All Saints
NETTLEHAM PARISH CHURCH

DATA PROTECTION POLICY
JULY 2017
NETTLEHAM PCC ON BEHALF OF ALL SAINTS' NETTLEHAM
DIOCESE OF LINCOLN

POLICY STATEMENT

As a Data Controller, as defined under the Data Protection Act 1998 [DPA 1998] Nettleham PCC takes data protection very seriously and recognises the potential legal implications and reputational damage should data be compromised or misused in any way. Nettleham PCC is exempt from registration with the Information Commissioner's Office but must still meet the legal obligations of the DPA 1998.

This Data Protection Policy establishes the standards required to protect personal data and mitigate any detrimental impact on individuals resulting from poor data controls.

Terminology

The Parochial Church Council of All Saints' Nettleham is referred to in this document {*inter alia*} as "Nettleham PCC" or "the PCC".

The Data Protection Act 1998 is referred to in this document as "the DPA 1998"

The eight principles of the DPA 1998 are referred to in this document as "the DPA Principles"

The Information Commissioner's Office is referred to in this document as "the ICO"

The PCC Data Protection Advisor is referred to in this document as "the PCC DP Advisor"

A Data Subject Access Request is referred to in this document as a "DSAR"

Document Governance

The PCC is responsible for creating and maintaining this document. Any amendments or enhancements to this document must be approved by PCC, and the document must be reviewed at least annually. These changes and reviews should be documented in the table below.

Date of Change	Version No.	Reason for Change	Sections Impacted	Submitted on	Reviewed by Approved on
29/12/2016	Draft	Initial creation	All	Jan 2017	Nettleham PCC
23/05/2017	V0.2	PCC Feedback	All	June 2017	SC
21/07/2017	V0.3	Restructure	All	July 2017	SC
30/07/2017	V0.4	Consistency	All	Aug 2017	PCC Approved
03/09/2017	V1.01	Consistency	All (tracked)	Sep 2017	

Policy Responsibilities

Policy Sponsor	Incumbent
Policy Owner	Nettleham PCC
Policy Author	The PCC DP Advisor
Key Stakeholders	Nettleham PCC, Clergy, Parish Officers, Lincoln Diocese
Review Frequency	Annual; ad-hoc as legislation changes (Nettleham PCC)
Last Review date	03-Aug-2017
Storage Location	Nettleham PCC Minutes, Benefice Rectory; Benefice DP Advisor's home; http://www.allsaintsnettleham.co.uk/dataprotection/

Table of Contents

1. Introduction

The DPA 1998 reinforces common-sense rules of good information handling. It is there to ensure that organisations manage the personal information they hold in a fair, lawful and secure manner. Nettleham All Saints' PCC is a legally defined entity under Parochial Church Councils (Powers) Measure 1956 (as amended) and Synodical Government Measure 1969 (No. 2) Act, and therefore must explicitly comply with the legislation.

All UK organisations that use '**personal data'**[1] for their own purposes must comply with the DPA. Certain types of personal data have special protection under the DPA; this is known as '**sensitive personal data'**[2] and its use is highly restricted.

The Information Commissioner's Office [ICO] is the UK's independent authority set up to protect personal data. The ICO has enforcement powers and can check whether Nettleham PCC and its officers and representatives are using personal data appropriately. More details about the ICO and its powers can be found at its website at: https://ico.org.uk/

The purpose of this Policy is to help you understand your responsibilities under the DPA and how to comply with its provisions. All representatives must read this Policy and complete a form indicating that they have understood it. New volunteers and officers should complete this process within 1 month of engagement.

[1] **Personal Data** - information about living individuals that allows identification. It includes but is not restricted to name and address information in electronic format and on paper, and information that may affect an individual's privacy e.g. CCTV footage.

[2] **Sensitive personal data** - is personal data consisting of information relating to a data subject's race or ethnic origin; political opinions; religious or similar beliefs; trade union membership; physical or mental health or sexual life; or actual or alleged commission of any offence, proceedings for such offence or disposal of or sentence in such proceedings.

2 Scope

This policy applies to:

1. Personal data held centrally by the Parish of All Saints Nettleham {'the Parish'}
2. Personal data from the central store passed to partners in other Church organisations
3. Data from 3rd parties appended to Parish central data store, known as: '3rd party data'

As a representative of the Parish and the Church of England, there is a personal responsibility in accessing and using the data, to read and to comply with this Policy by:

1. Officers of the Parish (clergy, laity, PCC, administrators)
2. Anyone holding data for, or receiving data from, the Parish (eg Electoral Roll officer)
3. Anyone acting as a representative of the Parish in any voluntary or paid capacity
4. Any representative of 3rd parties receiving personal data from the Parish or its officers

3 Individual & Collective Responsibility

Compliance with this Policy is required as part of your activity on behalf of the Parish. A breach of the DPA 1998 can lead to individual responsibility for those involved and personal exposure to criminal proceedings including a fine and potential prison sentences for the most serious breaches.

