Parochial Church Council

Policies and Guidance

Trustee Declaration

1. PCC Trustee Declaration

Financial

2. PCC Financial Code
3. PCC Financial Liability

General Data Protection Regulations (GDPR)

4. General Data Protection Notice
5. General Data Protection Notice – Role Holders
6. Data Breach Procedure

Conflicts of Interest

7. Guidance on Managing Conflicts of Interest

St Nicolas Great Bookham

PCC Trustee Declaration

In signing the declaration below the PCC member is declaring:

- That they are willing to act as a Trustee (PCC member) and is fully aware of the organisation's object(s) as set out in the governing documents (namely: our charity sets out to undertake religious activities for the general public/mankind and may make grants to organisations, provides buildings/facilities/open space and provides services. Its current activity is: Building Faith in the Community, as a Church of England Parish Church).

- That they are not disqualified from acting as a Trustee because:

    - They have not been convicted of an offence involving deception or dishonesty
    - They are not an undischarged bankrupt
    - They have not previously been removed from trusteeship as a result of misconduct or mismanagement
    - They have not been disqualified to act as a Company Director

- That they are not disqualified from acting as a Trustee of St Nicolas specifically:

    - Because of disqualification from working with children
    - Because of being on the protection of vulnerable adults list

(We declare that we are not required by law to carry out CRB checks on our Trustees and also that we are not allowed by law to carry out such checks).

You are declaring that the information in this Declaration and the information in the Trustee Details: Information Required Form is complete and correct and that you accept that knowingly making a false statement is a criminal offence under the Charities Act.

St Nicolas Great Bookham

Financial Code – A summary outline of the church's Financial Controls with particular emphasis on budgeting and expense authorisation

1 Introduction

The PCC members are the Charity Trustees of St Nicolas. As Trustees, they are required to understand what funds are received by the church, how they are being spent and why. In order to provide a clear account of how the funds have been received and spent, it is necessary to produce a number of financial reports required by Charity law.

The accounts and reports help the PCC inform parishioners and others how their monetary gifts support the mission and ministry of the church. They also help show how money given for specific purposes has been used solely for those purposes.

The responsibility for ensuring that appropriate financial controls exist over income and expenditure and financial assets and liabilities of St Nicolas, and the provision of appropriate financial reports in line with Charities Act requirements, rests with the PCC, but has been delegated by the PCC to the Treasurer.

2 Role of the Treasurer in relation to Financial Controls and Financial Reporting

In relation to financial controls and financial reporting the Treasurer is expected to provide appropriate guidance, ensuring that there are essential controls and procedures in place for the proper management of church funds. This includes keeping full and accurate accounting records of all income due to the church as well as proper records of expenditure, both for restricted and unrestricted church funds, within policies established by the Charities Commission, the Church of England and the PCC.

The following summary of key financial controls covers a number of areas where more extensive documented procedures should also exist.

3 Budgetary Control

An important element of good financial control is the use of budgets which, if effective, have the following benefits:

- They enable the PCC to determine plans and priorities for the use of the church's resources
- They help give early warning of potential financial problems
- They enable the PCC and the Treasurer to monitor actual outcomes against expectations and to take corrective action when unexpected or undesirable outcomes occur.

The budget should include best estimates of income and expenditure required to meet the essential objectives set by the PCC.

Those responsible for incurring expenditure (Budget Holders) should endeavour to manage such expenditure so that it remains within the allocated budget and should only exceed the approved budget with appropriate prior approval.

The Treasurer should present a draft budget for the following year to be considered by the PCC at its November meeting. The final budget should be presented for approval by the PCC at its January meeting.

The Treasurer should monitor actual outcomes against expectations and report to the PCC on material variances between actual income and expenditure and budget on a quarterly basis. The Treasurer should provide a more formal report at the half year and full year. Where material variances occur which significantly affect the full year outcome, the Treasurer should additionally provide a forecast of the full year result to allow the PCC to consider relevant action at the earliest opportunity.

The PCC, via the Treasurer, may delegate responsibility for the preparation of budget sections (either income or expenditure) to additional individuals. It is then the responsibility of the delegated individual to seek appropriate approval for expenditure which cannot be met from the delegated budget.

