St Nicholas, Old Marston, Oxford

DATA PROTECTION POLICY

1. Introduction to data protection

During the course of its activities as a church and to carry out its duties under ecclesiastical law and various "Measures", St Nicholas as a church and its PCC collects, stores and processes personal data about members of the congregation (such as electoral roll, gift aid information, time & talents, baptisms, funerals, weddings, junior church, crèche, pulse members, holiday club, coffee pot, safeguarding, choirs, social events, sides persons, sub-committees, prayer & support network, Marston Times, church hirers, toddler group members, allergies, next of kin etc., staff contractors and other people with whom we deal. We will do this correctly and lawfully, and in accordance with the data protection legislation, predominantly the General Data Protection Regulation 2016 ("GDPR") and the Data Protection Act 2018 ("DPA 2018").

St Nicholas/the PCC is obliged to comply with this policy when processing personal data. Any breach of this policy may result in disciplinary action for employees and could lead to the termination of contract/ engagement for those who are not employees.

2. Background to the GDPR and DPA 2018

The purpose of the GDPR and DPA 2018 is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge and that it is processed in line with lawful conditions (of which consent is one).

The legislation applies to the processing of personal data by automated means (i.e. by computer) and to processing as part of a filing system (i.e. certain categories of paper records).

3. Definitions used by St Nicholas/PCC (from the GDPR)

Personal data – any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, concerning a natural person's sex life or sexual orientation. GDPR treats data relating to criminal offences/convictions separately; however, for the purposes of this policy, we include this data within "special categories of personal data".

Data controller – the natural or legal person, public authority, (church), agency or other body which, alone or jointly with others, determine the purposes and means of the processing of personal data; where the purpose and means of such processing are determined by the EU or Members State law, the controller or the specific criteria for its nomination may be provided by EU or Member State law.

Data processor - a natural or legal person, public authority, (church), agency or other body which processes personal data on behalf of the controller.

Data subject - any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to,

personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent – means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he/she, by a statement or by a clear affirmative action, signifies agreement to the processing of their personal data.

Third party – a natural or legal, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

4. Policy Statement

This policy applies to members of the PCC, staff, contractors and workers of St Nicholas. It does not form part of any employee's contract of employment and may be amended at any time. For simplicity, this policy refers to the obligations of St Nicholas/PCC and its staff throughout but for the avoidance of doubt this includes members of the congregation who process personal data, contractors and other workers. For the sake of transparency, this policy is also published on our website for others/third parties to see how we process personal data fairly, lawfully and transparently and in accordance with the GDPR and DPA 2018.

We recognise the importance of data protection in maintaining trust and confidence in the church generally and St Nicholas in particular.

The PCC is committed to compliance with the GDPR and, in turn the DPA 2018 and the protection of the "rights" of individuals whose information we collect and process.

Compliance with GDPR and DPA 2018 is described by this policy and other relevant policies and procedures such as Privacy Notices, Data Retention Policy, Personal data breach management policy and procedure, IT & Communications Systems Policy and Procedure (where they exist).

This policy applies to all of St Nicholas/PCC personal data processing functions, including those performed on personal data of or received from employees,

contractors and other workers of St Nicholas/PCC, and other people that St Nicholas/PCC deal with.

The Data Protection/Contact Person ("DPO") is responsible for reviewing the processing annually in the light of any changes of St Nicholas/PCC activities and to any additional requirements identified by means of data protection impact assessments. The register will be made available on request by the Information Commissioner's Office ("ICO").

Any breach of the GDPR or DPA 2018 or of this policy will be dealt with under St Nicholas/PCC "disciplinary policy" and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

5. Responsibilities and roles under the DPA 2018

St Nicholas/PCC is a data controller under the GDPR in relation to the large amount of personal data we collect and may also be a data processor in relation to other personal data from other data controllers.

Compliance with the DPA 2018 is the responsibility of every member of the PCC – all those who process personal data, which can include merely accessing or receiving such data as part of their role.

The PCC must ensure that any personal data they hold is accurate and up-to-date (including where appropriate relating to dependents, next of kin etc).

The PCC, DPO/Contact Person and those with managerial or supervisory roles are responsible for developing and encouraging good information handling practices at St Nicholas.

The DPO/Contact Person is accountable to the PCC (Vicar) for all the management of personal data and ensuring that compliance with GDPR and DPA 2018 and good practice can be demonstrated. This accountability includes development and implementation of the DPA 2018 compliance as required by this policy.

The DPO/Contact Person has specific responsibilities in respect of procedures and is the first point of call for the PCC, members of the congregation and third parties seeking clarification on any aspect of data protection compliance.

6. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR.

