THE CHURCH OF ENGLAND

NATIONAL CHURCH INSTITUTIONS

Privacy Notice Policy

Policy summary

The National Church Institutions (NCIs) use personal information to carry out their many functions supporting the mission and ministry of the Church of England. Legislation requires and sometimes empowers the NCIs to provide goods and services to the wider Church.

The NCIs therefore collect a wide range of personal data required for or incidental to the discharge of its functions, involving employees, clergy, pensions, housing, public consultations, recruitment and appointment, parliamentary functions etc. The NCIs will endeavour to ensure that they use personal information in line with the expectations and interests of those with whom they come into contact, including their employees, office holders and customers, for the benefit of the Church and wider society and in compliance with data protection legislation.

This policy provides guidance on the provision of information to data subjects about how their personal data is processed, in order to meet the requirements for transparency in the data protection legislation. The NCIs are committed to being open and transparent about their collection, use, sharing, storage, archiving and disposal or personal data, and will provide all necessary and relevant information about these activities to data subjects.

Transparency will engender trust and will support effective business operations and minimise the risk of harm to individuals.

Adherence to this policy is mandatory for all NCI employees, contractors, agency workers, consultants and volunteers who use personal data held by the NCIs.

Contents

Introduction

1. The NCIs, as data controllers of personal data, are under an obligation of transparency concerning the processing of such data, under data protection legislation. Such transparency concerns specifically, the provision of information to data subjects about how their data is being processed, and facilitating individuals to access and understand this information. The NCIs are committed to engendering trust in the processes we undertake with regard to personal data, by enabling data subjects to understand, and if necessary, to challenge these processes, and to empower data subjects to hold us to account and to exercise their control over their personal data.

2. The NCIs will comply with applicable legislation, including:

    a. **General Data Protection Regulation 2016**
    b. **Data Protection Act 2018**
    c. **and other regulatory requirements and applicable guidance.**

Purpose

3. The primary purpose of this policy is to set out the relevant legislation and to describe the steps that the NCIs are taking to comply. It is our policy to ensure that our compliance with the relevant legislation is clear and demonstrable at all times.
4. In addition, this policy is intended to establish best practice in relation to the information provided to data subjects, how and when the information is communicated, and the key principles underpinning these actions and activities.

Scope

5. This policy applies to the NCIs as listed, and to any separate legal entities owned and controlled by them.

    The NCIs are:
    The Archbishops' Council
    The National Society for Promoting Religious Education
    Church of England Central Services
    The Church Commissioners for England
    The Archbishop of Canterbury in his corporate capacity
    The Archbishop of York in his corporate capacity
    The Church of England Pensions Board

6. This policy is applicable to and must be followed by all employees, including agency workers, consultants, contractors and volunteers. Failure to comply could result in disciplinary action, including dismissal for employees, and termination of contracts with contractors, consultants or agency staff.

Definitions

7. **Personal Data** - Any information that relates to an identifiable living individual.
8. **Data processing** – Any activity relating to the collection, recording, organising, structuring, use, amendment, storage, access, retrieval, transfer, analysis, disclosure, dissemination, combination, restriction, erasure or disposal of personal data.

9. **Data Subject** - The individual to whom the data being processed relates.
10. **Data Controller** - A body or organisation that makes decisions on how personal data is being processed.
11. **Joint Data Controller** – A data controller in another organisation who has joint decision-making powers over how or why data is processed.
12. **3rd Party Data Processors** - These are parties that process data on behalf of a Data Controller, they do not have the ability to make any decisions about how the data should be processed. They must always be designated through a Contract or a Data Processing Agreement.

Policy

Policy Statement

13. Data subjects have the right to be informed personal data relating to them is processed by the NCIs, and the commonest way to be transparent and to provide accessible information is in a Privacy Notice (PN). A PN (also called a privacy policy or fair processing notice), is a term used to describe all the privacy information made available to data subjects when data is collected from, or obtained about them to enable them to determine what the scope and consequences are of the data processing.

14. The NCIs will:

    1. Provide individuals with explicit and required privacy information before or at the start of the data processing i.e. at the time they collect or obtain the personal data, this will be in the form of a privacy notice;
    2. If the NCIs obtain personal data from other sources, they will provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month;
    3. Provide information that is concise, transparent, intelligible, easily accessible, and that uses clear and plain language;
    4. Provide information in a format that is appropriate for the data subjects e.g. children, vulnerable adults etc;
    5. Provide privacy information to people using a combination of different techniques and methods to ensure accessibility i.e. on-line, hard copy, verbally etc.;
    6. Notify data subjects if there is a change to the data processing and PN;
    7. Take all reasonable steps to communicate with data subjects to ensure they are informed, unless exempt from doing so by legislation;
    8. Regularly review and update privacy information.
    9. Take active steps to furnish the information, ensuring that data subjects are not themselves obliged to search for PNs, to ensure that information is provided at different times and at appropriate points during their interaction with data subjects.

