# PAROCHIAL CHURCH COUNCIL OF BUCKSHAW VILLAGE

# DATA PROTECTION POLICY

## 1. INTRODUCTION AND SCOPE

Data protection laws are designed to protect the privacy of individuals and to keep their information safe from misuse, whilst still ensuring that important information is given to the right people and authorities in appropriate circumstances.

This policy identifies the types of individuals who deal with Buckshaw Village Church ("BVC") and will be affected by data protection laws:-

1. Clergy and liturgical office-holders
2. Leadership team
3. Staff team / employees
4. PCC councillors
5. Volunteers with designated responsibility for co-ordinating ministry activities / official Church business
6. Casual volunteers
7. Members
8. Visitors

In this policy, references to "Church Workers" will include people in categories 1 to 5 inclusive above, whether or not they are paid.

## 1. RELEVANT LEGISLATION

Data Protection Act 2018
General Data Protection Regulation (EU/2016/679)

## 2. GOVERNING PURPOSES OF DATA PROCESSING

The Parochial Church Council (Powers) Measure 1956 defines the functions and powers of a "PCC". Under the amended Measure, the principal function of the PCC is "*promoting in the parish the whole mission of the Church, pastoral, evangelistic, social and ecumenical.*" This mission operates within the secular law of England and the United Kingdom which includes legal duties owed to third parties. From these core functions and duties, we establish the following key legitimate interests of BVC which are relevant to data processing as including:-

- **Evangelism**
  - To proclaim the good news of Jesus Christ and to make disciples of all nations.

- **Pastoral**
  - To make disciples includes an obligation to walk with Christ and each other on our individual and collective journeys of faith. Pastoral care includes spiritual, emotional, mental and physical needs.
- **Community engagement and social justice**
  - In addition to our evangelistic and pastoral work, we aim to bring joy through events which build and celebrate friendships and community, and to advance causes of social justice.
- **Safeguarding**
  - We will do our utmost to ensure that any child, young person or adult who is at risk/vulnerable is protected, and that concerns are reported appropriately to both legal and Church authorities in line with the Diocesan Safeguarding Policy.
- **Employment**
  - As Christian employers we will treat our employees with love, dignity and respect. We will ensure the security of our employees' data and will collect and use it to ensure that we meet our legal employment obligations.
- **Health and Safety**
  - We will use information we know about people in order to keep them safe, to complete accident reports where they were injured etc and to fulfil our legal and moral duty.
- **Administration**
  - In all of the above considerations, effective administration of Church business is a necessary interest and reason for processing of personal data.

## 4. DATA CONTROLLERS AND OFFICERS

The Data Controller is Buckshaw Village Church, a parish church body of the Church of England. The BVC Church office is based at 1 Bridgewater Drive, Buckshaw Village, PR7 7EU.

BVC is not legally required to appoint a Data Protection Officer but chooses to do so unless the PCC resolves not to at a given time, for example if nobody suitable is available to fulfil the role.

The Data Protection Officer can be contacted via the BVC Church office. If nobody is appointed as the Data Protection Officer, or the Data Protection Officer is unavailable, matters relating to BVC's compliance with data protection laws (including Data Subject Access Requests) should be addressed to the Secretary of the PCC who will liaise with the PCC Standing Committee if needed.

## 5. DATA SUBJECTS AND DATA CATEGORIES

We acknowledge that in the course of BVC's legitimate interests, we will hold and process personal data regarding the following categories of data subjects:-

- Clergy and liturgical office-holders
- Leadership team
- Staff team / employees
- PCC councillors
- Volunteers
- Members
- Visitors
- Other third parties (e.g. ministers in other churches, employees of statutory agencies, employees of businesses with whom we agree contracts)

"Personal data" means any information relating to an identified or identifiable "natural person" (i.e. a living individual) – referred to as a "data subject". This includes where that individual can be identified from the data in question plus other information which is available, and has historically included "statements of opinion or intent".

We will process personal data either with the informed consent of the data subject(s) or where it is necessary for one or more other lawful purposes, which can include BVC's legitimate interests.