St Nicholas/PCC's policies and procedures are designed to ensure compliance with these principles, though it should be noted that there are exceptions which apply to these overarching values.

Principle 1: Personal data must be processed lawfully, fairly and transparently.

Lawfully: St Nicholas/PCC must identify a lawful basis before we can process personal data. This is often referred to as the "condition for processing".
Fairly: In order for processing to be fair, St Nicholas/PCC must make certain information available to the data subjects as required under the GDPR regardless of whether the personal data was obtained directly from the data subjects or from other sources.
Transparently: The GDPR includes comprehensive requirements for the PCC to provide privacy information to data subjects. These are detailed and specific, placing emphasis on making privacy notices understandable and accessible. Please note that, in certain circumstances, it may not always be appropriate to alert every data subject about the processing activities that PCC undertakes on behalf of St Nicholas. Where disclosure of personal data is necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings); necessary for the purpose of obtaining legal advice; necessary for the purpose of establishing, exercising or defending legal rights, transparency is not always required where to do so would prevent the PCC from making the disclosure.

Principle 2: Personal data can only be collected for specific, explicit and legitimate purposes.

Data obtained for specified purposes by St Nicholas/PCC must not be used for a purpose that differs from those formally notified to data subjects. If St Nicholas/PCC wishes to use the personal data for a different purpose, it will notify the data subjects prior to the new processing taking place and will ensure that a lawful condition applies before undertaking the new activity.

Principle 3: Personal data must be adequate, relevant and limited to what is necessary for processing (aka "data minimisation").

St Nicholas/PCC must not collect data that is not strictly necessary for the purpose for which it is obtained.

Principle 4: Personal data must be accurate and kept up to date with every effort to erase or rectify without delay.

Data already stored by St Nicholas/PCC must be reviewed and updated as necessary. Whilst usually no data should be kept unless it is reasonable to assume that it is accurate, there are again exceptions, particularly where it is necessary to keep a record of data as it existed at a given time.

St Nicholas/PCC reviews on at least an annual basis the retention dates of all the personal data processed and data which is no longer required to be held will be securely deleted/destroyed in line with the procedures set out in section 10 of this policy.

Principle 5: Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

It follows from the commentary for Principle 4 that wherever possible and practicable, if personal data is retained by St Nicholas/PCC beyond the processing date, access to it should be restricted (and it could also be minimised, encrypted or pseudonymised in order to protect the identity of the data subject in the event of a data breach).

The DPO/Contract Person/PCC must specifically approve any data retention that exceeds the retention periods defined in retention records procedures set out in section 10 of this Policy.

Principle 6: Personal data must be processed in a manner that ensures the appropriate security.

In determining appropriateness, the DPO/Contact Person/PCC will also consider the extent of possible damage or loss that might be caused to data subjects if security breach occurs, the effect of any security breach on St Nicholas/PCC, and any likely reputational damage including the possible loss of trust.

The additional "accountability" principle – the data controller must be able to demonstrate compliance with the other Principles.

The GDPR includes provisions that promote accountability and governance, including Article 5(2) which requires us to demonstrate compliance with the principles above.

St Nicholas/PCC demonstrates compliance by implementing policies, adhering to procedures and best practice, and implementing appropriate technical and organisational measures (including data protection by design and by default, breach notification procedures and incident plans etc).

7. Data subjects' rights

Data subjects may be able to exercise a number of rights in relation to the processing of their data by St Nicholas/PCC. These include the right to:

- Make access requests: regarding the nature of information held and to whom it has been disclosed (Subject Access Requests).
- Correction and deletion: rectify, block, erase (including the right to be forgotten) or destroy inaccurate data.
- Prevent processing: likely to cause damage or distress, or for the purposes of direct marketing.
- Complain to St Nicholas/PCC: relating to the processing of their personal data or handling of requests.
- Claim compensation: if they suffer damage by any contravening of the DPA 2018.
- Involve the ICO: to assess whether any provision of the DPA 2018 has been contravened.
- Portability: to have personal data transmitted to another controller.

Data subjects may make data access requests, which ensures that St Nicholas/PCC's response to the data access request complies with the requirements of the DPA 2018.

However, it should be noted that a data subject's right to be notified that St Nicholas/PCC even has their data in the first place, or their right to access, correction, erasure, etc, may be removed or curtailed where St Nicholas/PCC can show that it is necessary on the basis of compelling legitimate grounds, for

the compliance with a legal obligation or establishment, or the exercise or defence of legal claims.

8. Lawful basis for processing

The DPA 2018 is not intended to prevent the reasonable day -to-day processing of personal data, but to ensure that it is done lawfully, fairly and transparently.

