PERSONAL FILES RELATING TO CLERGY

Policy
for
Bishops and their staff

Approved by the House of Bishops May 2018

Personal Files relating to Clergy

Policy for bishops and their staff

Approved by the House of Bishops May 2018

Foreword

Guidance on clergy personal files has been issued since at least 1987 and has been updated periodically. The latest edition addresses changes necessary to ensure compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. For convenience the acronym GDPR will be used throughout this guide when referring to data protection legislation in the UK.

Although this is a policy document rather than legislation, it is important that there is consistency of approach in relation to how we process personal information in relation to clergy. Indeed, we regard this policy as best practice and as such, we strongly encourage you to comply with its terms.

You should also note that section 5 of the Safeguarding and Clergy Discipline Measure 2016 means that certain relevant individuals (including all clergy) have to pay "due regard" to all guidance in relation to safeguarding issued by the House of Bishops. Therefore, this will apply to any safeguarding guidance in this document.

On behalf of the House we commend this important document to all bishops and their colleagues who hold personal information about the clergy.

+Justin Cantuar **+Sentamu Ebor**

May 2018

Approval and review

Approved by	House of Bishops (via delegation committee)
Policy owner	House of Bishops
Policy author	Declan Kelly, Stephen York
Date	May 2018
Review date	May 2019

Revision History

Version No	Revision Date	Previous revision date	Summary of Changes
March 2013	March 2013	2011	Now with House of Bishops approval.
Nov 2017	Nov 2017	March 2013	Update retention schedules to meet updated safeguarding requirements.
May 2018	May 2018	Nov 2017	Update to ensure GDPR compliance and change sharing basis from consent to legitimate interest.
	August 2019	May 2018	Paragraph references in appendices corrected

What does this guidance cover?

1. This guidance is designed to assist bishops in managing personal information about the clergy for whom they are responsible, and to promote good and consistent practice in record keeping. It considers the requirements of data protection legislation and the law of confidentiality, and also addresses practical issues of file management. It supersedes the March 2013 edition and November 2017 update of this guidance .

2. The guidance deals only with personal files about clergy ("clergy personal files", also commonly known as "blue files"). It does not cover personal files relating to readers and other licensed lay ministers, although the same general principles apply to these. Nor does it cover files relating to those who are exploring a vocation to ministry or who are in training but not yet ordained. Ministry Division issues guidance to Diocesan Directors of Ordination about record keeping in this context.

3. The personal files of the Archbishops are held by the provincial registrars of Canterbury and York respectively, and the personal files of diocesan bishops are managed by the archbishop of the relevant province and his staff. The personal files for cathedral deans are held by the diocesan bishop. An exception to this are the deans of peculiars. In such cases, the personal files are held with the relevant provincial registrar. This guidance does not extend to these files, although again the same general principles apply.

Overview of relevant legal requirements

Data Protection

4. On 25 May 2018, the General Data Protection Regulation (the "GDPR") will replace the Data Protection Act 1998 ("DPA")[1]. The good news is that the GDPR's main concepts and principles are very similar to those contained in the DPA. The Information Commissioners Office (ICO) will remain as the organisation in charge of data protection and privacy issues. If an organisation is complying with the DPA much of what it does will still apply. There are, however, some changes and additions, which will be highlighted here.

5. The GDPR applies to the processing of any information which relates to a living individual who can be identified from that information alone or when taken together with other information held by the same person or body. Such information continues to be termed 'personal data' in the GDPR. Processing is widely defined and includes obtaining information, holding it (whether in paper or electronic form) and sharing it with others.

[1] The Data Protection Act 2018 received Royal Assent on 23 May 2018. The 2018 Act supplements and implements the key provisions of the GDPR; outlines where UK law will deviate from certain GDPR provisions and updates and strengthens UK law to make the shift to GDPR (and the UK's withdrawal from the EU) as smooth as possible.

6. The GDPR sets out 6 fundamental principles which must be observed when processing personal data. These can be summarised as follows:

(a) processed lawfully, fairly and in a transparent manner;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means that individuals should be told what you are going to do with their personal data before you use it and consent to such use where appropriate;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are used;

(d) accurate and, where necessary, kept up to date. Personal data that is found to be inaccurate should be deleted or corrected without delay. All personal data should be periodically checked to make sure that it remains up to date and relevant;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. For instance, records of pastoral care discussions should not be kept for a number of years without justification. Records could be kept, for instance, if all identification features were removed, referred to as "anonymisation"; and

(f) kept securely. Personal data storage should be safe and secure – in lockable filing cabinets or in password protected computer files. Names and addresses of individuals should not be left unattended.

7. In addition, one of the main changes to note in the GDPR is that it places a much greater emphasis on transparency, openness and the documents that need to be retained in order to show that an organisation is complying with the legislation. This is known as "accountability".

8. Accountability means that an organisation must be able to show that it is complying with the principles. This means that you cannot merely state that you are complying with the legislation; you also have to prove it and provide evidence. To do this there are a number of actions you will need to take, such as documenting decisions you take about processing activities or various other ways of illustrating compliance, such as attending training, reviewing and updating policies and auditing processing activities.

9. Like its predecessor, the GDPR also provides that certain information is to be treated as 'sensitive' (this is known as 'special categories of personal data" in the GDPR)in relation to which particular conditions apply. This includes information about a person's religious beliefs, racial or ethnic origin, political opinions, sexual life, physical or mental health or union membership.