Personal information shared by Individuals with other individuals as part of a friendship or relationship, even if noted in a personal diary, is excluded from this scope (as always, the intent should be to consider the data subject's wishes, expressed or implied).

How does the Data Protection Act apply to Nettleham PCC?

The Parish '**processes**'[3] personal data: like all organisations, we use personal data internally to operate. For example, we store and process information about our Officers, Congregation, Volunteers, Clergy, Suppliers, Partners, & Volunteers such as their names, addresses, dates of birth, job titles, roles, emails, etc.,.

Nettleham PCC is a '**data controller**'[4] as defined in the DPA 1998. This means that PCC is directly responsible to the ICO and the **Data Subjects**[5] for the way in which we process the data. Data Subjects are the individuals who may be identified by the personal data held.

The DPA 1998 obliges all data controllers to register with and to notify the ICO of the fact that they process personal data, giving a brief description of how they process such data, with the exception of entities meeting specific criteria (see Appendix). Nettleham PCC is exempt from mandatory registration.

What if you think a mistake has been made?

If a member of Nettleham PCC, an employee, officer, representative or volunteer, thinks that a mistake has been made by themselves or anyone else which could lead to a breach of the DPA 1998, this must be reported immediately or as soon as is practical to the PCC DP Advisor who will record certain details and may contact Diocesan officers for guidance.

Unfortunately, breaches and mistakes do sometimes happen and when they do Nettleham PCC must ensure that it deals with these situations quickly and professionally so as to limit any damage to the individuals concerned and to Nettleham PCC itself.

---

[3] **Process –** any use of personal information including collection, creation, reading, amending, copying, storage, disclosure, transfer, archiving deletion and/or destruction.

[4] **Data Controller -** A person who determines the purposes for which, and the manner in which, personal information is to be processed. This may be an individual or an organization and the processing may be carried out jointly or in common with other persons.

[5] **Data Subjects** are the individuals who may be identified by the personal data held.

4 The DPA 1998 Principles

Whilst all organisations depend upon the flow of, and use of, information including personal data, the DPA 1998 requires such use to be carried out in a fair, lawful and secure manner. The DPA 1998 therefore allows organisations like Nettleham PCC to use personal data, provided this use is carried out in line with DPA 1998 requirements.

Any organisation which processes personal data must comply with the eight DPA 1998 principles, which state that personal data must:

i) be fairly and lawfully processed
ii) be processed for legitimate & lawful purposes
iii) be adequate, relevant and not excessive
iv) be accurate and up to date
v) not be kept for longer than is necessary
vi) be processed in line with the data subject's rights & expectations
vii) be secure
viii) not be transferred to other countries without adequate protection

The DPA 1998 also provides individuals with certain rights that help to regulate how their information is processed by organisations. This includes the right to find out what personal data an organisation holds about them.

5 Corporate Responsibility

Nettleham PCC, its employees, officers, representatives and volunteers have a responsibility to carry out their duties in accordance with this Policy to ensure that we comply with the DPA 1998. Both Nettleham PCC and the individuals concerned can be held liable for data protection breaches.

It is however important for you to understand who has overall corporate responsibility for data protection within Nettleham PCC and who you should contact if you have any questions or issues in relation to data protection or this Policy.

(i) Policy Sponsor

The Parish Incumbent is the sponsor of this Policy. During an interregnum or pastoral reorganisation, the Rural Dean will substitute as sponsor. Day-to-day decisions required of the sponsor may be assumed by a churchwarden (usually with knowledge of the Archdeacon), in the absence of the Rural Dean and particularly in a time-sensitive issue.

(ii) Policy Owner

Nettleham PCC is the Policy owner. Any queries relating to any aspects of data protection or this Policy should therefore be sent to Nettleham PCC Secretary and the PCC DP Advisor.

(iii) Key Stakeholders

Key Stakeholders (ie Nettleham PCC, Clergy, Parish Officers, Lincoln Diocese) will sponsor and support initiatives to facilitate the implementation of this Policy. In particular, they will:

- Ensure that new data elements (ie new fields) to the central database are approved by the PCC DP Advisor and ratified by PCC.
- Promote data protection knowledge and awareness as an ongoing priority for all users of the data.
- Support action to enable data protection obligations to be specified, proven and then observed.
- Inform the Benefice Data Protection Advisor of any new data sources, to enable appropriate action.