For personal data to be processed lawfully, such data must be processed on the basis of one of the lawful grounds set out in the GDPR. These include (i) the data subject's consent to the processing, (ii) that the processing is necessary for the performance of a contract with the data subject, (iii) for the compliance with a legal obligation to which the data controller is subject, (iv) for the legitimate interest of the data controller or a third party or (v) for processing necessary for a public task set out in law. (In connection with special category personal data, i.e. sensitive personal data, a different condition must also be met.)

<u>Consent</u>

Consent is one of the lawful bases for processing personal data.
For consent to be valid, it must have been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by a clear affirmative action, signifies agreement to the processing of personal data relating to him/her.

As the data controller, if consent is being relied upon, St Nicholas/PCC must be able to demonstrate that consent was obtained for the processing operation, and that the data subject can then withdraw their consent at any time.

For these reasons, in practice, except in very limited circumstances, St Nicholas/PCC is unlikely to rely on consent as a lawful basis for processing any personal data.

For special categories of personal data, explicit written consent of data subject must be obtained unless an alternative basis for processing exists, such as

processing may be “necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement”.

Necessary for the performance of a contract with the data subject

This is lawful basis on which St Nicholas/PCC will often rely in relation to processing the personal data of its employees, contractors and other workers etc.

Compliance with a legal obligation to which the data controller is subject

This lawful basis can be relied upon when St Nicholas/PCC processes data in relation to records relating to weddings, gift aid declarations, PAYE, pensions and tax, by virtue of its legal obligation to comply with common law, ecclesiastical law, measures, statute and regulations.

Legitimate interest of the data controller or third party

St Nicholas/PCC will most commonly rely on this as a lawful basis for processing personal data that it is the legitimate interest of the church/PCC and/or third parties to do so. Such interests will differ according to the specific circumstances but, broadly, much of the processing undertaken by St Nicholas/PCC is likely to be in the legitimate interest of St Nicholas in carrying out its function/purpose as a church in the most effective way.

In respect of relying on legitimate interests as a lawful basis for processing personal data, St Nicholas/PCC will always consider the interests/ fundamental rights and freedoms of the data subject.

Necessary for the discharge of a public task

This lawful basis can be relied upon when St Nicholas/PCC processes data in exercise of official authority discharging functions and powers as a church/ worshiping community as set out in law. The processing must be *necessary* to the discharge of function or power. St Nicholas/PCC carries out the specific processing required in order to discharge its obligations under church law.

9. Security of data

The PCC and personnel holding personal data are responsible for ensuring that any personal data that St Nicholas processes and for which we are responsible as part of our roles, is kept securely and is not disclosed to any third party unless that third party has been specifically authorised by the PCC to receive that information and has entered into a contract recognising their role as a data processor (see section 16 below).

What follows are the "golden rules" for protecting personal data.

10. Retention and disposal of personal data

St Nicholas shall not keep personal data in a form and in such a manner that permits identification of data subjects longer than the PCC or church law has determined is necessary, in relation to the purposes for which the data was originally collected or for other purposes in accordance with law and best practice.

The retention period for different categories of personal data along with criteria used to determine this period will include legal or church regulations/obligations the church has to retain the data.

Personal data must be disposed of securely in accordance with the sixth principle of the DPA 2018 – which requires that such data is processed in an appropriate manner to maintain security, thereby protecting the rights and freedoms of data subjects.

11. Data outside the EEA

The default position under the Act is that all exports of data from within the European Economic Area ("EEA") to non- EEA countries are unlawful unless there is an appropriate "level of protection for the fundamental rights of data subjects" on the basis that one or more of the specified safeguards, or derogations apply. Providing a third party outside the EEA with access to personal data will amount to "transferring" or "exporting" such data.

We do not envisage transferring personal data outside the. If circumstances required that we transfer personal data outside the EEA, we will notify the PCC/DPO/Contact Person.

12. Accountability

Data protection impact assessments ("DPIA")

DPIAs will be carried out where required in relation to the processing of personal data by St Nicholas/PCC, and in relation to processing undertaken by third parties on behalf of St Nicholas/PCC This is where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of individuals.

Where as a result of a DPIA it is clear that St Nicholas is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not St Nicholas may proceed must be escalated for review to the PCC/DPO/Contact Person. If there are concerns, the DPO/Contact Person may need to escalate the matter to the ICO.

13. Personnel responsibilities and training

As noted, all members of the PCC and those with day-to-day responsibilities involving personal data and processing operations and those with permanent /regular access to personal data, must demonstrate compliance with the GDPR and, the DPA 2018. The PCC may also assign specific data protection responsibilities, including in connection with training ands awareness to the DPO/Contact Person as part of its policy and procedures on personal data management and accountability principle. For example, responsibilities in relation to the secure storage of electronically stored data and use of IT systems.