Criminal records (including any allegation that a criminal offence has been committed) are not classed as "special category" but stand as a class of their own but similar conditions will apply and such records should be treated as "sensitive".

10. The Information Commissioner's website (www.ico.gov.uk) is a useful resource which provides general and specialist guidance on many aspects of the GDPR.

11. Under the GDPR, the data controller - defined as a person or body who (either alone or jointly or in common with others) determines the purpose for which, and the manner in which, any personal data is processed - is no longer required to notify the ICO if he or she processes personal data electronically. Nevertheless, data controllers will have to pay an annual "data protection fee" unless the processing falls within certain exempt categories. Failure to pay will result in a fine. The fee is used to fund the work of the ICO[2].

12. It is important to note that within the context of the Church of England the diocesan bishop will be a data controller in his/her own right. Dioceses will also need to consider whether suffragan bishops will be separate data controllers or whether they will merely process personal data for and behalf of the diocesan.

13. The administration of pastoral care by a minister of religion is not exempt from the "data protection fee" and therefore the processing of clergy personal files will mean that the relevant fee will need to be paid. The diocesan bishop, as the data controller for these files, will be responsible for paying this fee. Guidance on the annual fee can be found on the Information Commissioner's website, although for charitable organisations this is fixed at £40 (or £35 if the charity pays by direct debit)[3].

Consent

14. Under the DPA many organisations relied on consent in order to process personal data. The GDPR both sets a much higher standard in relation to the obtaining and managing of consent in relation to individuals and provides for many other legal bases for processing personal data. As a result, consent may no longer be the most appropriate legal basis for processing personal data. You should be aware that consent is only one of the lawful bases for processing personal data and there are a number of alternatives, (e.g. legal obligation and/or legitimate interest).

15. Under the GDPR consent will only be the most appropriate basis if you can offer people real choice and control over how you use their data. If you cannot offer a genuine choice, consent is not appropriate. The processing of personal data of people working in and for organisations will typically be based not on consent but legitimate interest or performance of a contract.

[2] https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf
[3] Data Protection (Charges and Information) Regulations 2018 (SI 2018/480)

16. The processing of the personal data contained within clergy personal files is based on the legitimate interest and activities of the Bishop who needs to be able to develop, support, administer, regulate and manage clergy through their ministry; and not on consent which was previously relied upon for the transfer of files from the Bishop to another data controller. Therefore, whereas previously the consent of a cleric was sought to allow his/her file to be transferred between Bishops in different dioceses this is no longer the most appropriate basis for processing (i.e. transferring) this data, (see paragraph 22 for more details).

Confidentiality

17. A duty of confidence arises where information which is not already lawfully in the public domain is given on the understanding that it will not be shared with others. This understanding may be explicit, or it may be clear from the circumstances that there was a legitimate expectation on the part of the person giving the information that it would be held in confidence.

18. There is no breach of the duty of confidence where the person to whom the duty is owed has given consent to the disclosure. Where such consent has not, for whatever reason, been obtained, information may nonetheless be shared provided that this can be justified in the public interest. Where the information relates to the commission of a crime or where there is reasonable cause to believe that a child or adult may be at risk of serious harm if the information is not disclosed to the proper authorities, the public interest test is clearly satisfied.

19. In other cases, the key factors are necessity and proportionality. The person holding the confidential information must weigh up what might happen if the information is shared against what might happen if it is not, and make a decision based on a reasonable judgement as to whether the proposed sharing is likely to make an effective contribution to preventing or reducing a risk (e.g. of malpractice or incompetence) to which the public would otherwise be subjected.

The content of clergy personal files

General principles

20. The bishop needs to take account of the data protection principles described in paragraph 6 above when deciding what information should be held in any clergy personal file. The bishop should consider the following questions in relation to any category of personal data:

    - *Is there a proper and lawful reason why I need to have this information*? The first and second data protection principles in the GDPR (as in the DPA) state that personal data must only be obtained for a lawful and specified purpose, (see paragraphs 22-24 below).

- *Is the processing of this information on file a legitimate activity? If not, can I rely upon another legal basis for processing this personal data*? Because the information in clergy personal files is held in the context of their Christian ministry, much of the personal data in those files is likely to be regarded by the ICO as "special categories of personal data" (i.e. sensitive) for the purposes of the GDPR meaning that there will be additional requirements in order to process this data, (see paragraph 22 below).

Is there a proper and lawful reason why I need to have this information?

21. In making this assessment the bishop should have regard to his/her responsibilities under the Canons: these include his general responsibilities as chief pastor of the diocese (Canon C18) and the requirement that he should satisfy himself/herself as to certain specified matters before ordaining a person as deacon or priest and before instituting or licensing a cleric who has been ordained by another bishop or who has come from another diocese (Canons C5-7, C9-10, C12).

Is the processing of this information on file a legitimate activity under the GDPR? If not, is there another legal basis on which I can rely for processing this personal data?