We acknowledge that in the course of BVC's legitimate interests, we are likely to hold and process personal data regarding the following types of information which additionally qualify as "special category" personal data:-

- Religious or philosophical beliefs – this will almost always be a given assumption in a data subject's interactions with BVC as we engage mostly with people who are (or identify as) Christians or who are enquiring about the Christian faith
- Racial & ethnic origin
- Political opinions
- Data concerning health including physical and mental health, and gender identity
- Sex life and sexual orientation
- Criminal offences

We will process personal data either with the informed consent of the data subject(s) or for one or more other lawful purposes, which can include BVC's legitimate interests or where it is necessary for us to comply with a legal obligation (e.g. Diocesan returns; Police investigation, complying with employment law etc.) or there is another lawful basis for processing.

## 6. **COLLECTION**

We collect or record personal data in the following circumstances:

- Emails, text messages, telephone & video call logs, online messages including social media, and letters sent and received;

- Telephone/video calls and face-to-face meetings for which any notes are kept;
- Notes and entries in diaries and rotas;
- Applications for paid or voluntary work;
- Taking and maintaining registers, including public registers;
- Organising group trips and activities;
- Subscribing to newsletters or mailing lists, in writing or online.

We will only collect and record personal data where it is given voluntarily, or we can show that it is necessary to collect and record the data for one or more of BVC's legitimate interests, or where it is necessary for us to comply with a legal obligation (e.g. Diocesan returns; Police investigation, complying with employment law etc) or there is another lawful basis for processing.

We will not actively collect or record personal data which is not necessary or relevant to the purposes for which it is intended to be used.

## 7. OBTAINING AND RECORDING CONSENT

Under GDPR, consent to processing should be:-

- Freely and voluntarily given (positive opt-in or default consent);
- Specific, not generalised;
- Easily identified and understood;
- Easy to withdraw;
- Recorded for future reference;
- Kept under review, and updated if anything changes.

We will endeavour to include a consent statement when we collect or record personal data. If consent cannot be shown to have been given, then we will process data where it is necessary for one or more of BVC's legitimate interests, or where it is necessary for us to comply with a legal obligation (e.g. Diocesan returns; Police investigation, complying with employment law etc.) or there is another lawful basis for processing.

Consent to receive circular emails and e-bulletins is dealt with in section 12, "*Website, Cookies and Email Communications from Church*".

Consent to receive notifications via BVC social media channels is governed by the consent protocols of the individual sites. A social media policy is available for those with Administrator rights to the Buckshaw Village Church Facebook page.

In some circumstances, consent to processing is given verbally, for example when a visitor to church gives their contact details to a minister and invites them to make contact by that method. It is the responsibility of the person who receives this personal data to ensure that free, clear and unequivocal consent for the data to be recorded, stored and used for the agreed purposes has been given.

Consent to processing will be presumed withdrawn if a data subject who has been a member or regular worshipper at BVC communicates that they no longer wish to be considered as such, or have not participated in any Church activity for more than 12 months.

## 8. STORAGE AND SECURITY

A number of individuals identified in Section 1, categories 1 to 5 are required to store personal data securely by virtue of their role and the sensitivity of the data held.

All PCC Councillors are aware of their duties as trustees to comply with data protection law. Personal data will be stored with a degree of security which is appropriate to the sensitivity of the data held and should only be processed where it is lawful to do so. Others are reminded that the officers, employees and trustees of the Church may be held legally responsible for personal data security breaches caused by volunteers.

Certain specific examples are identified as being of particular importance:-

- Portable data storage devices or media must be subject to appropriate security measures. If they include "special category" personal data, financial data, or databases of personal contact details and where there is a risk of unauthorised access, then the owner should consider whether the device/media should be encrypted; and data which is stored remotely must be password-protected. This includes laptops, tablets, mobile phones, and USB storage memory sticks. For the avoidance of doubt, encryption is not required if:
    - The device / media is exclusively used and kept in a secure location e.g. in a Church office or a person's home, provided that nobody else can gain access to it (e.g. kept in a locked cabinet); or
    - No "special category" personal data, financial data, mobile/telephone numbers, or email addresses can be accessed (please note this includes being able to log in to an email account or cloud storage).
- Church Workers who for official Church purposes keep other people's "special category" personal data or financial data in online accounts or cloud storage (e.g. on social media, email, Dropbox, OneDrive) must ensure that neither login details nor shared folders are accessible to any unauthorised persons except on an electronic device which is protected by appropriate security measures – e.g. encrypted, or exclusively used and kept in a secure location (as above).
- Church Workers who for official Church purposes keep other people's "special category" personal data or financial data, or any data relating to children & young people in written form, must not leave them accessible to third parties unless legally required or authorised to do so (e.g. in relation to official Church public notices) and must keep them stored securely when not in use (as above).
- Registers are sometimes kept for health & safety or safeguarding purposes – once the activity has ended the register should either be converted to electronic storage and the hard copy shredded, or kept stored securely when not in use (as above).

