conduct.

22.2 This policy aims to guard against those risks. It is therefore important that all staff read the policy carefully and ensure that they use the internet, email and other communication systems in accordance with it. If you are unsure whether something you are about to do complies with this policy, you should seek advice from your line manager.

22.3 This policy also explains when we will monitor the use of email and the internet and the action we will take if the terms of this policy are breached.

22.4 References in this policy to 'email' apply equally to other electronic communications, messaging tools and posts.

Scope

22.5 This policy applies:

(a) to all staff, including employees, workers, temporary and agency workers, interns, volunteers and apprentices, and to consultants and other contractors who have access to our computer and other communications systems;

(b) to personal use of our systems and equipment in any way that reasonably allows others to identify any individual as associated with the DBF;

(c) to the use of our email, telephone and internet systems both in the workplace and from outside it, eg via remote access, and to the use of a DBF laptop, tablet, mobile phone, smartphone or personal digital assistant (PDA).

22.6 You must familiarise yourself with this policy and comply with its terms.

22.7 You should also refer to our data protection policy and data protection privacy notice and, where appropriate, to our other relevant policies including in relation to generative AI.

Use of the DBF's computer systems

22.8 You may use our computer systems (including equipment) for authorised purposes only. If you wish to use the DBF's systems or equipment for another purpose, you must obtain express permission from your line manager before doing so.

22.9 To reduce the risk to the DBF's systems or network of virus infections, hacking and other unauthorised access attempts, you may only access the DBF's systems and network as follows:

22.9.1 from your workplace or other DBF premises, using authorised equipment only;

22.9.2 remotely (via broadband, dial up, etc, using authorised equipment via secure means, eg VPN software only; or

22.9.3 remotely, using unauthorised equipment, eg your home computer or an internet café terminal, providing sufficient security arrangements are in place to protect your activity.

22.10 You must not use any software owned or licensed by the DBF for any purpose other than those of our DBF without express permission from your line manager or as otherwise permitted by the terms of this policy, and you must not copy, download or install any software without first obtaining express permission from your line manager.

Email use—general

22.11 All communications, including email, should reflect the highest professional standards at all times. In particular, you must ensure:

(a) messages are brief and to the point;
(b) emails are checked before sending, including spelling and grammar;
(c) all emails sent from the DBF include the current disclaimer wording;
(d) ensure that an appropriate heading is inserted in the subject field; and

check the recipient(s) before pressing the send button—not only can it be embarrassing if a message is sent to the wrong person, it can also result in the unintentional disclosure of confidential information about the DBF, a client/customer or other third parties, which may be a data breach.

22.12 You must not send messages from another person's email address (unless authorised in the proper performance of their duties), or under an assumed name.

22.13 You must not send or post messages or material that are offensive, obscene, defamatory or otherwise inappropriate in the work environment.

22.14 You must not send or post any message or material which could be regarded by the recipient or any other person as personal, potentially offensive or frivolous.

22.15 You should not send or post anything in an email that they would not be comfortable writing (or someone else reading) in a letter. Emails leave a retrievable record and, even when deleted, can be recovered from our back-up system or an individual's

computer. They are admissible as evidence in legal proceedings and have been used successfully in libel and discrimination cases, and they can also be reviewed by regulators.

22.16 You must not create congestion on the DBF's systems or network by sending trivial messages, by unnecessary copying or forwarding of messages to recipients who do not need to receive them, or by sending or forwarding chain mail, junk mail, cartoons, jokes or gossip.

22.17 You must use a DBF email address for sending and receiving work-related emails and must not use your own personal email accounts to send or receive emails for the purposes of our DBF. You must not send (inside or outside work) any message in our name unless it is for an authorised, work-related purpose.

22.18 You must not send unsolicited commercial emails to anyone with whom you do not have a prior relationship without the express permission of the relevant manager.