The DPO/Contact Person shall demonstrate and communicate to the PCC the importance of data protection and information security in their role and ensure that they understand how and why personal data is processed in accordance with our policies and procedures.

The DPO/Contact Person is responsible for organising training for all responsible individuals and personnel generally, and for maintaining records of the attendance of persons at relevant training at appropriate intervals.

All PCC members and those who regularly handle personal data, are required to undergo data protection and information security training appropriate to their role, including mandatory refresher training from time to time, and to

ensure that they are aware of their responsibilities and obligations with regards to data protection.

14. Data breach notices

Any information security breaches, near-misses, risks, weaknesses and events must be reported to the DPO/Contact Person, in their absence the Vicar, immediately after they are seen or experienced. Such issues could potentially range from major systems failures involving loss of services on one hand (e.g. caused by external threats) to minor breaches of information integrity on the other (e.g. email to the wrong recipient(s)). [A Person Data Breach Incident Management Policy may be required if necessary.]

15. Privacy Notices

St Nicholas/PCC will always be transparent in its processing of personal data, subject to the derogations and exceptions noted in this Policy.

St Nicholas/PCC will rarely collect personal data from data subject whilst relying on consent only as the lawful basis for processing. Where this is the case, St Nicholas/PCC will provide full and clear information on the processing purposes and in particular on the potential recipients.

When personal data has been obtained from a source other than the data subject, where required we will still take all reasonable steps to ensure and demonstrate that the processing is fair, transparent, which includes explaining the categories of personal data received by St Nicholas/PCC and the potential recipients if any.

Exceptions to the need to provide such information include:

- Where the data subject already has the information as it was provided to them by another party;
- If the provision of the above information proves impossible or would involve an excessive effort; or
- Where another exception applies which means that the provision of the privacy information is not required or not permissible.

16. Managing Data Processors

The PCC will only select contractors/ (suppliers to provide services to St Nicholas) who can provide adequate technical, physical and organisational security in accordance with the GDPR/DPA 2018.
When the supplier will meet the definition of the PCC's data processor, including when data processing activities are not the necessary reason for the contract, the PCC as a data controller will ensure that adequate security arrangements are provided for in the contract with the external processor and that the requirements of Article 28 of the GDPR are met.

If the DPO/Contact Person/PCC consider it necessary because of the nature of the personal data to be processed or because of the particular circumstances of the processing, an audit of the supplier's security arrangements may be conducted before entering into the contract.
Please ensure that you consult the PCC/DPO/Contact Person in advance of agreeing supplier contract terms, so that the centralised list of such suppliers is maintained.]

17. Making a subject accessor other request

If you reasonably believe that St Nicholas processes your personal data, you can submit a subject access or other request relating to rights under the GDPR/DPA Act 2018 to St Nicholas's DPO/Contact Person:

Name: Millius Palayiwa

Address: 27 Ouseley Close, Marston, Oxford, OX3 0JS

Telephone: 01865 725423, 07770 920 299

Email address: milliuspalayiwa@gmail.com

18. Complaints procedure

If you are dissatisfied with the DPO/Contact Person's response we would encourage that you discuss the decision with him. However, if an informal discussion does not resolve your complaint, you may submit it in writing to the

Vicar/PCC either by email to (email address: vicar@stnicholasmarston.org.uk) or by letter posted to the following address:
Name Reverend Skye Denno

Address: The Vicarage, Elsfield Road, Marston, Oxford, OX3 0PR

She will consider your complaint, and will confirm, reverse or amend the decision and advise you in writing of the outcome.

If you are dissatisfied with the response to your complaint you have the right to apply to the Information Commissioner for a decision as to whether the Church (St Nicholas) has dealt with your request for information in accordance with the requirements of the Data Protection Act legislation and the GDPR.

An application may be made to the Information Commissioner's Office by post to the following address:

Information Commissioner's Office
Casework and Advice Division
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF.

The Information Commissioner's telephone help line is **08456 306060** or 01625 545 745. The ICO's website is www.ico.gov.uk. You can access further information about making a complaint at http://www.ico.gov.uk/complaints/data/protection.aspx.

Millius Palayiwa
June 2018.

NB: This policy should be read in conjunction with other existing policies, briefing and guidance notes from the Diocese, and good practice that is in

existence for the time being. In particular, please see the following:-
https://www.oxford.anglican.org/support-services/general-data-protection-regulation-parishes/

How long to keep records:-
https://www.oxford.anglican.org/wp-content/uploads/2018/Keep-or-Bin.pdf

Advice about personal email addresses of volunteers:-
http://gdprforchurches.org.uk/your-responsibilities/volunteers-and-personal-email-addresses/