5 Commitment to incur Expenditure

Expenditure incurred by St Nicolas should be valid, authorised, accurately recorded and incurred only for purposes within the objects of the church. Restricted funds should only be spent on the purpose for which they were given.

Any individual who commits St Nicolas to expenditure should ensure such expenditure is within the allocated budget and should only exceed the budget if further appropriate approval is given.

If individuals other than Budget Holders commit St Nicolas to expenditure they should agree this with the relevant Budget Holder in advance. It is the responsibility of each Budget Holder to ensure expenditure is within budget, or if not, to seek appropriate additional approval.

The following considerations should apply before an individual commits St Nicolas to potential expenditure:

- Is the expenditure necessary to achieve the church mission and ministry (its objects)?
- Is the expenditure essential or unavoidable (eg. legal necessity)?
- If the expenditure is optional or discretionary has it been agreed in principle by the PCC?
- Is the expenditure budgeted?
- Is the expenditure reasonable in respect of the church and of the supplier?
- Is the cost less than £1,000?

Only if all of these conditions are met should expenditure be committed without the need for appropriate additional approval.

No individual or Committee should commit to expenditure on any item or service exceeding £1,000 without prior approval of the PCC.

Project expenditure, where there are multiple commitments over time totalling more than £1,000, but relating to a single substantial objective (eg. building alterations), require a single approval from the PCC prior to commitment.

For expenditure on items in excess of £1,000, whether budgeted or not, a full specification of requirements should be provided to potential suppliers. This ensures any necessary quotations are provided on a consistent basis. A proposal should be provided to the PCC including a recommendation as to which quotation it is proposed to accept.

Normally one quotation should be obtained for purchases or project expenditure between £1,000 and £3,000. Two quotations should be obtained for expenditure between £3,000 and £5,000. Three quotations should be obtained for expenditure above £5,000.

The Fabric Committee will maintain a list of preferred suppliers/contractors for work specified on the church and its ancillary buildings. These will be suppliers/contractors who have been used previously and have completed work to a high standard and at a reasonable price. Where only one quote is obtained the supplier/contractor must be selected from the preferred list.

In addition enquiries should be made of the experiences of other churches or the Diocese to ensure that the expenditure is likely to represent value for money.

A proposal, including the recommended quote, should be presented to the PCC for approval. The proposal should clarify which fund will be looked upon to provide the necessary finance. In addition it should clarify whether VAT is likely to be recoverable on certain fabric expenditure. For this reason the Treasurer should be consulted prior to the proposal being submitted to the PCC.

In addition, if doubt exists as to whether the expenditure satisfies the above guidelines, the matter should be referred to the Treasurer for consideration prior to any commitments being made.

For smaller items of unbudgeted expenditure up to £400 the Treasurer should have the authority to approve the expenditure without recourse to the PCC. For items of unbudgeted expenditure between £400 and £1,000 the Standing Committee may approve the expenditure.

The Standing Committee may authorise budgeted or unbudgeted expenditure over £1,000 in an emergency between PCC meetings or to deal with sensitive matters that it would not normally be appropriate to discuss in the full PCC, provided that it is reported to the PCC at the first appropriate opportunity.

6 Invoice Approval

Although the budget as a whole has been approved by the PCC, the PCC expects individual invoices for goods or services (including project expenditure) to be separately approved before payment so as to verify that the expenditure was incurred only for purposes within the objects of the church, that the goods have been received and are fit for purpose or that work done or services rendered have been satisfactorily completed and that the prices charged are correct and in line with any quotations received. This approval should be evidenced on the invoice by the words ‘OK to pay’ and the initials of the approver (normally the Budget Holder)

7 Payment

Once an invoice or personal expense claim has been approved it can be passed to the Treasurer for payment. Currently payment is usually made by use of the CAF bank on line payment process.

When payment of approved invoices or personal expense claims is made by cheque, two signatures are required (except for amounts up to £400 where the Treasurer can sign singly).

For the on line payment process there is a requirement for two individuals to process the payment in all cases without any small amount concession. Currently the process requires the Treasurer to initiate the payment and either of the two Church Wardens to authorise it. The Treasurer ensures that an approved invoice or other relevant documentation is in place before initiating the payment and confirms this to the payment authorisers before they carry out their part of the payment process. The payment authorisers complete the process on line which then releases the BACS payment to the supplier.