22.19 You must be vigilant when using our email system. Computer viruses are often sent by email and can cause significant damage to the DBF's information systems or network. Be particularly cautious in relation to unsolicited emails from unknown sources.

22.20 If you suspect that an email may contain a virus, you should not reply to it, open any attachments to it or click on any links in it and must contact your line manager immediately for advice.

Emails—confidentiality

22.21 Do not assume that emails sent or received internally or externally are private and confidential, even if marked as such. Email is not a secure means of communication and third parties may be able to access or alter messages that have been sent or received. Do not send any information in an email which you would not be happy being publicly available. Matters of a sensitive or personal nature should not be transmitted by email unless absolutely unavoidable and if so, should be clearly marked in the message header as highly confidential.

22.22 Lists of contacts compiled by you during the course of your employment and stored on our email application, information manager and/or other database(s) (irrespective of how they are accessed) belong to us. You must not copy or remove such lists for use outside your employment or after your employment ends.

Emails—personal use

22.23 Although the email system is primarily for DBF use, we understand that you may occasionally need to send or receive personal emails while at work.

22.24 The sending of personal emails using the work email address is therefore permitted. When sending personal emails using the work email address, you should show the same care as when sending work-related emails.

22.25 Reasonable personal use of our systems or network to send personal email is also permitted, provided that it does not interfere with the performance of any individual's duties and the terms of this policy are strictly adhered to. We reserve the right, at our absolute discretion, to withdraw this privilege at any time and/or to restrict access for personal use.

22.26 Personal use must meet these conditions (in addition to those set out elsewhere in this policy):

(a) it must be minimal (both in terms of time spent and frequency) and reasonable and must take place mainly outside normal working hours, ie during lunch or other breaks, or before and after work;

(b) personal emails must be labelled 'Personal' in the subject header and in the sensitivity settings;

(c) personal use must not affect the job performance of you or your colleagues, or otherwise interfere with our DBF; and

(d) it must not commit us to any marginal costs.

Emails—monitoring

22.27 We may monitor the email and instant messaging systems or network in the workplace for the following reasons:

(a) to determine whether they are communications relevant to the carrying on of our DBF;

(b) if you are absent from work, to check communications for DBF calls to ensure the smooth running of the DBF;

(c) to record transactions;

(d) where we suspect that messages being sent or received are:

(e) detrimental to the DBF;

(f) in breach of an individual's contract, or this policy;

(g) in breach of data protection rights;

(h) to monitor staff conduct;

(i) to investigate complaints, grievances or criminal offences.

22.28 When monitoring incoming or outgoing emails, we will, unless exceptional circumstances apply:

(a) look at the sender or recipient of the email and the subject heading only; and

(b) avoid opening emails marked 'Private' or 'Personal'.

22.29 We do not as a matter of policy routinely monitor employees' use of the internet or the content of email messages sent or received. However, we have a right to protect the security of our systems or network, check that use of the system is legitimate, investigate suspected wrongful acts and otherwise comply with legal obligations imposed upon us. To achieve these objectives, we may carry out random spot checks

on the system which may include accessing individual email messages or checking on specific internet sites searched for and/or accessed by individuals.

22.30 We will only intercept (ie open) outgoing or incoming emails, received emails, sent emails and draft emails where relevant to the carrying on of our DBF and where necessary:

(a) to determine whether the message is relevant to the carrying on of our DBF;

(b) to establish the existence of facts;

(c) to check whether regulatory or self-regulatory practices or procedures to which we or our staff are subject have been complied with, ie to detect unauthorised use of the system;

(d) to check whether staff using the system in the course of their duties are achieving the standards required of them;

(e) for the purpose of investigating or detecting the unauthorised use of the system;

(f) for the purpose of preventing or detecting crime; or

(g) for the effective operation of the telecommunication system.

Telephones—personal use

22.31 Although the telephone system is primarily for DBF use, we understand that you may occasionally need to make or receive personal telephone calls while at work. The making or receiving of personal telephone calls while at work using our telephone system AND/OR your personal mobile phone is therefore permitted.