22. As explained in paragraph 20 above, the personal data stored on a cleric's personal file is likely to be regarded as "special category" personal data (i.e. sensitive). Therefore, there will be additional requirements in order to process this personal data. Not only will you have to satisfy an Article 6 processing condition under the GDPR, you will also have to satisfy a processing condition contained in Article 9[4]. The processing of this personal data is considered to be necessary for the purposes of legitimate interest (Article 6(1)(f)) and is also a legitimate activity of a not-for-profit body because the processing relates solely to individuals who are "members" or "former members" of the Church of England "or have regular contact with it…" (Article 9(2)(d)). Consent will only be required if this personal data is disclosed outside the bodies that make up the institutional Church of England, (although for comments about the Episcopal Reference and the Clergy Current Status Letter ("CCSL"), see paragraph 80 below). This legal basis

[4] If the personal data relates to criminal conviction or offence data (this will include data about criminal allegations) then as well as satisfying an Article 6 processing condition, you will need to satisfy Article 10 of the GDPR rather than Article 9. This means that to process such data you will need legal authorisation. Such authorisation is contained within the Data Protection Act 2018 and compliance with the additional safeguards set out in this 2018 Act – See section 10(5) of the Data Protection Act 2018. Provisions are contained in the 2018 Act allowing processing "in the substantial public interest" without consent to protect members of the public from dishonesty, malpractice or other seriously improper conduct or for safeguarding purposes, (Schedule 1 Part 2, paragraph 11 and 18). Alternatively, Schedule 1 Part 3, paragraph 31 of the 2018 Act, allows the processing of criminal conviction etc. data by not-for-profit bodies where the processing relates solely to individuals who are "members" or "former members" of the Church of England "or have regular contact with it" and the data is not disclosed outside the institutional Church of England without consent. The ICO have stated that they will issue guidance about Article 10 processing in due course.

will be valid, provided that the cleric understands the basis for the processing and the purposes for which his/her personal data will be used and his/her various rights in relation to this data (as to which see the section on privacy notices later in this guidance).

23. Where information is supplied by a third party (i.e. a person outside the bishop's office and senior staff) without the consent (and/or knowledge) of the cleric, the bishop will need to consider whether the circumstances permit him/her to hold the personal data (i.e. what is the legal basis for processing that data? Is it a legitimate activity?).

24. The vast majority of processing by the bishop will be permitted on the basis that it is necessary for reasons of legitimate interest and because it is a legitimate activity and is carried out in order to regulate/administer "membership" or those who are in regular contact. Nevertheless, if the bishop has concerns he/she should seek the advice of his/her registrar about whether he or she is entitled to hold a particular piece of personal information in a clergy file and what is the appropriate legal basis for processing that data. It is essential to document any decisions taken about the processing of personal information, including a note of the grounds on which the decision was made, in case that decision is subsequently challenged.

Categories of information in personal files

Biographical details

25. In the past a composite 'Register of Ministers' form has been used in many dioceses both as a record for the clergy personal file and as a Curriculum Vitae to be shared with patrons seeking to fill a vacancy. The practice of using such as form as a CV for the purpose of appointment is no longer recommended. The bishop may, if he or she wishes, prepare and use a standard form or checklist within the diocese to collect, and periodically update, basic biographical details about his or her clergy for their personal files.

26. Where a cleric is being considered for an appointment then - whether or not there are other candidates for the post – he or she should be asked to complete the application form and process in use in his or her diocese [5] or the senior appointment equivalent form and process. This will help to ensure that the information used in the appointment process is accurate and up to date and that it complies with the requirements of equality law as they relate to clergy appointments.

27. It is recommended that a cleric's personal file should include the following biographical information so far as practicable.

    - Name, date of birth and contact details. Canon C.6 requires a person who is to be made deacon to produce to the ordaining bishop a certificate or other evidence of the date and place of

[5] https://jobs.churchofengland.org/clergycandidatesfaq

his or her birth, and a copy should be kept on file as confirmation that this requirement has been met.

- If the cleric is not a British citizen, evidence of immigration status and permission to work in the UK.
- Family/household. Particular care should be taken in relation to personal information about third parties such as family members. Any details kept should be relevant to the cleric's ministry (housing needs, pension etc) or to the bishop's pastoral responsibility for the cleric.
- Qualifications. Information (especially in relation to degree and post-graduate qualifications) should be supported by copy certificates where possible.
- Career before ordination. The file should contain a full CV since leaving school, with explanations for any gaps in education or employment, and any other information that is relevant to the skills and aptitudes of the cleric.

Ordination and ministry

28. In relation to selection and training, it should only be necessary to retain on the personal file material which demonstrates that the ordaining bishop satisfied himself, as required by the Canons, as to the person's suitability for admission to holy orders. This may include the candidate's registration form and references; the report of the Bishops' Advisory Panel and the reports sent to the bishop by the cleric's training institution in the penultimate and final years of training. If a faculty under Canon C4.5 has been granted, a copy should be kept on the file.

29. The following should also be kept on file:

- Copies of the cleric's letters of orders and (if relevant) permission under the Overseas and Other Clergy (Ordination and Ministry) Measure 1967.

- If the cleric has not served all his or her ministry in one diocese, a copy of all Episcopal References and CCSLs or 'safe to receive' letters (the predecessor to CCSL) obtained on a move between dioceses.

- In relation to the current appointment, copies of the application form and references (where applicable), copy licence or deed of institution and, where the post is subject to Common Tenure, a copy of the Statement of Particulars.