On a sample basis the authorisers may ask to examine the approved invoice or other documentation before completing the payment authorisation as an added security measure.

The establishment of Standing Orders and Direct Debits (eg. for the payment of utility bills) requires two authorised signatories.

8 Authorised Signatories

Authorised signatories are as set out in the mandates for the operation of the various bank accounts used by the church. In general they will include the Treasurer and the Church Wardens. Copies of the mandates are retained by the Treasurer.

9 Personal Expense Claims

For smaller items of expenditure, generally individually less than £50, an individual may purchase goods or incur expenditure and then claim reimbursement of personal expenditure (using a standard expense claim document). In these cases the commitment to incur such expenditure should have been evaluated against the criteria set out in Section 5 above prior to purchase.

Claims for reimbursement of personal expenses should be submitted on the standard expense form, signed by the claimant, and supported by necessary vouchers in all cases. Claims should be approved by the Rector, a Church Warden, a Deputy Church Warden or a line manager as appropriate. Any claims not supported by adequate supporting vouchers may be referred by the Treasurer to a Church Warden for approval before payment.

Treasurer
St Nicolas, Great Bookham
Updated July 2014

St Nicolas Great Bookham

PCC Financial Liability

The Parochial Church Council (PCC) is a statutory body registered as charity number 1127867. Claims against a PCC are limited to the extent of the PCC's assets. However the status of the individual members of the PCC is that of a charitable trustee, and personal liability can be incurred in the event of gross negligence in undertaking their duties.

The essential principles that should be remembered by members of the PCC in order to mitigate this potential liability when carrying out their role as trustees are as follows:

- A duty of **compliance** with charity and church law
- A duty of **prudence** ensuring that the church is solvent, is using its funds wisely and not exposing the church to undue risk
- A duty of **care** using care, skill and experience in undertaking church activities (which includes seeking appropriate advice from experts where necessary)

The following examples illustrate how these principles may be translated into a sensible approach to significant activities undertaken by the church:

- Any powers delegated to committees, working groups or individuals should be clearly communicated, understood, documented and properly approved
- Progress on key activities or projects should be regularly reported to the PCC and any major proposals discussed and key decisions minuted

All PCC members are advised to read and understand the publication 'The essential trustee : What you need to know' which is available on line from the Charity Commission web site

The church's 'Parishguard' insurance policy provides trustee indemnity insurance up to £100,000 in any one period of insurance. This covers wrongful acts (but not wilful or deliberate acts) giving rise to a claim against an individual trustee or the PCC as a whole.

Approved by the PCC on 12 November 2012

St Nicolas Great Bookham

GENERAL PRIVACY NOTICE

1 Your personal data – what is it?

1.1 "Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be by the information alone or in conjunction with any other information. The processing of personal data is governed by the Data Protection Bill/Act 2017 the General Data Protection Regulation 2016/679 (the "GDPR" and other legislation relating to personal data and rights such as the Human Rights Act 1998.

2 Who are we?

2.1 This Privacy Notice is provided to you by the Parochial Church Council (PCC) of St Nicolas Great Bookham which is the data controller for your data.

2.2 The Church of England is made up of a number of different organisations and office-holders who work together to deliver the Church's mission in each community. The PCC works together with:

- the incumbent and clergy of the parish (that is, our Rector and ordained ministers);
- the bishops of the Diocese of Guildford;

2.3 As the Church is made up of all of these persons and organisations working together, we may need to share personal data we hold with them so that they can carry out their responsibilities to the Church and our community. The organisations referred to above are joint data controllers. This means we are all responsible to you for how we process your data.

2.4 Each of the data controllers have their own tasks within the Church and a description of what data is processed and for what purpose is set out in this Privacy Notice. This Privacy Notice is sent to you by the PCC on our own behalf and on behalf of each of these data controllers. In the rest of this Privacy Notice, we use the word "we" to refer to each data controller, as appropriate.

3 What data do the data controllers listed above process?

3.1 They will process some or all of the following where necessary to perform their tasks:

- Names, titles, and aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to our mission, or where you provide them to us, we may process demographic information such as gender, age, date of birth, marital status, nationality, education/work histories, academic/professional qualifications, hobbies, family composition, and dependants;
- Where you make donations or pay for activities such as use of a church hall, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;

4 How do we process your personal data?

4.1 The data controllers will comply with their legal obligations to keep personal data up to date; to store and destroy it securely; to not collect or retain excessive amounts of data; to keep personal data secure, and to protect personal data from loss, misuse, unauthorised access and disclosure and to ensure that appropriate technical measures are in place to protect personal data.