22.32 Personal use must meet these conditions (in addition to those set out elsewhere in this policy):

(a) it must be minimal (both in terms of time spent and frequency) and reasonable and must take place mainly outside normal working hours, ie during lunch or other breaks, or before and after work;

(b) it must not affect the job performance any member of staff or otherwise interfere with our DBF;

(c) it must not commit us to any marginal costs; and

(d) you may not use the telephone during working hours to perform work for yourself or another employer, or to look for work;

22.33 Our telephone system may not be used for premium rate or international calls.

Telephones—monitoring

22.34 We may monitor the use of our telephone system, and DBF mobile phones (including smartphones) for the following reasons:

(a) if you are absent from work, to check communications (including your voicemail) for DBF calls to ensure the smooth running of the DBF;

(b) to record transactions;

(c) where we suspect that an individual is acting in a way that is:

(d) detrimental to the DBF;

(e) in breach of the individual's contract, or this Policy;

(f) in breach of data protection rights;

(g) to monitor staff conduct;

(h) to investigate complaints, grievances or criminal offences.

22.35 When monitoring telephones, we will, unless exceptional circumstances apply, look at the numbers from which calls are received and the numbers dialled and the duration and frequency of calls.

22.36 We will only intercept (ie listen to) telephone calls or saved messages where relevant to the carrying on of our DBF and where necessary:

(a) to determine whether the message is in fact relevant to the carrying on of our DBF;

(b) to establish the existence of facts;

(c) to check whether regulatory or self-regulatory practices or procedures to which we or our staff are subject have been complied with, ie to detect unauthorised use of the system;

(d) to check whether staff using the system in the course of their duties are achieving the standards required of them;

(e) for the purpose of investigating or detecting the unauthorised use of the system;

(f) for the purpose of preventing or detecting crime; or

(g) for the effective operation of the telecommunication system.

Internet—general

22.37 Access to the internet during working time is primarily for matters relating to your work duties and employment. Reasonable, limited personal use of the internet is permitted.

22.38 Any unauthorised use of the internet is strictly prohibited. Unauthorised use includes (but is not limited to):

(a) creating, viewing or accessing any webpage, or posting, transmitting or downloading any image, file or other information that is unrelated to your employment and, in particular, which could be regarded as pornographic, illegal, criminal, offensive, obscene, in bad taste or immoral and/or which is liable to cause embarrassment to us or to our clients/customers and/or suppliers;

(b) engaging in computer hacking and/or other related activities; and

(c) attempting to disable or compromise security of information contained on our systems or network or those of a third party.

22.39 Staff are reminded that such activity may also constitute a criminal offence.

22.40 Posts placed on the internet may display our address. For this reason you should make certain before posting information that the information reflects our standards and policies. Under no circumstances should information of a confidential or sensitive nature be placed on the internet. You must not use the DBF's name in any internet posting (inside or outside work) unless it is for a work-related purpose.

22.41 Information posted or viewed on the internet may constitute published material. Therefore, reproduction of information posted or otherwise available over the internet may be done only by express permission from the copyright holder. You must not act in such a way as to breach copyright or the licensing conditions of any internet site or computer program.

22.42 We may block or restrict access to any website at our discretion.

Internet—personal use

22.43 Reasonable personal use of our systems or network to browse the internet is allowed provided that it does not interfere with the performance of your duties and the terms of this policy are strictly adhered to. We reserve the right, at its absolute discretion, to withdraw this privilege at any time and/or to restrict access for personal use.

22.44 Personal use must meet these conditions (in addition to those set out elsewhere in this policy):

(a) it must be minimal (both in terms of time spent and frequency) and reasonable and should take place mainly outside normal working hours, ie during lunch or other breaks, or before and after work;

(b) it must not affect the job performance of any member of staff or otherwise interfere with our DBF; and

(c) it must not commit the DBF to any marginal costs.