- Personal data which are stored electronically on a physical device for official Church purposes (e.g. computer, laptop, mobile phone) should be kept regularly backed up online or on separate portable storage media.

Casual volunteers are not subject to the full range of data protection law in their own right provided that they are using personal data for what might be termed “personal use”, e.g. organising an informal social gathering. This does not absolve individuals from the general civil law on confidentiality or the criminal offence of making unauthorised disclosures of personal data. Church Workers will retain overall responsibility for the appropriate use of personal data by casual volunteers.

## 9. FINANCIAL DATA

Although financial data are not classed as “special category” data, we will treat such information confidentially and sensitively (Section 8, “*Storage and Security*”).

We are required to maintain records of individual financial data including the following:-

- Donations received;
- Tax claimed back through Gift Aid;
- Salaries / stipends, PAYE, National Insurance, in-work benefits administered by HMRC e.g. Tax Credits, pension contributions, other deductions from salaries / stipends;
- Expenses of employees and volunteers;
- Donations and gifts given to others.

Maintenance of financial records shall be the primary responsibility of the PCC Treasurer, however others identified in Section 1, categories 1 to 5 may be authorised to access individual financial records held by BVC.

Anonymised or aggregated data (e.g. total donations) shall be made available on a confidential basis and where appropriate to others identified in Section 1 for the purposes of discharging their duties as officers and trustees. This does not affect any right or duty of the Church to publish budgetary information to members of the congregation or the public.

BVC may disclose individual financial data to third parties where this is legally required e.g. HMRC, the Charity Commission, Blackburn Diocese / Methodist Church, the Serious Fraud Office/Police (e.g. in connection with money laundering), etc. or where the disclosure is necessary in order to process a financial transaction (e.g. communications with a bank or building society).

## 10. EMPLOYMENT DATA

BVC will hold personal data in connection with employment in order to comply with employment law. This may include certain types of “special category” personal data.

Employee personal data will be kept in the following locations:-

- Paper records (e.g. employment contracts) in a locked filing cabinet in the Church office.
- Electronic employment records/information on the Church office computer.

Anglican Clergy are office-holders rather than employees and so their data in this regard are held by the Blackburn Diocese.

## 11. EXPORTING DATA

BVC does not export personal data outside of the EU except to the following extent:-

- Cloud data storage and email servers which comply with GDPR requirements
- Sharing personal information (with the express consent of the data subject(s) in question) to overseas missionaries etc.

## 12. WEBSITE, COOKIES AND EMAIL COMMUNICATIONS FROM CHURCH

The BVC website uses "cookies" for necessary purposes which enable the website to function appropriately and to understand how the website is used by visitors. Cookies are not currently used to create targeted content or in relation to advertisements. A link to the cookies policy is carried on every page of the website.

The BVC website includes a privacy statement explaining that certain data may be analysed in order to make the website accessible and for aggregated data analysis.

BVC uses a third party provider to administer regular bulletins/updates. This provider is compliant with GDPR legislation/requirements.

BVC does not currently use large scale text message communications. Such communications should be restricted to small groups where the proposed recipients have given consent (Section 7, "*Obtaining and Recording Consent*"), where this is necessary for Church administration, to enable compliance with a legal obligation or where there is another lawful basis for processing.

Church Workers may on occasion send emails or text messages with consent from recipients (Section 7, "*Obtaining and Recording Consent*") where this is necessary for Church administration, to enable compliance with a legal obligation or where there is another lawful basis for processing. Where emails are sent to more than one recipient at a time, email addresses should be typed in the "BCC" field of the email unless all recipients are aware in advance that they will be on an open mailing list; or where this is necessary for Church administration, to enable compliance with a legal obligation or where there is another lawful basis for processing.