Ministerial development and training

30. Regulation 18(5) of the Ecclesiastical Offices (Terms of Service) Regulations 2009 requires the bishop to keep a written record of the outcome of any ministerial development review ('MDR') undertaken by an office-holder on

Common Tenure, together with any relevant matters relating to the review. The record must be signed by the office holder and the person conducting the review. All MDR's should be retained in the personal file. Where clergy who are not on Common Tenure participate in MDR, it is good practice to keep a similar record in relation to them.

31. Office holders on Common Tenure are under a duty to participate in arrangements made by the bishop for their continuing ministerial education ('CME'). Although this is not mandatory under the Terms of Service legislation, a record of CME undertaken will be helpful to the bishop in assessing whether a cleric has complied with this duty, and in assessing what CME is appropriate for his or her further development. If a separate training file is kept, a cross-reference to this should be noted on the personal file.

Safeguarding

32. Under section 5 of the Safeguarding and Clergy Discipline Measure 2016, all members of the clergy authorised to officiate, bishops, archdeacons, churchwardens, licensed readers, lay workers and parochial church councils must pay due regard to guidance issued by the House of Bishops in relation to safeguarding. As such, it is important to note that this "due regard" provision will apply to paragraphs 32 to 39 inclusive. A duty to have 'due regard' to guidance means that the person under the duty is not free to disregard it but is required to follow it unless there are cogent reasons for not doing so. ('Cogent' for this purpose means clear, logical and convincing.) Failure by clergy to comply with the duty imposed by the 2016 Measure may result in disciplinary action.

33. The Disclosure and Barring Service[6] ('DBS') has issued guidance about the record-keeping aspects of criminal record checks[7]. The bishop should check that the registered or umbrella body through which criminal record checks are obtained in his diocese has a written policy on the correct handling and safekeeping of criminal record check information, as required by the DBS Code of Practice.

34. The DBS does not permit certificates to be retained for longer than six months after a recruitment or other relevant decision is made, unless there are exceptional circumstances and the DBS has been consulted. However, a record may be kept of the following:
    - The date of issue of a certificate;
    - The name of the subject;
    - The type of certificate requested;
    - The position for which the certificate was requested;
    - The unique reference number of the certificate;

[6] The Criminal Records Bureau and the Independent Safeguarding Authority merged to form the Disclosure and Barring Service with effect from 1st December 2012

[7] https://www.gov.uk/government/publications/handling-of-dbs-certificate-information/handling-of-dbs-certificate-information

- Details of the recruitment decision taken, including a brief précis of the information provided.

If this information is kept in a consolidated list for the diocese rather than on each personal file, there should be a clear cross reference on the personal file indicating where the individual's criminal record check history can be found. Any police information should be held on the personal file. Currently under House of Bishops' policy criminal record or conviction certificates are renewed every 5 years. Please refer to the House of Bishops' Safer Recruitment Practice Guidance for further details [8].

35. It is essential that a record of any safeguarding allegations and concerns, and how these are handled-how the information was followed up; actions taken; decisions reached and eventual outcomes - should be kept on the clergy personal file so that the bishop is equipped to provide information to the police or other statutory authorities, or to the bishop of another diocese when a request for an Episcopal Reference and CCSL is received. Where relevant papers are not held by the bishop (for example, minutes of meetings of a diocesan safeguarding panel) a cross-reference should be kept on the file with a note that such material should also be consulted if a request for information about safeguarding issues is received.

36. Where an allegation is found to be baseless, or is not substantiated, a record should still be kept, for the benefit of the cleric concerned as well as the bishop[9].

37. A record of a cleric's safeguarding training must be retained on the personal file. Including the exact nature of the training, the date the training was received and who provided the training.

38. Where a file has been scrutinised under the Past Cases Review Protocol, evidence that it has been independently reviewed, together with a note of any action taken as a result, should be kept on the file.

39. A copy of any safeguarding information must be retained when the cleric moves to another diocese (see paragraph 60 below)

Informal complaints

40. Where allegations of misconduct are made which do not result in a formal complaint, it will generally be sufficient to retain a brief summary of the issues and how the matter was resolved.

Complaints under the Clergy Discipline Measure 2003('CDM')

41. A record should be kept on the file of any complaint made under the CDM. Where a complaint is made under the CDM, copies of the complaint, the report on preliminary scrutiny, the respondent's answer (if any), any

[8]. https://www.churchofengland.org/sites/default/files/2017-11/safeguarding%20safer_recruitment_practice_guidance_2016.pdf

[9] See further *Protecting All God's Children* (4th edition) paragraphs 7.28 -7.34

supporting evidence and (if the bishop has determined to dismiss the complaint or to take no further action) the bishop's letter recording his decision should be kept.

42. Where the misconduct is proved or admitted and a penalty imposed, a record of any penalty imposed by consent or the decision of the bishop's disciplinary tribunal (as appropriate) should also be held on the file. If any documents are sent to Lambeth or Bishopthorpe to support an entry on the Archbishops' List, copies should be kept on the personal file so that the bishop retains a full record of the complaint and how it was handled.

Capability and health

43. Any discussion between a cleric and a member of the bishop's senior staff concerning the cleric's capability should be recorded, preferably in the form of a note agreed with the cleric. This practice should be followed whether or not a formal capability inquiry has been instigated under Regulation 31 of the Ecclesiastical Offices (Terms of Service) Regulations 2009.