Internet—monitoring

22.45 We may monitor internet usage (including searches made, the IP addresses of sites visited, and the duration and frequency of visits) if we suspect that an individual has been using the internet in breach of the contract of employment or this policy, eg:

(a) by viewing material that is pornographic, illegal, criminal, offensive, obscene, in bad taste or immoral and/or which is liable to cause embarrassment to us or to our clients/customers;

(b) by spending an excessive amount of time viewing websites that are not work-related.

22.46 Monitoring may include internet usage at the workplace, internet usage outside the workplace during working hours using DBF systems or network and internet usage using hand-held or portable electronic devices.

Passwords and security

22.47 You are personally responsible for the security of all equipment allocated to or used by you. You must not allow equipment allocated to you to be used by any other person, other than in accordance with this policy.

22.48 You must use passwords on all IT equipment allocated to you, and keep any password allocated to you confidential and change your password regularly.

22.49 You must not use another person's username and/or password to access our systems or network, nor allow any other person to use your password(s). If it is anticipated that someone may need access to your confidential files in your absence, you should arrange for the files to be copied to a network location that is properly secure where the other person can access them or give the person temporary access to the relevant personal folders.

22.50 You must log out of the system or lock your computer when leaving your desk for any period of time. You must log out and shut down your computer at the end of the working day.

DBF systems and data security

22.51 You must not download or install software from external sources without prior authorisation from your line manager.

22.52 You must not connect any personal computer, mobile phone, laptop, tablet, USB storage device or other device to our systems or network without express prior permission from your line manager. Any permitted equipment must have up-to-date anti-virus software installed on it and we may inspect such equipment in order to verify this.

22.53 You must not run any '.exe' files, particularly those received via email, unless authorised to do so in advance. Unauthorised files should be deleted immediately upon receipt without being opened.

22.54 You must not access or attempt to access any password-protected or restricted parts of our systems for which you are not an authorised user.

22.55 You must inform your line manager immediately if you suspect your computer may have a virus and must not use the computer again until informed it is safe to do so.

22.56 All laptop, tablet, smartphone and mobile phone users should be aware of the additional security risks associated with these items of equipment. All such equipment must be locked away in a secure location if left unattended overnight.

Data Protection issues

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

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

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

22.60 If in doubt about a particular situation staff should seek advice from the **Data Protection Manager.**

Regulatory advice

22.61 The ICO email security advice states:

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

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

Staff and members of the Cohort should remember:

(c) The use of 'bcc' only protects the recipient's identity not the content of the email.

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

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

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

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

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

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

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

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

23 Social Media Policy

23.1 The DBF recognises that internet and social media platforms are used as a means of communication both at work and at home. This policy outlines the standards we require staff to observe when using social media, the circumstances in which we will monitor your use of social media and the action we will take if this policy is breached.

23.2 This policy should be read in conjunction with our Internet, email and communications policy, which sets out how the DBF's internet and email systems and networks can be used by our staff and representatives.

23.3 This policy applies to all individuals, including employees, workers, temporary and agency workers, contractors, interns, volunteers and apprentices (referred to as 'staff' in this policy).

23.4 Staff should refer to the DBF's data protection privacy notice and, where appropriate, to its other relevant policies.

Social media

23.5 In this policy, 'social media' means internet-based applications which allow users to collaborate or interact socially by creating and exchanging content, such as social networks or platforms, community sites, blogs, microblogging sites, wikis, web forums, social bookmarking services and user rating services. Examples include Facebook, LinkedIn, YouTube, Instagram, X, Bluesky, Tumblr, TikTok, Flickr, SlideShare, Foursquare and Pinterest and the review areas of e-commerce sites.

23.6 Social media platforms allow us to build connections and to share ideas and content more broadly and quickly, and we support their use. However, improper use of social media may give rise to a breach of your contract and/or our policies, and/or defamation (ie damaging the good reputation of another person or organisation), breach of data protection laws, misuse of our confidential information or that of our customers, clients and/or suppliers and/or reputational damage.