4.2 We use your personal data for some or all of the following purposes:

- To enable us to meet all legal and statutory obligations (which include maintaining and publishing our electoral roll in accordance with the Church Representation Rules);
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments;
- To minister to you and provide you with pastoral and spiritual care (such as visiting you when you are gravely ill or bereaved) and to organise and perform ecclesiastical services for you, such as baptisms, confirmations, weddings and funerals;
- To deliver the Church's mission to our community, and to carry out any other voluntary or charitable activities for the benefit of the public as provided for in the constitution and statutory framework of each data controller;
- To administer the parish, deanery, archdeaconry and diocesan membership records;
- To fundraise and promote the interests of the Church and charity;
- To maintain our own accounts and records;
- To process a donation that you have made (including Gift Aid information);
- To seek your views or comments;
- To notify you of changes to our services, events and role holders;
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other fundraising activities;
- To process a grant or application for a role;
- To enable us to provide a voluntary service for the benefit of the public in a particular geographical area as specified in our constitution;

5 What is the legal basis for processing your personal data?

5.1 Most of our data is processed because it is necessary for our legitimate interests, or the legitimate interests of a third party (such as another organisation in the Church of England). An example of this would be our safeguarding work to protect children and adults at risk. We will always take into account your interests, rights and freedoms.

5.2 Some of our processing is necessary for compliance with a legal obligation. For example, we are required by the Church Representation Rules to administer and publish the electoral roll, and under Canon Law to announce forthcoming weddings by means of the publication of banns.

5.3 We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. An example of this would be processing your data in connection with the hire of church facilities.

5.4 Religious organisations are also permitted to process information about your religious beliefs to administer membership or contact details.

5.5 Where your information is used other than in accordance with one of these legal bases, we will first obtain your consent to that use.

6 Sharing your personal data

6.1 Your personal data will be treated as strictly confidential. It will only be shared with third parties where it is necessary for the performance of our tasks or where you first give us your prior consent. It is likely that we will need to share your data with some or all of the following (but only where necessary):

- The appropriate bodies of the Church of England including the other data controllers;
- Our agents, servants and contractors. For example, we may ask a commercial provider to send out newsletters on our behalf, or to maintain our database software;
- Other clergy or lay persons nominated or licensed by the bishops of the Diocese of Guildford to support the mission of the Church in our parish. For example, our clergy are supported by our area dean and archdeacon, who may provide confidential mentoring and pastoral support. Assistant or temporary ministers, including curates, deacons, licensed lay ministers, commissioned lay ministers or persons with Bishop's Permissions may participate in our mission in support of our regular clergy;
- On occasion, other churches with which we are carrying out joint events or activities.

7 How long do we keep your personal data?

7.1 We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is current best practice to keep financial records for a minimum period of 7 years to support HMRC audits. In general, we will endeavour to keep data only for as long as we need it. This means that we may delete it when it is no longer needed.

8 Your rights and your personal data

8.1 You have the following rights with respect to your personal data:

8.2 When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

8.2.1 The right to access information we hold on you

- At any point you can contact us to request the information we hold on you as well as why we have that information, who has access to the information and where we obtained the information from. Once we have received your request we will respond within one month.
- There are no fees or charges for the first request but additional requests for the same data may be subject to an administrative fee .

8.2.2 The right to correct and update the information we hold on you

- If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

8.2.3 The right to have your information erased

- If you feel that we should no longer be using your data or that we are illegally using your data, you can request that we erase the data we hold.
- When we receive your request we will confirm whether the data has been deleted or the reason why it cannot be deleted (for example because we need it for our legitimate interests or regulatory purpose(s)).

8.2.4 The right to object to processing of your data

- You have the right to request that we stop processing your data. Upon receiving the request we will contact you and let you know if we are able to comply or if we have legitimate grounds to continue to process your data. Even after you exercise your right to object, we may continue to hold your data to comply with your other rights or to bring or defend legal claims.

8.2.5 The right to data portability

- You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

8.2.6 The right to withdraw your consent to the processing at any time for any processing of data to which consent was sought.