44. Further advice on record keeping in relation to capability inquiries is contained in paragraph 6 of the supporting advice to the Capability Procedure Code of Practice[10]

45. Where there are significant issues relating to a cleric's health, sufficient evidence to indicate how those issues have been managed in the context of his or her ministry should be held on the file: for example, copies of occupational health reports and a note of any adjustments made to the cleric's duties or pattern of work.

46. The bishop will need to bear in mind, however, that there are statutory restrictions on the disclosure of information about health when a cleric is being considered for appointment to a post (see Annex B to the *Guidance on Parochial Appointments*).

Grievance

47. Annex 1 of the supporting advice to the Grievance Procedure Code of Practice[11] advises that a record should be kept on the personal file of grievances raised under the procedure either by or against the cleric, including details of the grievance, the process followed and the outcome.

Finance

[10] https://www.churchofengland.org/sites/default/files/2017-11/Capability%20Procedure%20Code%20of%20Practice%20Supporting%20Advice.pdf

[11] https://www.churchofengland.org/sites/default/files/2017-10/grievanceprocadvice%20SA.pdf

48. Financial problems can materially affect a cleric's ministry. An undischarged bankruptcy or arrangement with creditors disqualifies a cleric from acting as a charity trustee (including membership of a PCC) unless a waiver is granted by the Charity Commission.

49. Serious financial embarrassment is one of the grounds on which a bishop may refuse to admit or institute a priest to a benefice[12], and a question about financial matters is included in the Episcopal Reference and CCSL. Any significant unresolved financial problems of which the bishop is aware should therefore be noted on a cleric's personal file.

Management of clergy personal files

Format

50. It is for the bishop, as the data controller for the purposes of the GDPR, to determine how information about his clergy is held and managed. In practice, this is likely to involve a combination of paper-based and computer records.

51. For a number of years, the Bishoprics and Cathedrals Department has provided files in the form of blue card folders, with sub-divisions (hence the widely accepted use of the term 'blue files' when referring to clergy personal files). These folders have no official status and bishops are not obliged to use them. They have, however, been found helpful in promoting consistency. The format of these folders will be updated from time to time.

52. It is important that, when personal files are kept in paper-based and electronic format, that the file structures should mirror each other and that all material should be cross-referenced across both formats.

Location

53. The guiding principle here is that all personal information about clergy must be held together in one place and be managed by the diocesan bishop and his staff, although in larger dioceses it may be necessary for suffragan bishops to hold the personal file of those clergy for whom they are responsible (see further paragraphs 66- 68). Those staff who contribute information to clergy personal files (for example, archdeacons) need to be clear about where the file of any cleric is kept and the arrangements for keeping it updated. They should not keep separate files (other than day to day working papers), and where this is the case a note should be placed on the file to indicate that material is held elsewhere and to explain how it may be accessed. Such working papers should be transferred periodically to the main file: each diocese should have in place a policy to ensure that this happens regularly and systematically.

54. It is important to have a clear policy in place explaining who among the bishop's staff may have access to the files and the conditions of use (which should include a stipulation that the files are not removed from the bishop's

[12] Canon C10.3(a)

office). Confidential or sensitive material may be kept on the file in a sealed envelope marked with instructions that it may only be opened by the bishop and particular members of his staff.

Security

55. The sixth data protection principle provides that personal data shall be processed in manner that ensures appropriate security for that data, including protection against unlawful and unauthorised processing of personal data and against accidental loss, destruction or damage, using appropriate technical or organisational measures

56. What is appropriate in any case will depend on the particular circumstances, but the following suggestions are offered as examples of standard good practice[13]:

- establishing clear rules as to which members of the bishop's staff may have access to the files (see paragraph 54 above);
- keeping paper files in locked, cabinets, with access to keys limited to authorised staff;
- Ensuring that premises are properly protected with burglar and fire alarms;
- protecting records held on computer with permissions managed to ensure access is restricted only to those who are entitled to access files;
- transmitting personal data electronically only in encrypted form;
- using secure delivery methods such as "guaranteed delivery" and "track and trace" if sending personal data through the post;
- regularly backing up electronic files.

57. If you use 'cloud' based services for data storage (or for any other data processing), you can only use a processor that provides "sufficient guarantees to implement appropriate technical and organisational measures" in such a way that the processing will meet the requirements of the GDPR and ensure the rights of the data subjects. This means that there is an obligation on the data controller to test and examine the service it intends to use. Enquiries must therefore be made before personal information is committed to a cloud service provider.

Updating and retention

[13] The ICO has issued guidance on IT security measures for small organisations and businesses: https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf

58. The fourth data protection principle states that personal data must be accurate and, where necessary, kept up to date. The data controller is required to take reasonable steps to ensure accuracy. The bishop should therefore put in place a means whereby clergy are asked to check and update their biographical details from time to time. One possible way of doing this would be to link the updating exercise to the ministerial review cycle, thus ensuring that the data is reviewed at least once every two years.

59. The fifth data protection principle provides that personal data should not be kept for longer than is necessary in relation to the purpose or purposes for which it is being processed. Whilst there is no statutory provision as to how long any particular category of data should be retained, provided that it is still required for the purpose for which it was obtained. The Retention Schedule (Appendix 1) contains details of agreed common retention periods for particular categories of personal data in clergy personal files.