23.7 This policy does not seek to regulate how staff use social media in a purely private capacity, provided that use has no bearing on the DBF or its activities. This policy is intended to ensure that staff understand the rules governing their use of social media in relation to their work for us, or when referencing the DBF, or where use of social media may affect us or our activities. It is designed to help you use these platforms and services responsibly, so as to minimise the risks set out above and to ensure consistent standards of use of social media. This policy therefore applies where:

23.7.1 your use of social media relates to the DBF or its activities;

23.7.2 your use of social media relates to, or is otherwise connected with, your work, whether the intended use is personal or professional; and/or

23.7.3 you represent yourself, or are otherwise identifiable, as someone employed by, or otherwise associated with, the DBF.

23.8 This policy applies to your use of social media whether on a DBF, personal or other device.

General rules for use of social media

23.9 You must not use your work email address to sign up for personal use of social media platforms.

23.10 You should have no expectation of privacy or confidentiality in anything you create or share on social media platforms. When you create or exchange content using social media you are making a public statement. As such, your content will not be private and can be reposted, copied or forwarded to third parties without your consent. You should therefore consider the potential sensitivity of disclosing information (such as health information) on a platform. Once sensitive or confidential information (or offensive or defamatory information) has been disclosed, it cannot be recovered and this may result in liability both for the DBF and also for you personally.

23.11 Bear in mind that, even if you are using social media in a personal capacity, other users who are aware of your association with us might reasonably think that you speak on our behalf. You should always take account of any adverse impact your content might have on our reputation or our relationships with clients, customers, suppliers and other business partners.

23.12 When creating or exchanging content on a social media platform, you must at all times comply with your contract of employment (or other contractual arrangements) with us, our disciplinary rules and any of our policies that may be relevant. In particular you must:

(a) not harass, sexually harass or bully other members of staff, or customers, clients, suppliers or other third parties;

(b) not discriminate against other members of staff or third parties;

(c) not breach our data protection or Internet, email and communications policies;

(d) respect any confidentiality obligations owed by you or us, and not disclose commercially sensitive material or infringe any intellectual property or privacy rights of the DBF or any third party;

(e) not make defamatory or disparaging statements about the DBF, its shareholders, employees, customers, clients, suppliers or competitors;

(f) not create or exchange or link to abusive, obscene, discriminatory, derogatory, defamatory or pornographic content;

(g) not upload, post or forward any content belonging to a third party unless you have that third party's consent;

(h) ensure that any quotes from third party material are accurate;

(i) check that a third party website permits you to link to it before including a link and ensure that the link makes clear to the user that the link will take them to the third party's site; and not post, upload, forward or post a link to chain mail, junk mail, cartoons, jokes or gossip.

23.13 You should be honest and open but also be mindful of the impact your posting on a social network or platform may have on the perception of the DBF.

23.14 If you make a mistake in a posting, be prompt in admitting and correcting it.

23.15 Do not escalate 'heated' discussions. Try to be conciliatory and respectful and quote facts to lower the temperature and correct misrepresentations. Never contribute to a discussion if you are angry or upset; return to it later when you can contribute in a calm and rational manner.

23.16 Avoid posting in relation to or discussing topics that may be inflammatory, such as politics or religion.

23.17 You should regularly review the privacy settings on your personal social media accounts and appropriately restrict the people who can read your comments. Review the content of your personal social media accounts on a regular basis and delete anything that could reflect negatively on you in a professional capacity or on the DBF.

Using work-related social media

23.18 We recognise the importance of the internet and social media in shaping public thinking about the DBF, our services, staff, clients, customers and other business partners. We also acknowledge that our staff can have an important role to play in shaping industry/sector conversation and direction through interaction in social media.

23.19 Our staff are therefore permitted to interact on approved social media platforms about industry/sector developments.