6 Appendix A Criteria for Registering with ICO as Data Controller

Criteria for registering are found on the Government web-site
https://ico.org.uk/for-organisations/register/self-assessment/

1. Are you a not-for-profit organisation that qualifies for an exemption?

Answer 'Yes' if your organisation was established for not-for-profit making purposes and does not make a profit. You can answer 'yes' if your organisation makes a profit for its own purposes, as long as the profit is not used to enrich others. You must:

- only process information necessary to establish or maintain membership or support; and
- only process information necessary to provide or administer activities for people who are members of the organisation or have regular contact with it; and
- only share the information with people and organisations necessary to carry out the organisation's activities. Important - if individuals give you permission to share their information, this is OK (you can still answer 'yes'); and
- only keep the information while the individual is a member or supporter or as long as necessary for member/supporter administration.

You must answer 'No' if you use CCTV for crime prevention.

◉ Yes

1. Do you use CCTV for the purposes of crime prevention? **No**	Change this answer
2. Are you processing personal information? **Yes**	Change this answer
3. Do you process the information electronically? **Yes**	Change this answer
4. Is your organisation responsible for deciding how the information is processed? **Yes**	Change this answer
5. Do you only process information for one of the following purposes? **No**	Change this answer
6. Are you a not-for-profit organisation that qualifies for an exemption? **Yes**	Change this answer

You are under no requirement to register

Some not-for-profit organisations are exempt and based on the information you have provided you do not have to register with the ICO.

However, it is important that your organisation adheres to the principles of the Data Protection Act (DPA) and understands best practice for managing information. To help ensure you are complying with the DPA, we have produced a range of training materials including practical toolkits, training videos and more.

You can still register voluntarily if you wish.

7 Appendix B Checklist of Obligations

Principle 1	**Personal data must be fairly & lawfully processed**	
Nettleham PCC's Obligations	**How does Nettleham PCC comply?**	**How does this affect you?**
To ensure that the data subject has given his or her consent for their data to be held and processed by Nettleham PCC. To ensure that the purposes for which the data is intended is made clear to the data subject before the consent is provided. Not to release information to a 3rd party unless appropriate consent from the data subject is obtained, and certain undertakings given by the 3rd party (e.g. the entity has a Data Protection Policy). To have procedures in place to cover requests for personal information (exempt from consent above) made under Sections 28, 29 & 35 of the DPA 1998 and include purposes such as, the prevention and detection of crime. To ensure that personal data is processed in line with all other relevant UK legislation.	When taking on a new employee, Nettleham PCC's contract of employment will contain details of what their personal data will be used for. This will include various purposes such as legal, personnel management, training and development, administration and other management purposes. Volunteers will be given a role description which will include reference to personal information and the uses to which it will be put. For example, • Using personal data as part of an email campaign would require this use to be listed in the consent form / contract / role description. • Using information supplied when applying to join the electoral roll of the Parish, similar information will be requested, as well as skills and career history, to serve as input to PCC planning.	You should never process personal data (including reading, amending or deleting such data), unless the use is permitted by virtue of prior consent, and you have a legitimate business reason for doing so, or the data subject's consent has been explicitly obtained. Personal data should only be released to a 3rd party with the data subject's consent (unless the request for information is made under the DPA 1998 Sections 28, 29 & 35 exemptions as outlined above).

Principle 2	Personal data must be processed for limited purposes	
Nettleham PCC's Obligations	**How does Nettleham PCC comply?**	**How does this affect you?**
To ensure that personal data is only processed for the purposes for which it was originally collected.	The PCC DP Advisor is responsible for checking that the proposed use of any personal data complies with the original purpose for which the data was collected. The Compliance Sign-off form can be obtained from http://www.allsaintsnettleham.co.uk/dataprotection/	If an individual has been notified that his or her data will only be used for emailing newsletters, then use for electronic marketing purposes cannot be permitted unless consent is subsequently obtained for that additional purpose
Principle 3	**Adequate, Relevant and not Excessive**	
Nettleham PCC's Obligations	**How does Nettleham PCC comply?**	**How does this affect you?**
To ensure that when processing personal data, such data is adequate and relevant for the purposes for which it is being processed.	Nettleham PCC places controls within the organisation (such as the Sign-off procedure).	For example, it would not be excessive to collect and share an individual's medical history to ensure that their attendance at events including services can be safeguarded by first-aiders. It would be excessive to then use this information in a mailing list for healing services
Principle 4	**Accurate and Up to Date**	
Nettleham PCC's Obligations	**How does Nettleham PCC comply?**	**How does this affect you?**
To take reasonable steps to ensure that all personal data held is accurate and up to date.	The PCC DP Advisor will carry out regular reviews of the data held centrally and ensure the data is amended or deleted where required. Where possible, data will be validated before being loaded on to the central database to ensure that any data conflict or association is processed correctly. Nettleham PCC undertakes to insert or update information within a specific period of time as specified in the Policy published on its web-site. Nettleham PCC has specific processes in place to amend or delete data upon request from a data subject.	If your role involves data input (for example if you are responsible for loading details onto the central database / system) then you must ensure that you input data accurately. If your role involves carrying out updates to Nettleham PCC database you must ensure this is carried out in line with the relevant internal processes including any quality checks, such as contacting the provider of the data in regard to any data inconsistencies to ensure that records are updated accordingly