- You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

8.2.7 The right to object to the processing of personal data where applicable.

8.2.8 The right to lodge a complaint with the Information Commissioner's Office.

9 Transfer of Data Abroad

9.1 Any electronic personal data transferred to countries or territories outside the EU will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

10 Further processing

10.1 If we wish to use your personal data for a new purpose, not covered by this Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

11 Changes to this notice

We keep this Privacy Notice under regular review and we will place any updates on our website. This Notice was last updated in May 2018 and adopted by the PCC on 14th May 2018. It is due for review no later than November 2018.

12 Contact Details

12.1 Please contact us if you have any questions about this Privacy Notice or the information we hold about you or to exercise all relevant rights, queries or complaints at:

The Data Controller,
St Nicolas Church Parish Office,
2a Fife Way
Great Bookham
Surrey
KT23 3PH
Email: GDPR@stnicolasbookham.org.uk

12.2 You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

St Nicolas Great Bookham

PRIVACY NOTICE - ROLE HOLDERS

(e.g. Churchwardens, PCC Secretaries, PCC Treasurers, Deanery Synod reps, Safeguarding officers etc.)

1 Your personal data – what is it?

1.1 "Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be by the information alone or in conjunction with any other information. The processing of personal data is governed by *the Data Protection Bill/Act 2017 the General Data Protection Regulation 2016/679 (the "GDPR" and other legislation relating to personal data and rights such as the Human Rights Act 1998.*

2 Who are we?

2.1 This Privacy Notice is provided to you by the Parochial Church Council (PCC) of St Nicolas Great Bookham which is the data controller for your data.

2.2 The Church of England is made up of a number of different organisations and office-holders who work together to deliver the Church's mission in each community. The PCC works together with:

- the incumbent and clergy of the parish (that is, our Rector and other ordained ministers);
- the bishops of the Diocese of Guildford;

2.3 As the Church is made up of all of these persons and organisations working together, we may need to share personal data we hold with them so that they can carry out their responsibilities to the Church and our community. The organisations referred to above are joint data controllers. This means we are all responsible to you for how we process your data.

2.4 Each of the data controllers has their own tasks within the Church and a description of what data is processed and for what purpose is set out in this Privacy Notice. This Privacy Notice is sent to you by the PCC on our own behalf and on behalf of each of these data controllers. In the rest of this Privacy Notice, we use the word "we" to refer to each data controller, as appropriate.

3 How do we process your personal data?

3.1 The data controllers will comply with their legal obligations to keep personal data up to date; to store and destroy it securely; to not collect or retain excessive amounts of data; to keep personal data secure, and to protect personal data from loss, misuse, unauthorised access and disclosure and to ensure that appropriate technical measures are in place to protect personal data.

3.2 We use your personal data for some or all of the following purposes (for example some of the role-holders are volunteers and no financial information will be processed for these role holders):

- To enable those who undertake pastoral care duties as appropriate (e.g. visiting the bereaved);
- To enable us to meet all legal and statutory obligations (which include maintaining and publishing our electoral roll in accordance with the Church Representation Rules);

- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments;
- To deliver the Church's mission to our community, and to carry out any other voluntary or charitable activities for the benefit of the public as provided for in the constitution and statutory framework of each data controller;
- To administer the parish, deanery, archdeaconry and diocesan membership records;
- To fundraise and promote the interests of the church and charity;
- To manage our employees and volunteers;
- To maintain our own accounts and records;
- To seek your views or comments;
- To notify you of changes to our services, events and role holders
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other fundraising activities;
- To process a grant or application for a role;
- To enable us to provide a voluntary service for the benefit of the public in a particular geographical area as specified in our constitution;
- To share your contact details with the Diocesan office so they can keep you informed about news in the diocese and events, activities and services that will be occurring in the diocese and in which you may be interested.
- We will process data about role holders for legal, personnel, administrative and management purposes and to enable us to meet our legal obligations, for example to pay role-holders, monitor their performance and to confer benefits in connection with your engagement as a Role Holder. "Role Holders" includes volunteers, employees, contractors, agents, staff, retirees, temporary employees, beneficiaries, workers, treasurers and other role holders.
- We may process sensitive personal data relating to Role Holders including, as appropriate:
  - information about an Role Holder's physical or mental health or condition in order to monitor sick leave and take decisions as to the Role Holder's fitness for work;
  - the Role Holder's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
  - in order to comply with legal requirements and obligations to third parties.