23.20 When undertaking permitted work-related social media interaction, in addition to the general rules above, you must:

(a) clearly identify yourself, including your name and job title, and use the following disclaimer: '*The views expressed are my own and do not necessarily reflect the views of my employer*';

(b) ensure that all communications are of high quality (in terms of content and form) including being grammatically correct, accurate, objectively justifiable, reasonable and appropriate for the intended audience;

(c) not provide references or recommendations for anyone else on social media (whether employment or business recommendations) in any way that suggests any endorsement or recommendation by the DBF. If you wish to provide a reference or recommendation, you should seek advice from your line manager and ensure that any such reference or recommendation can be withdrawn at any time as we may require;

(d) if you become aware of adverse criticism of the DBF or of content you have created or shared, inform your line manager. Do not respond without their express approval;

(e) comply with the terms and conditions and policies of the social media platforms you use;

(f) maintain good information security practices. Use strong passwords and make appropriate use of security and privacy settings on social media platforms, and follow our email, internet and communications and information security policies, guidelines and standards;

(g) seek approval from your line manager before creating or exchanging comments on colleagues, customers, clients, suppliers or competitors;

(h) before you begin communication on a social media platform, evaluate your audience by gaining an insight into the type of content that is published and note any unwritten rules that are followed in discussions;

(i) not use DBF trade marks, brands or logos or other identifying material

Personal use of social media platforms

23.21 You may make reasonable use of social media platforms for personal use outside working hours using our computers, networks and/or systems (including via smartphones or tablets), provided use is minimal and takes place substantially out of normal working hours (ie during your lunch break or before or after work), it does not interfere with your duties and business and office commitments and is strictly in accordance with this policy.

23.22 Any unauthorised use of social media platforms is strictly prohibited. Permission to use our systems to access social media platforms for personal use may be withdrawn at any time at our discretion.

Monitoring

23.23 Our internet, email and communications policy, in particular in relation to our right to monitor, intercept and read communications, applies equally to use of social media platforms via the DBF's systems or network.

23.24 We will also monitor how we use social media generally and what is said about us and about our competitors.

23.25 We may monitor your LinkedIn and other business-related social media profiles during your notice period and during the period of any relevant post-termination restrictions to which you are subject, for the purposes of our legitimate interests, ie to ensure that any non-competition, non-disparagement provision is complied with.

23.26 We will only carry out such monitoring where there are no other, less invasive, means available.

Statutory Basis for Monitoring Activity

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

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

Breaches of this policy

23.29 Staff are also reminded that, in certain circumstances, an act that breaches this policy may also constitute a criminal offence.

23.30 If, in the course of using social media, you become aware of any misconduct or wrongdoing by any employee, officer, worker or agent of the DBF, you must report it to your line manager.

23.31 You may be required to remove content created or shared by you which we deem to be in breach of this policy.

23.32 Employees who feel that they have been harassed or bullied because of material posted or uploaded by a colleague onto a social media platform should inform their line manager.

24 Data Storage, transfer and retention

24.1 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

24.2 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.

24.3 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.

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

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

24.6 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.

24.7 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.

24.8 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.

24.9 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.

24.10 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

24.11 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.

24.12 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.

24.13 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.

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

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

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

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

24.18 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.

25 International data transfers

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

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

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

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

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

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

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

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

25.9 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.

Bangor Diocesan Board of Finance
Bwrdd Cyllid Esgobaeth Bangor

Data Protection Compliance Document

PART FOUR of FIVE

DATA RIGHTS & BREACH POLICIES

26 Data Subject Access Requests

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

26.2 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.

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

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

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

26.4 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.

26.5 This policy provides guidance on:

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

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

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

26.7 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.

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

How to recognise a data subject access request (DSAR)

26.9 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:

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

26.9.2 for access to that personal data

26.9.3 and certain other supplementary information

26.10 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.

26.11 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

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

26.13 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.

26.14 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.

26.15 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**.