Church Workers may on occasion create groups e.g. in Facebook Messenger or WhatsApp, for example in order to communicate with prayer groups or "Task Teams". Church Workers are recommended to seek at least verbal consent first from all proposed participants before the group is created or before new members are added, and to record consent afterwards

for anyone who is not a Church Worker (Section 7 "*Obtaining and Recording Consent*"). Individuals can opt-out of such communications either by following the online instructions on leaving the group or by asking a group administrator to remove them.

Church Workers and group administrators who set up or moderate open email lists or message board groups are reminded of the need to ensure that all recipients are treated with dignity and respect, and to take steps to prevent any abusive communications (this may include removing a group member or reporting communications to the Church authorities / Police as appropriate).

Anyone who sends communications on behalf of or related to BVC, by whatever means, are reminded of their duty to ensure the communication is accurate, relevant and appropriate, and should under no circumstances issue any communication which could bring the church into disrepute.

## 13. SORTING AND FILING

Church Workers are reminded of the need to keep records in an orderly fashion and to maintain secure and coherent filing systems for paper / electronic documents, emails etc.

## 14. THIRD PARTY DATA PROCESSORS

On occasion we may ask third party data processors to process personal data on our behalf, e.g.:-

- Payroll, accounting and auditing including Gift Aid administration;
- Legal advice and representation;
- Website and email / data storage;
- Venue hire and other service provision.

We will only do so where the data processor can demonstrate that they will comply with data protection laws.

## 15. EMERGENCIES AND "VITAL INTERESTS" CASES

A lawful ground for processing "special category" personal data is where it is necessary to protect vital interests – a life-or-death situation, e.g. telling a paramedic of a health condition for someone needing emergency medical assistance. If "special category" information is provided to a third party on this basis, this should be reported to the Data Controller as soon as possible by the person that has shared the information.

## 16. DBS, DATA SHARING, DISCLOSURES AND CONFIDENTIALITY

Church Workers and volunteers may be required to obtain a Disclosure and Barring Service certificate as part of their application for paid or voluntary work. Further details are available from the Safeguarding Officer. The individual is responsible for providing the Safeguarding

Officer with details of any convictions or other Police records which could relate to the person's suitability for the role, at the point the certificate is applied for. If the DBS result raises any safeguarding issues, details may be shared with the Police or other agencies as appropriate.

Church Workers and volunteers who are required to obtain a Disclosure and Barring Service certificate are also required to subscribe to the Update Service, and maintain their annual subscription.

BVC will follow the Diocese of Blackburn Safeguarding procedures when reporting concerns, as detailed in the policy document available on the BVC website.

BVC may be required to disclose personal data (including known or suspected offences) to the Police, statutory agencies, the Courts, or Church of England / Methodist Church authorities; or may be required to disclose personal data in connection with legal proceedings (including criminal, civil, family or Employment Tribunal proceedings).

## 17. RETENTION, ARCHIVING, DELETION AND DESTRUCTION

The standard period of retention for paper and electronic records will be in line with current legislation/Church of England policy. Further details are available in the Retention of Records Policy.

We will ensure that we securely destroy paper and electronic personal data where there is no further requirement to retain it.

## 18. DATA MINIMISATION AND DATA PRIVACY IMPACT ASSESSMENTS

A Data Privacy Impact Assessment ("DPIA") should be undertaken in the following situations:-

- When BVC undertakes a new activity
- Changes are made to an existing BVC activity which might have a bearing on the processing of personal data
- Other circumstances change which might have a bearing on the processing of personal data for an existing BVC activity

The nature and extent of the DPIA should be proportionate to the privacy risks involved. So if the personal data of many people will be involved, or if the nature of the personal data is highly sensitive, or if individuals could suffer financial loss or significant distress etc., then this might be considered high risk. If the personal data involves only a few people, the nature of the personal data is not particularly sensitive, and there is little or no risk of financial loss or emotional distress, then this would be considered low risk.