Privacy Notice Information

10. As a default, all PNs issued in writing or by electronic means by the NCIs will contain the following information:
    - The name and contact details of the NCI (data controller);

- The name and contact details of the NCI's representative (only applicable if the data controller is not based in the EU but processes the personal data of EU residents);
- Contact details for the department/team issuing the PN;
- Contact details for the NCI's data protection officer;
- Purpose of processing for which the personal data are being collected;
- Lawful basis for the processing;
- A legitimate interest assessment (if applicable);
- The recipients or categories of recipients of the personal data, if any;
- The details of transfers of personal data to any third country and the necessary safeguards (if applicable);
- The retention periods or retention policy for the personal data;
- The rights of the data subject in respect of the processing and how these may be exercised;
- The right to object to direct marketing (if applicable)
- The right to withdraw consent and how consent may be withdrawn (if applicable);
- The sources of the personal data (if the personal data is not obtained from the individual it relates to);
- The details of the existence of automated decision-making, including profiling (if applicable);
- Contact details for the Information Commissioners' Office.

Further information on elements listed above and PN templates are available in the Data Protection Guidance (see on Gateway).

11. Additional information should be provided in the PN if applicable to the circumstances:
    - For complex, technical or unexpected data processing, the PN must explain the most important consequences of the processing i.e. what the effect will be processing have on data subjects;
    - Where automatic processing or profiling is being used, the PN will explain the logic involved, and any significant consequences for the data subject;
    - Where a Data Protection Impact Assessment has been undertaken, departments/teams should consider may consider publishing part of the DPIA.

Joint Controllers

12. Where data is being shared between data controllers, it is responsibility of each controller to provide a suitable PN stating that the data is being shared, as stated in the Information Sharing Framework (see on Gateway).
13. The NCIs will specify who the joint data controllers are in their PNs, where this is applicable, so that data subjects know to which data controller to apply to exercise their individual rights.

Data Processors

14. Where data is being shared with 3rd Party Data Processors, the NCIs will specify in their PNs who such processors are, where applicable.

Vulnerable individuals

15. When collecting data from vulnerable individuals, e.g. children, adults with disabilities, the NCIs will provide privacy notices appropriate to the level of understanding of these individuals.

On-line platforms and software

16. Where the NCIs use specific on-line platforms or software with which the data subject is obliged to interact (e.g. Moodle, Survey Monkey, Doodle etc), the NCIs will not provide detailed information but will sign-post users to that processor's privacy statement.

Methods and formats

17. The NCIs will ensure that privacy notices are provided to data subjects in various formats and by various methods, as suits the data collection activity, for example:
    - Put PNs on their websites;
    - Include PNs with forms used to collect personal data;
    - Provide links to web-based privacy notices in e.g. emails, FAQs, webpages
    - Provide hard copy documents where data is collected face-to-face.

18. Departments will consider whether it is necessary to provide PNs in other languages, or for example, in Braille, or through video, depending on their intended audience.

19. Web pages
    - A privacy notice published on a website must:
        - Be easily accessible, i.e. appropriate colours, font, position, such that data subjects who may be colour-blind or otherwise impaired will still find it easily;
        - Be immediately apparent i.e. should not require searching by the data subject
        - Be clearly visible under a commonly used term such as "Privacy", "Privacy Policy" or "Data Protection";
        - Where data collection takes place on-line, a link to the PN must be provided on the same page on which the data is collected;

20. Layered PNs
    A layered PN provided electronically will be used as follows:
    - They will not be nested pages requiring several clicks to get to
    - The first page / layer will be immediately visible
    - The first page/layer will provide a clear overview of the information available with one click links to further information
    - The first page/layer will contain information that tells the data subject what the processing activity is

21. Oral or verbal PNs
    - PN information may be provided orally on a person-to-person basis, i.e. face to face or by telephone, or in automated form or pre-recorded messages. This may be on request by the data subject, or as a standard method of providing privacy information.

- If the data subject is making a subject access request orally, and is requesting the PN be provided orally, the NCIs will, where necessary, require the request to be in writing and that suitable identification checks are carried out before providing the PN in a oral format.
- The NCIs will keep a record of, and will be able to demonstrate:
  - That a request was made for the information by oral means;
  - The method by which the data subject's identify was confirmed (if applicable);
  - When and how the information was provided to the data subject.

22. Apps
    - The necessary information should be made available from an online store prior to download, and once the app is installed, the PN should never be more than "two taps away" and should be easily found in the app's menu.

23. Signage
    Where the NCIs use CCTV or Wifi, we will provide public signage indicating that CCTV / Wifi is in use and that data subjects' personal data will be captured.