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

26.17 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.

26.18 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.

26.19 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.

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

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

26.22 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:

26.22.1 that is manifestly unfounded or excessive, e.g. repetitive; or

26.22.2 for further copies of the same information.

Identifying the data subject

26.23 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.

26.24 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.

26.25 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.

26.26 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.

26.27 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

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

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

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

26.29 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

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

26.31 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.

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

(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

26.33 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:

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

(f) to object to its processing;

(g) to lodge a complaint with the ICO;

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

(i) 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.

26.34 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

26.35 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.

26.36 If the DBF 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 DBF, 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

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

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

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

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

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

(d) private devices used by employees and others;

(e) occupational health records;

(f) pensions data;

(g) share scheme information;

(h) insurance benefit information;

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

What is personal data?

26.39 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.

26.40 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

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

26.42 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

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

Crime detection and prevention:

26.44 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.

26.45 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:

26.46 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:

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

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

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

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

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

Confidential references:

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

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

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

(c) provision by the individual of any service

NB: For this exemption to apply a reference must have been noted as 'Confidential' when requested. However, in this situation, if access is granted to the reference doing

so may disclose the personal data of another individual (ie the person giving the reference), which means you must consider the rules regarding disclosure of third-party data before disclosing the reference.

Legal professional privilege:

26.48 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 DBF and its professional legal advisers for the purpose of seeking or obtaining legal advice;

(b) 'litigation privilege', which covers confidential communications between the DBF 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:

26.49 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:

26.50 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:

26.51 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

26.52 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.

26.53 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.

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

Consequences of failing to comply with this policy

26.55 The DBF 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 DBF 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.

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

27 Data Breach Policy

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

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

27.3 We have determined a policy to comply with Data Breaches in the DBF as follows:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(a) Demonstrate our response to the incident.

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

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

Bangor Diocesan Board of Finance
Bwrdd Cyllid Esgobaeth Bangor

Data Protection Compliance Document

PART FIVE of FIVE

LEGITIMATE INTEREST
&
UPDATES POLICIES

Policies requiring a Legitimate Interest Assessment

28 Marketing

28.1 We do not engage in Direct Marketing activity for the DBF.

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

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

28.4 We are familiar with the provisions of the Privacy & Electronic Communications Regulations 2003 (PECR).

29 Video Conferencing Policy

General

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

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

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

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

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

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

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

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

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

Phishing

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

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

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

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

The Platform

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

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

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

Passwords

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

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

Storage and Uploading of Video Conferencing

29.19 Video Conference recording facilities are available on most platforms.

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

29.21 Where we intend to keep recordings of Video Conference calls this will be notified to participants at the start of the call to provide an opportunity for them to 'Opt out' by closing their video link and remaining on the call using audio only or by leaving the call altogether.

Video Conferencing Applications – Legitimate Interest Assessment

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

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

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

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

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

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

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

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

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

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

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

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

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

(d) We will not always record the video conference call but if we do, any Personal Data processed will not be of the kind to cause any ethical issues and will be dealt with in line with our robust and fully operational UK GDPR privacy policies and systems.

29.28 Video Conferencing and the use of images both of the participants and with reference to non Personal Data information such as charts, graphs, photographs etc is the only

way to achieve the purpose and transmit the information necessary for the successful completion of the agenda of the call.

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

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

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

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

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

29.34 All participants in the call will be adults.

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

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

29.37 The Legitimate Interest Assessment Test determined the following:

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

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

29.40 To facilitate efficient video and telecommunications.

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

29.42 To support our primary objectives.

30 CCTV - Policy

30.1 We use closed circuit television (CCTV) to provide a safe and secure environment for staff, visitors and customers, and to protect DBF property. This policy relates to our use and management of CCTV.

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

30.3 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

30.4 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.**

30.5 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.

30.6 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

30.7 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

30.8 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:

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

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

30.8.3 monitor security and health and safety at our premises.