Principle 5	**Not be kept for longer than is Necessary**	
Nettleham PCC's Obligations	**How does Nettleham PCC comply?**	**How does this affect you?**
To ensure that personal data is only processed for the purposes for which it was originally collected.	Maintains a Data Retention Policy, a copy of which can be obtained from the web-site. The Data Retention Policy lists the different types of personal data we hold and for how long we should hold each data type.	You must read and understand PCC's Data Retention Policy; You should carry out regular reviews of records in your own work area to ensure that you are not holding personal information that is no longer required; for example, when helpers at Family Church change, the leader of that team must remove old records and add new ones. If this requires liaison between the leader and the administrator, then this is the responsibility of the team leader.
Principle 6	**Processed in Line with the Data Subject's Rights**	
Nettleham PCC's Obligations	**How does Nettleham PCC comply?**	**How does this affect you?**
To ensure that Data Subjects' rights in relation to the processing of, and access to, their personal data. Are properly maintained These include: • the right to request a copy of all the information held about them – a 'DSAR'; • the right to request inaccurate data to be updated, suppressed or deleted; • the right to ensure their details are excluded from any marketing activity.	Nettleham PCC Secretary will treat all data subject requests as urgent, and forward to Nettleham PCC DP Advisor on receipt. The procedures followed by this person ensure that such requests are processed within the relevant statutory time limits and that the individual's identity is verified before any personal data is released.	If you receive a request from a Data Subject requiring a copy of their personal information or requesting any personal data held by Nettleham PCC to be updated or deleted, then the subject is should be invited to submit a formal request to PCC Secretary, which will be processed as above.

Principle 7	**Secure**	
Nettleham PCC's Obligations	**How does Nettleham PCC comply?**	**How does this affect you?**
To have adequate measures in place to ensure that data is kept secure and protected against loss, damage or theft. This includes technical measures (such as firewalls, passwords, and data encryption) and physical security (such as locks, restricted access to sensitive areas, and processes for the secure disposal of confidential waste).	Nettleham PCC has implemented the technical and physical security measures mentioned above. Any access by a PCC member, an employee, officer, representative, or volunteer that is considered to be improper or inappropriate may result in action including reference to police authority.	You must be vigilant with regard to information security and ensure that you report any breaches to the Parish Data Protection Advisor in a timely manner. Prior to releasing any personal information, you must ensure that you have verified the individual or organisation's identity. If you are unsure as to the level of authority you have, or need guidance on what may constitute improper or inappropriate access, you should discuss this with the Parish Data Protection Advisor **before** you access and process any data.
Principle 8	**Not Transferred to Other Countries without Adequate Protection**	
Nettleham PCC's Obligations	**How does Nettleham PCC comply?**	**How does this affect you?**
To ensure that personal data is not transferred to any country outside the European Economic Area (EEA) unless adequate levels of data protection are in place in the target country.	Nettleham PCC, ,its employees, officers, representatives, and volunteers are not expected to be familiar with all data protection regimes around the world. They are however required to apply one of a possible range of measures (eg an explicit signed non-Disclosure Agreement) that allows us to satisfy the adequate safeguard requirement.	If you are requested to transfer or become aware of a transfer of personal data outside of the EEA, you must ensure that there are adequate levels of security and data protection in place within the organisation to which the data is to be transferred. Approval must be obtained from the Benefice Data Protection Advisor before any movement of data outside the EEA. You should ensure that there is a full written contract in place between PCC and the relevant recipient of the data detailing the steps to be taken to ensure that we have adequate levels of security and data protection in place for the data. Such standards can be obtained by the Benefice Data Protection Advisor when necessary.