4 What data do the data controllers listed above process?

4.1 They will process some or all of the following where necessary to perform their tasks:

- Names, titles, and aliases, photographs.
- Contact details such as telephone numbers, addresses, and email addresses.
- Where they are relevant to our mission, or where you provide them to us, we may process demographic information such as gender, age, date of birth, marital status, nationality, education/work histories, academic/professional qualifications, employment details, hobbies, family composition, and dependants.
- Non-financial identifiers such as passport numbers, driving license numbers, vehicle registration numbers, taxpayer identification numbers, employee identification numbers, tax reference codes, and national insurance numbers.
- Financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.

- Financial information such as salary, bonus, record of earnings, tax code, tax and benefits contributions, expenses claimed, creditworthiness, car allowance (if applicable), amounts insured, and amounts claimed.
- Other employee data (not covered above) relating to Role Holders including emergency contact information; gender, birth date, referral source (e.g. agency, employee referral); level, performance management information, languages and proficiency; licences/certificates, citizenship, immigration status; employment status, retirement date; billing rates, office location, practice and speciality; publication and awards for articles, books etc.; prior job history, employment references and personal biographies.

5 What is the legal basis for processing your personal data?

5.1 Most of our data is processed because it is necessary for our legitimate interests, or the legitimate interests of a third party (such as another organisation in the Church of England). An example of this would be our safeguarding work to protect children and adults at risk. We will always take into account your interests, rights and freedoms.

5.2 Some of our processing is necessary for compliance with a legal obligation. For example, we are required by the Church Representation Rules to administer and publish the electoral roll, and under Canon Law to announce forthcoming weddings by means of the publication of banns.

5.3 We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. An example of this would be processing your data in connection with the hire of church facilities.

5.4 We will also process your data in order to assist you in fulfilling your role in the church including pastoral and administrative support or if processing is necessary for compliance with a legal obligation.

5.5 Religious organisations are also permitted to process information about your religious beliefs to administer membership or contact details.

5.6 Where your information is used other than in accordance with one of these legal bases, we will first obtain your consent to that use.

6 Sharing your personal data

6.1 Your personal data will be treated as strictly confidential. It will only be shared with third parties including other data controllers where it is necessary for the performance of the data controllers' tasks or where you first give us your prior consent. It is likely that we will need to share your data with:

- The appropriate bodies of the Church of England including the other data controllers;
- Our agents, servants and contractors. For example, we may ask a commercial provider to send out newsletters on our behalf, or to maintain our database software;
- Other clergy or lay persons nominated or licensed by the bishops of the Diocese of Guildford to support the mission of the Church in our parish. For example, our clergy are supported by our area dean and archdeacon, who may provide confidential mentoring and pastoral support. Assistant or temporary ministers, including curates, deacons, licensed lay ministers, commissioned lay ministers or persons with Bishop's Permissions may participate in our mission in support of our regular clergy;

7 How long do we keep your personal data?

7.1 We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is current best practice to keep financial records for a minimum period of 7 years to support HMRC audits. In general, we will endeavour to keep data only for as long as we need it. This means that we may delete it when it is no longer needed.

8 Your rights and your personal data

8.1 You have the following rights with respect to your personal data:

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

8.1.1 The right to access information we hold on you

- At any point you can contact us to request the information we hold on you as well as why we have that information, who has access to the information and where we obtained the information from. Once we have received your request we will respond within one month.
- There are no fees or charges for the first request but additional requests for the same data may be subject to an administrative fee .

8.1.2 The right to correct and update the information we hold on you

- If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

8.1.3 The right to have your information erased

- If you feel that we should no longer be using your data or that we are illegally using your data, you can request that we erase the data we hold.
- When we receive your request we will confirm whether the data has been deleted or the reason why it cannot be deleted (for example because we need it for our legitimate interests or regulatory purpose(s)).

8.1.4 The right to object to processing of your data

- You have the right to request that we stop processing your data. Upon receiving the request we will contact you and let you know if we are able to comply or if we have legitimate grounds to continue to process your data. Even after you exercise your right to object, we may continue to hold your data to comply with your other rights or to bring or defend legal claims.