30.9 We have carried out a data protection impact assessment and consider that these purposes are legitimate, reasonable, appropriate and proportionate.

30.10 The CCTV system will NOT be used:

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

(b) for any automated decision making; or

(c) to monitor private areas of the premises.

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

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

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

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

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

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

Covert recording and monitoring of staff

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

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

Positioning cameras

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

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

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

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

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

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

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

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

Image quality

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

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

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

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

(d) cameras will be correctly positioned;

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

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

(g) if cameras break down or are damaged, the **Data Protection Manager** is responsible for arranging timely repair.

Data and image retention

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

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

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

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

Access to images

30.29 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:

(i) the date and time they were removed;

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

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

(iv) the reason for viewing the images; and

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

(e) 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

(f) 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.

(g) 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.

(h) 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;

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

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

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

(m) 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

(n) staff involved with our disciplinary processes.

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

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

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

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

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

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

Subject access rights to individuals' own data

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

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

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

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

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

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

(d) the location where the images were recorded.

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

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

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

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

Requests to restrict processing and objections to processing

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

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

Complaints

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

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

30.44 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.

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

CCTV – Legitimate Interest Assessment

30.46 THE PURPOSE TEST

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

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

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

30.50 THE NECESSITY TEST

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

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

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

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

30.55 THE BALANCING TEST

30.56 The CCTV cameras are clearly visible.

30.57 The operation of the CCTV cameras is Signposted.

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

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

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

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

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

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

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

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

30.66 CONCLUSIONS

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

30.68 To protect our business premises.

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

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

31 Dashcams

31.1 We intend to use dashcam recording equipment in our business and staff private vehicles used for business purposes.

Dashcam equipment – Legitimate Interest Assessment

31.2 THE PURPOSE TEST

31.3 We wish to use Dashcam units in our business vehicles to record in real time incidents which occur on the road.

31.4 Use of Dashcams will ensure accuracy in reporting of incidents on the road.

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

31.6 All parties in any claim would benefit from an accurate representation of the incident.

31.7 The general public benefit from the certainty of the record.

31.8 The importance of an accurate record of events is fundamental to road safety.

31.9 The camera record will allow us to understand incidents properly and determine whether drivers were abiding by Road Traffic legislation.

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

31.11 THE NECESSITY TEST

31.12 Use of Dashcams in our business vehicles will achieve our stated purposes.

31.13 The Dashcams are proprietary equipment designed for the purpose and are a proportional response to this need.

31.14 It is not possible to record real time driving and road traffic activity in this way without using camera technology

31.15 The Dashcam collects only the data it needs to perform its task and writes over the unused previous recordings unless an incident occurs.

31.16 Consequently this is a proportionate response to the requirement of data processing and ensures data minimization due to the operation of the technology.

31.17 THE BALANCING TEST

31.18 There is no special category data recorded in this manner.

31.19 The data of driver activity on the road occurs on public so is not considered private.

31.20 There may be children on the recordings depending on the circumstances encountered but they would only be identified by their appearance.

31.21 The Dashcams are used in the manner that would, objectively be expected.

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

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

31.24 The use of the Dashcams does not impact the Data Subject or their rights and freedoms in a negative way.

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

31.26 CONCLUSIONS

31.27 The legitimate Interest Assessment Test determined the following:

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

31.29 To protect our Employees, business assets and our reputation.

31.30 To correctly record incidents which occur on the road.

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

32 Review and Updating

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

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

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

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

32.5 A Data Audit will be conducted:

32.5.1 Regularly and in any event at least Annually.

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

32.5.3 When any other relevant changes are required

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

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

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

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

Policy Currency

Policy Active from: 1 June 2025

Update required by: 1 June 2026

Date	Update Required	Reason for Revision	Applicable to	Signed by DP Contact	Print Name
1.6.25	Policy updates	UK GDPR/DPA 18	All Staff	O Pritchard	Mr Owain Pritchard