60. Section 5 of the Safeguarding and Clergy Discipline Measure 2016 will apply to this paragraph, (see paragraph 32). Any material which relates to safeguarding allegations and/or concerns; how such issues were dealt with and the ultimate outcome of any investigations must be retained in the file until 70 years after the cleric's death. Where a cleric moves diocese and the personal file is passed to the receiving bishop, a copy record of all safeguarding matters, as mentioned above, must be included in the personal file sent to the new diocese. The originals must be retained for the same period in the diocese which dealt with the allegation or complaint, so that the bishop or his/her successor can provide evidence of how a particular matter was handled if necessary.

61. Material relating to CDM complaints should be retained during the lifetime of the cleric and thereafter following the guidance in paragraphs 64-65 below. This applies even where a CDM complaint has been shown to be baseless or malicious, so that the cleric is protected if the complainant seeks to reopen the same issues. Where a cleric moves diocese and the personal file is passed to the receiving bishop, a copy record of disciplinary matters must be included in the personal file sent to the new diocese. The originals must be retained for the same period in the diocese which dealt with the disciplinary matter, so that the bishop or his/her successor can provide evidence of how a particular matter was handled if necessary.

62. It is also advisable to keep during the cleric's lifetime (and thereafter following the guidance in paragraph 65 below) a record of how capability issues that have arisen have been addressed. Clergy on Common Tenure have a right of appeal to an Employment Tribunal if they are removed from office under the capability procedure, and in such cases the Tribunal will expect the bishop to provide evidence of all the relevant history, including any discussions and actions that precede the formal process.

63. For other categories of personal data which are not covered by Data Sharing Agreements (for example, routine administrative correspondence relating to a particular cleric) the bishop, with his staff, should develop a retention policy,

incorporating regular reviews of what is held. This policy should then be applied consistently to the clergy personal files which he holds.

64. Where information is held electronically, care should be taken to ensure that a decision to delete it is properly implemented so that it cannot be reinstated (or at the very least that it is put beyond use). The Information Commissioner has produced guidance on this[14]. Paper records containing confidential and/or sensitive information should be incinerated, shredded or pulped (and pending destruction should be stored securely in a sealed bag or box appropriately marked).

65. When a person dies, the GDPR ceases to apply. It is important that, when a retired cleric dies, the Pensions Board should inform the bishop of the diocese where the cleric last resided. Files should no longer be passed to third parties such as local record offices, but after the cleric's death the file should be retained by the Bishops office for 70 years and then destroyed.

66.

Sharing information in clergy personal files

The bishop's office and senior staff

67. The guiding principle is that all personal information about a cleric must be held in one place – the personal file – and that no separate files (other than day to day working papers) be kept (see paragraph 53). Staff who contribute information to clergy personal files need to be clear about where the file of any cleric is kept and the arrangements for keeping it updated.

68. Wherever practicable, the files should be kept together in the diocesan bishop's office and under his or her control. However, in larger dioceses, especially those with formal area schemes, it may be necessary for suffragan bishops to hold and manage the personal files relating to clergy for whom they have delegated responsibility. Where this is the case, it is important that the diocesan bishop and the relevant suffragan should both register as joint data controllers and pay the "data protection fee" (see paragraph 11) to the ICO as joint data controllers in respect of the same files.

69. These principles should be followed, and if they are there should be no difficulty from a data protection perspective in the bishops within a diocese sharing information from clergy personal files between themselves or with members of their senior or administrative staff for proper purposes, provided that appropriate security measures are taken. There should be a clear policy setting out who may have access to the files and for what purpose. The safeguarding adviser should always be among those who are given permission to consult the files.

[14] https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf

The cleric

70. Similar to the DPA, the GDPR confers a right of access by an individual to personal data held about him or her. This does not mean, however, that clergy can simply demand to see their files. Under the GDPR, individuals have the right to be given confirmation that their data is being processed; access to their personal data and supplementary information, (i.e. information that is usually included in the privacy/data protection notice, such as the purposes of the processing, the retention periods etc.). Individuals continue to be able to make "Subject Access Requests" to access their personal data so that they are aware of and can check the lawfulness of the use and the accuracy of the data.

71. In most cases, data controllers can no longer charge for "Subject Access Requests" and will have only 1 month to respond from the receipt of the request rather than the 40 days under the DPA. Data controllers will be able to charge a "reasonable administrative fee" for requests that are manifestly unfounded, excessive or repetitive. If a request is refused you must be able to the explain to the individual why and that he/she has a right to complain to the ICO or to a judicial remedy.

72. Not all personal data should necessarily be disclosed on a subject access request, and bishops should seek advice from the diocesan registrar. In particular, care must be taken when any information relates to an identifiable third party. Such information should not normally be disclosed without the third party's consent, unless it is reasonable in all the circumstances to do so.

73. There are also exceptions which permit data to be withheld on a subject access request where disclosing it would prejudice the prevention or detection of crime, or the proper exercise of functions designed to protect the public from professional misconduct or incompetence.