8.1.5 The right to data portability

- You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

8.1.6 The right to withdraw your consent to the processing at any time for any processing of data to which consent was sought.

- You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

8.1.7 The right to object to the processing of personal data where applicable.

8.1.8 The right to lodge a complaint with the Information Commissioners Office.

9 Transfer of Data Abroad

9.1 Any electronic personal data transferred to countries or territories outside the EU will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

10 Further processing

10.1 If we wish to use your personal data for a new purpose, not covered by this Data Protection Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

11 Changes to this notice

11.1 We keep this Privacy Notice under regular review and we will place any updates on our website. This Notice was last updated in May 2018 and adopted by the PCC on 14th May 2018.

12 Contact Details

12.1 Please contact us if you have any questions about this Privacy Notice or the information we hold about you or to exercise all relevant rights, queries or complaints at:

The Data Controller,
St Nicolas Church Parish Office,
2a Fife Way
Great Bookham
Surrey
KT23 3PH
Email: GDPR@stnicolasbookham.org.uk

12.2 You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

St Nicolas Great Bookham

DATA BREACH PROCEDURE

1 Policy Statement

1.1 The PCC of St Nicolas Great Bookham holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by the Parish and all members of the clergy, lay ministers, parish staff, volunteers and contractors, referred to herein after as 'staff'.

2 Purpose

2.1 This breach procedure sets out the course of action to be followed by all staff at St Nicolas Great Bookham if a data protection breach takes place.

3 Legal Context

Article 33 of the General Data Protection Regulations
Notification of a personal data breach to the supervisory authority

3.1 In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

3.2 The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3.3 The notification referred to in paragraph 3.1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
(c) describe the likely consequences of the personal data breach;
(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

3.4 Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

3.5 The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

4 Types of Breach

4.1 Data protection breaches could be caused by a number of factors. A number of examples are shown below:

(a) Loss or theft of church members, staff or PCC data and/ or equipment on which data is stored;
(b) Inappropriate access controls allowing unauthorised use;
(c) Equipment Failure;
(d) Poor data destruction procedures;
(e) Human Error;
(f) Cyber-attack;
(g) Hacking.

5 Managing a Data Breach

5.1 In the event that the Parish identifies or is notified of a personal data breach, the following steps should followed:

5.1.1 The person who discovers/receives a report of a breach must inform the Incumbent and Parish Office or, in their absence, either the PCC Secretary and/or the Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

5.1.2 The Incumbent/DPO (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the Parish Administrator.

5.1.3 The Incumbent/DPO (or nominated representative) must inform the PCC Secretary as soon as possible. As the Data Controller, it is the PCC's responsibility to take the appropriate action and conduct any investigation.

5.1.4 The Incumbent/DPO (or nominated representative) must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the PCC's or Diocesan legal support should be obtained.

5.1.5 The Incumbent/DPO (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage.

5.2 Steps might include:

5.2.1 Attempting to recover lost equipment.

5.2.2 Contacting the relevant Diocesan Authorities, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all church members. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the Incumbent/DPO (or nominated representative).

5.2.3 The use of back-ups to restore lost/damaged/stolen data.

5.2.4 If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

5.2.5 If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed

6 Investigation

6.1 In most cases, the next stage would be for the Incumbent/DPO (or nominated representative) to fully investigate the breach. The Incumbent/DPO (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation.

6.2 The investigation should consider:

Article I.	The type of data;
Article II.	Its sensitivity;
Article III.	What protections were in place (e.g. encryption);
Article IV.	What has happened to the data;
Article V.	Whether the data could be put to any illegal or inappropriate use;
Article VI.	How many people are affected;
Article VII.	What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

6.3 A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

7 Notification

7.1 Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The Incumbent/DPO (or nominated representative) should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

7.2 When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the Parish is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish. The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach.

8 Review and Evaluation

8.1 Once the initial aftermath of the breach is over, the Incumbent/DPO (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Standing Committee Meeting and Full PCC meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the person leading the investigation should liaise with the Standing and Finance Committee for advice and guidance. This breach procedure

may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

9 Implementation

9.1 The PCC should ensure that staff are aware of the Church's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the Church's Data Protection policy and associated procedures, they should discuss this with the DPO or the Incumbent.