24. Icons
    The NCIs will only use icons or provide privacy information in the following circumstances, using standardised icons:

    - Where icons are used in combination with other methods and techniques, and
    - Where icons presented electronically are machine readable or
    - Appear on signage to indicate e.g. CCTV or wifi tracking.

Further processing

25. Where the NCIs intend to further process the personal data for a purpose that is not compatible with the original purpose for which the data was collected, they will update their privacy information and inform the data subject about the changes before starting any new processing.
26. Where such further processing is not based on consent or legal obligation, the PN will contain additional details of how such processing is compatible with the original processing purpose. Further guidance on compatibility is available in the Data Protection guidance (see on Gateway).

Amending the PN

27. The right to be informed applies not just at the point of collection, but throughout the lifecycle of the processing activity, which may require PNs to be changed or amended over time.
28. The NCIs will regularly review and, where necessary update their privacy information. If the change is because of a fundamental change to the processing activity e.g. using automatic profiling, transferring to a 3rd country; or will have a significant impact on data subjects in any other way, the PN must be provided to data subject prior to the processing change taking effect, using explicit and effective methods to ensure data subjects are informed and able to exercise their rights.

29. The NCIs will take all measures necessary to ensure that any changes to the PN are communicated in such a way that most recipients will see that a change has been made, e.g. by email, letter, etc.

Retention of PNs

30. The NCIs will ensure that all PNs are dated, version controlled, and retained for the full period of the processing activity and will be provide previous versions to data subjects where necessary.

PNs and Access Requests

31. When responding to a Subject Access Request (SAR), the NCIs will provide a relevant PN, containing minimally what is specified in paragraph 9, with the response to such requests.

32. Further guidance on responding to SARs is available in the Individual Rights Policy, and Individual Rights Procedure (see on Gateway).

Third Party right to be informed

33. The NCIs will provide a privacy notice when legitimate data processing request(s) are made by an appropriate third party acting on behalf of the data subject. These may include:
    - Parent or Legal Guardian
    - Legal representatives
    - Someone with legal power of attorney
    - Written and verified permission of the data subject

Consent

34. Where processing relies on consent, such consent must be informed in order to be valid. The NCIs by default will provide the data subject with the following information in any declarations of consent or consent forms:
    - The identity of the controller; and
    - The purposes of the processing for which the personal data are intended; and
    - The consequences to the data subject if they fail to provide the information.
35. Departments may provide full PNs with consent forms if this is suitable and appropriate.

Anonymised information

36. The NCIs will include in the relevant privacy notice an intention to anonymise information following data collection, and that such data will need to be processed in order to do this.
37. Where data is collected anonymously, i.e. there is no collection of identifiable personal data, a Privacy Notice is not required, however, there must be possibility that any of the data collected can be used by the NCIs to identify individuals. If this is possible, then additional safeguards must be put in place and a Privacy Notice issued.

Exemptions

38. The NCIs will not provide any privacy information when collecting or obtaining personal data on the data subject if:
    - The data subject already has the information; or
    - Providing the information to the data subject would prove impossible; or
    - Providing the information to the data subject would involve a disproportionate effort; or
    - Providing the information would impair the accomplishment of the purposes of the processing; or
    - The NCIs are required by law to obtain or disclose the personal data; or
    - The NCIs have a duty of professional secrecy regulated by law that covers the personal data; or
    - Where UK legislation restricts the scope of data subjects' rights in relation to transparency.

39. Where exemptions apply, the NCIs will inform data subjects of such, and indicate where applicable the relevant legislative restrictions, unless doing so would be prejudicial to the purpose of the restriction e.g. the prevention, investigation and prosecution of criminal offences.

40. Departments should consult the Data Protection Guidance or contact the Information Governance Officer if there is any doubt about whether or not to provide a PN.

Fees and charges

41. The NCIs will provide privacy notices free of charge.

Timescales

42. The NCIs will:
    - Provide privacy notices before or at the time of obtaining the personal data from data subjects; and
    - Provide privacy notices to the data subject within 30 working days of receipt of personal information from a source other than the data subject.

43. Where the data obtained from a 3rd party is used specifically for the purposes of communicating with the data subject, the PN will be provided at the time of that communication, OR within one month of receipt of the data, whichever is the shorter.
44. Where personal data is being disclosed to another recipient not previously noted on the PN e.g. another data controller, a 3rd party processor etc., the data subject will be notified at the time of the disclosure, at the latest within one month of such disclosure, unless exemptions apply that prevent such notification.
45. Where processing is likely to continue over a significant period, the NCIs will remind data subjects of the PN at appropriate intervals.

Review and complaints

46. All responses issued by the NCIs will contain the details of how a requestor may request a review or make a complaint about how their personal data is being processes.
47. If a data subject is not satisfied with how the processing of their data is being conducted, or how it has been communicated, they are entitled to contact the Information Commissioner's Office (ICO) directly.