74. The Information Commissioner has produced a useful code of practice for handling subject access requests [15].

Third parties

75. As a general principle, other than providing an Episcopal Reference and CCSL (see para 79 below), personal information from clergy files should not be shared with third parties outside the institutional Church of England without the explicit consent of the individual concerned, unless the information is already in the public domain as the result of action deliberately taken by him or her or where there are clear exceptions (see subsequent paragraphs). Article 9(2)(d) of the GDPR permits the processing of "special categories of personal data" if the processing is carried out in the course of the legitimate activities of a not-for-profit body, with appropriate safeguards (see paragraph s 55-58 above in relation to security). This is provided that the processing relates solely to members or former members or individuals who have regular contact with it in connection with the bodies' purposes and the

[15] https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf

personal data is not disclosed outside "that body" without the consent of the data subject. The view has been taken that the body in this instance should apply to the institutional legal bodies/organisations that comprise the Church of England and so personal data can be shared between these bodies for the purposes of administration and connected purposes, in order that the Church can function as an institution.

76. There continue to be circumstances where sensitive (now special category) personal data can be shared without consent. In particular, where the disclosure is necessary for the prevention or detection of any unlawful act, or for the discharge of any function which is designed for protecting members of the public against seriously improper conduct or incompetence, and it must necessarily be carried out without explicit consent being sought so as not to prejudice those purposes, the disclosure may be made.

77. Additionally, there has been an amendment to the data protection legislation, which now provides a lawful ground for the processing of special category personal data, without consent if the circumstances justify it in safeguarding situations, where it is in the substantial public interest, and is necessary for the purposes of:-

    - Protecting an individual from neglect or physical, mental or emotional harm; or
    - Protecting the physical, mental or emotional well -being of an individual

    where that individual is a child (i.e. under 18) or is an adult at risk, (i.e. vulnerable – as defined). That said, in the first instance, obtaining consent should still be considered. If, after having considered the position, consent cannot be obtained (e.g. because the obtaining of consent would prejudice the safeguarding purposes) then the ground can be relied upon.. As such, the disclosing of safeguarding information without consent to the police and/or the statutory authorities should be justifiable in most cases.

    It is good practice to document any decision to share personal data without consent, detailing what was shared and explaining why the disclosure was made. The ICO recognises that in time-critical situations it may not be possible to record the decision until after the disclosure has been made.

78. The sharing of information about clergy between diocesan bishops, and the transfer of such files when clergy move to a new diocese within the Church of England (including the Diocese in Europe), is governed by Data Sharing Protocol and agreements in place between the institutional organisation of the Church of England and is necessary for the legitimate interest of the data controller and part of a legitimate activity of a not-for-profit body, in order to regulate/administer membership and/or those in regular contact.

79. Where a priest or deacon moves to take up a new appointment or permission to officiate ('PTO') in another diocese in the Church of England, the sending bishop will not transfer to the receiving bishop the clergy personal file until

the point where the priest or deacon's ministry in the sending diocese ends (which, in the parochial context, means in practice the person's last Sunday in the parish). Once the new appointment is confirmed and the ministry in the sending diocese ends then the file should be transferred. It is not necessary to wait until after licensing to the new post before transferring the file. Under the DPA, consent of the cleric was always sought prior to the transfer of the file. Under the GDPR consent is no longer an appropriate legal basis that can be relied upon to process this personal data. Instead, the transfer of the file between two Church of England bodies is considered to be a legitimate activity of a not-for-profit body for its own internal purposes in order to regulate/administer etc. its membership and/or those in regular contact, so under the GDPR no consent will be required. Nevertheless, the position remains that the file ***follows*** the cleric. It should not be made available to the receiving Bishop until ***after*** an appointment is confirmed.

80. Where a priest or deacon takes up appointment in a diocese which is not part of the Church of England (including the Church in Wales, the Church of Ireland or the Episcopal Church of Scotland) the clergy personal file will be retained by the bishop in whose diocese the cleric last served, and information from it will **only** be disclosed outside the Church of England with the individual's consent, (with the exception of an Episcopal Reference and CCSL). Clergy personal files must not be transferred outside of the Church of England.

81. Where a priest or deacon is being considered for an appointment or PTO in another diocese, (i.e. the receiving bishop's diocese), and the sending bishop receives a request from the receiving bishop for an Episcopal Reference and CCSL, the sending bishop will share with the receiving bishop such personal information about that priest or deacon as is necessary to provide a full and accurate response. The legal basis for disclosing this information is that it is necessary for the legitimate interests of the data controller (pursuant to Article 6 of the GDPR) and in so far as the information is "special category" (i.e. sensitive) under Article 9 or criminal conviction and offence data under Article 10, it is necessary for the reasons of substantial public interest on the basis of UK law, (see Article 9(2)(g) and section 10(5) of the Data Protection Act 2018, Schedule 1 Part 2, paragraph 11) for the protection of members of the public from harm by ensuring that those who pose a risk or are otherwise unfit for ministerial positions, (due to, for instance, dishonesty, malpractice or other seriously improper conduct) are not able to gain access to ministerial posts. This applies to not only posts within the Church of England but also posts outside the Church of England. The Episcopal Reference and CCSL provide sufficient information for a Bishop in the receiving diocese/church outside of the Church of England to make an appointment decision and start his/her own personal file on the cleric.