In a low risk scenario, the DPIA might be carried out very briefly and informally by considering the impact of the proposals or situation, and whether any reasonable changes could be made which would sensibly mitigate the impact without detracting from the activity in question – Church Workers are at liberty to ask for further advice but do not need to do

so. In a high risk scenario, Church Workers should consider asking for advice or assistance from the Data Protection Officer or another suitable Church Worker or a specialist, to ensure that the DPIA is carried out appropriately.

In all situations where personal data are being processed, Church Workers are reminded that processing should be limited to what is justifiable, for example:-

- Processing based on consent must only be for the purposes for which consent has been given and only for so long as consent is given;
- Processing based on a legal obligation must only be to the extent necessary to discharge the legal obligation in question; and
- Processing based on legitimate interests must only be to the extent necessary to achieve or promote the legitimate interest in question.

For this reason, BVC will not seek to accumulate personal data unnecessarily or speculatively, or merely for convenience.

## 19. COMPLIANCE WITH DATA SUBJECT RIGHTS INCLUDING THE RIGHT OF ACCESS

GDPR provides the following eight rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Of these, one of the most important on an operational level is the Right of Access (exercised by means of a Data Subject Access Request ("DSAR")).

If a DSAR is received, it shall be forwarded immediately upon receipt to the Data Protection Officer who shall deal with the request within the statutory time limits (usually 1 month), taking such steps as is reasonable to verify the identity of the person making the DSAR.

Once identity has been verified, the Data Protection Officer shall acknowledge receipt of the DSAR in writing (which can include by email or instant messaging service where appropriate) and co-ordinate compliance with the request.

Individuals identified in Section 1 may be asked to carry out a search of their records where the Data Protection Officer deems this necessary in order to comply with the DSAR. This search includes paper and electronic records, text messages and message board information. The results should be provided promptly to the Data Protection Officer.

Where compliance with a DSAR would involve providing personal data relating to other people, the Data Protection Officer shall consider whether consent to disclosure should be

obtained and/or whether the results of the search can be communicated in their original form or, for example, need to be redacted or summarised, or whether it is not possible to comply with the request (or aspects of it) due to the prejudice that would be caused to the other parties. Those identified in Section 1 are reminded that by virtue of their role, they do not have an absolute right to privacy of their communications.

The Data Protection Officer may delegate tasks under this section to another officer of the Church if this would help BVC comply with the DSAR effectively and in time. If nobody is appointed as the Data Protection Officer, or the Data Protection Officer is unavailable, matters relating to DSARs should be addressed to the Secretary of the PCC who will liaise with the PCC Standing Committee if needed.

## 19. MAXIMISING PRIVACY

All Church Workers are encouraged to think carefully before recording personal data in a permanent form and in particular whether it is necessary, for example: should the full name and address of a person hosting a prayer evening be disclosed in a public notice. This should be balanced against ensuring that information is communicated without disadvantaging those with disabilities.

## 20. DEALINGS WITH THE REGULATOR INCLUDING REGISTRATION, AND REPORTING DATA BREACHES

The following people will have primary responsibility for ensuring that BVC complies with its regulatory data protection obligations:-

- Data Protection Officer
- Churchwardens
- PCC Secretary
- PCC Treasurer

BVC considers that it is exempt from the data protection fee introduced under the GDPR at this time, unless and until advised otherwise.

Church Workers **must** report known or suspected personal data breaches **immediately** to the Data Protection Officer or, if they are not contactable, to the PCC Secretary and the Vicar / Priest in Charge (or equivalent). All substantial breaches of personal data security must be reported to the ICO within 72 hours of becoming aware of the breach, where feasible. The Data Protection Officer must keep a record of all personal data breaches, regardless of whether we are required to notify the ICO.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must inform those individuals without undue delay. This will be co-ordinated by the Data Protection Officer and the PCC Secretary.

Further details on data breaches and what should be considered can be found on the ICO website.

If you have any queries or concerns regarding this policy, please contact BV Church, 1 Bridgewater Drive, Buckshaw Village, PR7 7EU or email buckshawchurch@gmail.com.

## Version control

This is Version 2.0 of the policy and was adopted by the PCC on XXXXXX 20[XX]. Next review due [+3 years].
Version 1.0 – adopted 14th October 2018
Version 1.1 – adopted XXXXXXXXX