Responsibilities

1. **Chief Officers** are responsible for the approval and implementation of this policy and related policies, for informing the trustees, where applicable, of the relevant NCI of current legislative requirements that may affect their criminal and civil liability; for ensuring that Directors at the NCIs fulfil their responsibilities; for undertaking their own responsibilities as Information Asset Owners and Heads of Departments, and for supporting the DPO to undertake necessary tasks and duties.

2. **Data Protection Officer** is responsible for reviewing Privacy Notices in the event of a complaint from a data subject.

3. **Heads of Department** are responsible for ensuring that privacy information and privacy notices are developed and provided to data subjects.

4. **Information Governance Officer** is responsible for monitoring privacy notices to ensure that teams are providing them and that they are appropriate; for supporting teams and department to create Privacy Notices; for providing guidance and templates.

5. **Records Management team** is responsible for supporting the NCI departments' compliance with the policy by advising on best practice, providing guidance.

6. **All staff** (including volunteers and contractors) are responsible for ensuring that they have issued appropriate privacy notices, and that they can provide these to data subjects on request; that they assist colleagues who are responsible for individual rights requests by providing the necessary privacy notices in a timely way.

Approval and review

Approved by	Chief Officers, JSC, JESCB
Policy owner	Information Governance Officer
Policy author	Madi McAllister, Information Governance Officer
Date created	21 August 2018
Approved date	2 October 2018 JESCB
Review date	July 2019

Revision History

Version No	Revision Date	Previous revision date	Summary of Changes
0.1	3/7/18		First draft of new policy
1.0	21/8/18	3/7/18	Final version of new policy

Related policies and procedures

The Privacy Notice Policy works in conjunction with and is supported by a number of other policies and documents including those shown in the diagram below:

APPENDIX 1 – PN Information Table

Required information	Data collected from data subject	Data collected from 3rd party	Requirements
Identity and contact details of the controller	Article 13.1 (a)	Article 14.1(a)	Easy identification of the controller and all forms of contact information (phone number, email, postal address etc)
Contact details for the data protection officer	Article 13.1(b)	Article 14.1(b)	Data Protection Officer, Church House, Great Smith Street, London, SW1P 3AZ or gdpr@churchofengland.org
The purposes and legal basis for the processing	Article 13.1(c)	Article 14.2(b)	The purpose of the processing for which the data is intended, and the relevant basis relied upon under Article 6 or Article 9 or 10 must be specified.
Where legitimate interests (Article 6.1(f) is the legal basis, state what these legitimate interests are (controller or a third party).	Article 13.1(d)	Article 14.2(b)	The specific interest in question must be identified for the benefit of the data subject. A copy of the Legitimate Interest Assessment (LIA) should be provided.
Categories of personal data concerned	Not required	Article 14.1(d)	This is necessary of data has been collected from a 3rd party because the data subject may be unaware that this data has been obtained.
Recipients (or categories of recipients)	Article 13.1(e)	Article 14.1(e)	This must include all recipients – data controllers, joint data controllers, data processors, 3rd parties.
Details of transfers to 3rd countries	Article 13.1(f)	Article 14.1(f)	Include all 3rd countries involved; relevant safeguards, including the existing or absence of an adequacy agreement, and the means for the data subject to obtain a copy of the safeguards. State the relevant GDPR Article permitting the transfer and the mechanism.
Storage period or criteria used to determine that period	Article 13.2(a)	Article 14.2(a)	Must be stated in a way that the data subject can assess, on the basis of his or her situation, what the retention period will be for that data/purposes. Stipulate different retention periods for different categories of data and/or processing activities.

The rights of the data subject	Article 13.2(b)	Article 14.2(c)	Include a summary of what the right involves and how the data subject can exercise these rights.
Where processing is based on consent (or explicit consent) state the right to withdraw consent	Article 13.2(c)	Article 14(2(d)	Include how consent can be withdrawn.
The right to lodge a complaint with a supervisory authority	Article 13.2(d)	Article 14.2(e)	Explain the right to complain to the Information Commissioner's Office:
Where there is a statutory or contractual requirement or an obligation to provide the data, state the obligation and the possible consequences for failure to provide the data	Article 13.2(e)	Not required	Online forms must clearly indicate "required" fields, and the consequences for not filling in these fields
Source of the data, and if applicable, if it came from a publicly accessible source	Not required	Article 14.2(f)	Nature of the sources i.e. publicly/privately held; the type of organisation/industry/sector; and where the information was held (EEA or non-EEA). Provide the specific source if possible.
The existence of automated decision-making including profiling, if applicable	Article 3.2(f)	Article 14.2(g)	Provide meaningful information about the logic used and significance and consequences for the data subject