10 Contact Details

10.1 Please contact us if you have any questions about this Procedure or the information we hold about you or to exercise all relevant rights, queries or complaints at:

The Data Controller,
St Nicolas Church Parish Office,
2a Fife Way
Great Bookham
Surrey
KT23 3PH
Email: GDPR@stnicolasbookham.org.uk

10.2 You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

PAROCHIAL CHURCH COUNCIL OF ST NICOLAS GREAT BOOKHAM

CONFLICT OF INTEREST GUIDANCE

Preamble

Those responsible for administering a charity (the 'charity trustees') must act in the best interests of the charity. Amongst other things, that requires them to avoid anything that prevents decisions being taken by reference to other considerations. It also follows that charity trustees need to avoid putting themselves in a position in which their duty to act only in the best interests of the charity could conflict with any personal interest they may have.

This has implications in practice for both individual charity trustees and for the charity trustees collectively:

- individual charity trustees must identify and declare any conflict of interest on their part; and
- the charity trustees collectively must ensure that they have arrangements in place that enable conflicts of interest to be identified and dealt with effectively.

The early identification of conflicts of interest is therefore key to ensuring that both individual charity trustees and the charity trustees collectively do what is expected of them.

Conflict of interest guidance is designed to ensure that the discussions and decisions of the charity trustees are not influenced by any other interests. Its purpose is to make sure that everything that may affect an individual charity trustee's contribution to a decision is identified, dealt with appropriately and recorded. For general guidance to charities, you may find the Charity Commission's guidance on this helpful[1].

A Parochial Church Council (PCC) is in no different a position in these respects from any other charity. Its charity trustees (i.e. all the individual members of the PCC) are under a legal obligation to act in its best interests. The church does not, however, operate in a vacuum: both it and its members form an integral part of the life of the community. This can give rise to conflicts of interest for individual members of the PCC where the best interests of the PCC may be at odds with those of other community organizations. And other conflicts of interest may arise from personal or family circumstances.

Where a conflict of interest is not identified and dealt with appropriately, it can result in decisions or actions that are not in the best interests of the PCC and/or which, in the case of interests of a personal kind, can confer an unauthorised benefit on one or more members of the PCC. [See also the Parish Resources *Guidance Note: PCC members and private benefit*[2]]

---

[1] https://www.gov.uk/guidance/manage-a-conflict-of-interest-in-your-charity

[2] http://www.parishresources.org.uk/wp-content/uploads/remunerationguidance.pdf

Conflicts of interest can take many forms. Some will make it inappropriate for the individual to participate in a discussion or decision; others may simply need to be identified and declared, so allowing the individual to continue to contribute their experience and expertise to the matter at hand.

Guidance

1. This Guidance applies to all members of the PCC, the Standing Committee and any other committees or working parties set up by the PCC.
2. A conflict of interest is any situation in which a member's personal interests or loyalties could prevent, or could be seen to prevent, the member from making a decision only in the best interests of the PCC. Such a situation may arise either:
   (a) where there is a potential financial benefit to a member, whether directly or indirectly through a connected person (such as a close family member or business partner); or
   (b) where a member's duty to the PCC may compete with a duty of loyalty he or she owes to another organization or person (e.g. by virtue of being a trustee or committee member of a body which has an interest in the matter).
3. It is desirable that any conflicts of interest are declared to the Chair of the meeting as soon as the agenda is circulated. They must also be declared at the meeting when the relevant agenda item is reached.
4. Subject to paragraph 6, where a conflict of interest arises in connection with a personal benefit, the member concerned must withdraw from the meeting and not take part in any discussions relating to it (including discussions for the purpose of obtaining any authority from the Charity Commission that would be required to authorize the benefit – see the *Guidance Note: PCC members and private benefit*).
5. Subject to paragraph 6, where a conflict of loyalty arises, the PCC will consider what level of participation, if any, is acceptable on the part of the conflicted member, having regard to the duty to act in the best interests of the PCC. However, the normal expectation will be that the conflicted member should withdraw from the meeting during discussion of the item of business in question.
6. A member need not withdraw from a meeting if his or her interest (whether financial or non-financial) is common to a class of persons and is neither (i) significant nor (ii) substantially greater than the interests of other members of that class.
7. The existence of a conflict of interest must be recorded in the minutes, together with the decision as to how it should be dealt with.