82. Under the Data Protection Act 2018, where a data controller (in this case the Bishop) is seeking to rely on Article 9(2)(g) and the "substantial public interest" condition, (this will also apply to the processing of criminal conviction and offence data under Article 10), the data controller must have an "appropriate policy document", which sets out the procedures in place for

ensuring compliance with the data protection principles, (see paragraph 6 above) in connection with the processing of the data. The policy document must also explain the data controller's policies as regards retention and erasure of the personal data involved in this processing and must give an indication of how long the personal data will be retained.

83. The Bishop must retain the policy document; review and update it from time to time and make it available to the ICO, if requested so to do[16].

84. The Bishop must also keep a record of any processing that is done in reliance on this condition. Such a record, must state which condition is being relied upon; how the processing satisfies Article 6 of the GDPR and whether the personal data is retained and erased in accordance with the policy document. If not, reasons must be given. Provided there is a "data protection policy" already in place, which, inter alia, covers the matters mentioned above, then that should suffice as "an appropriate policy document".

85. Where a cleric moves to a specialist ministry in England (e.g. the Secretary of a Missionary Society) and he or she holds a bishop's licence in connection with that ministry, the personal file should be transferred to the diocesan bishop who issues the licence. If he or she is to serve under contract without a licence, the file should remain in the diocese where the cleric last served.

86. Where a cleric is appointed as a regular chaplain to the Armed Forces the personal file will be sent to Lambeth Palace. Where a cleric is appointed to a role at a Royal Peculiar, the personal file will be sent to the head (e.g. the Dean) of the relevant Peculiar. The personal file of the head of a Royal Peculiar will be held by the registrar of the Archbishop of Canterbury or York, depending where the Peculiar is situated. If that person returns to diocesan ministry, a brief summary of his or her Forces posting or appointment in the Royal Peculiar will be added to the personal file before the file is sent to the receiving bishop, to ensure that the record of his or her ministry is complete. Armed Forces Chaplaincies are aware of the procedures governing Episcopal References and CCSLs and will comply with these when providing or requesting references.

87. Where a cleric retires, the personal file should remain in the diocese in which he or she last served unless and until he or she is granted permission to officiate ('PTO') in another diocese.

88. Where a cleric ceases to hold a PTO or leaves the ministry of the Church of England, the personal file should be retained in the diocese where he or she last served.

89. Where a cleric holds a licence or PTO concurrently in more than one diocese, the personal file should be held in the diocese where the cleric exercises the greater part of his or her ministry. A note should be kept on the file as to

[16] Under the Data Protection Act 2018, the "appropriate policy document" must be kept from the start of the processing which is relying on the "substantial public interest condition" until 6 months after the processing has ceased.

which other dioceses have issued a licence or PTO and the expiry date(s); and arrangements put in place for the appropriate staff of those dioceses to have access to the file as necessary. The other dioceses should in turn keep a record of where the personal file is held.

Privacy Notices

90. The first principle of "fair and transparent" processing requires the data controller to provide information to an individual about its processing of his/her data, unless the individual already has this information. The information to be provided is specified in the GDPR and summarised below. The data controller may also have to provide additional information if, in the specific circumstances and context, this is necessary for the processing to be fair and transparent.

The information must be provided in a concise, transparent, intelligible and easily accessible way, using clear and plain language (in particular where the data subject is a child).

91. What must a data controller tell individuals?

The GDPR requires more extensive information to be provided than the DPA. The data controller must provide the following details:-

- Identity and contact details of the controller (or its representative, for a non-EU established controller); contact details of the Data Protection Officer.
- Purposes of processing and legal basis for processing – including the "legitimate interest" pursued by the controller (or third party) if this is the legal basis.
- Recipients, or categories of recipients
- Details of data transfers outside the EU: including how the data will be protected (e.g. the recipient is in an adequate country; Binding Corporate Rules are in place etc.); and
- how the individual can obtain a copy of the BCRs or other safeguards, or where such safeguards have been made available.
- The retention period for the data – if not possible, then the criteria used to set this.
- That the individual has a right to access and port data, to rectify, erase and restrict his or her personal data, to object to processing and, if processing is based on consent, to withdraw consent.
- That the individual can complain to a supervisory authority.
- Whether there is a statutory or contractual requirement to provide the data and the consequences of not providing the data.

- If there will be any automated decision taking – together with information about the logic involved and the significance and consequences of the processing for the individual.

92. When must a data controller provide this information?

    This depends on whether the data controller gets the information directly from the data subject or from a third party.

Data controller obtains information directly from individual

- At the time the data are obtained.
- The data controller must also tell individuals what information is obligatory and the consequences of not providing information.

Data controller does not obtain information directly from individual

- Within a reasonable period of having obtained the data (at most one month); or
- If the data are used to communicate with the individual, at the latest, when the first communication takes place; or
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- The data controller must also tell individuals the categories of information and the source(s) of the information, including if it came from publicly accessible;
- The data controller does not have to provide this information to the individual if it would be impossible or involve a disproportionate effort. In these cases, appropriate measures must be taken to protect individuals' interests and the privacy notice must be made publicly available.
- There is also no need to provide the privacy notice if there is an EU or Member State law imposing an obligation on the data controller to obtain/disclose the information; or if the information must remain confidential, because of professional or statutory secrecy obligations, regulated by EU or Member State law.

93. If the data controller later processes personal data for a new purpose, not covered in the initial notice, then it must provide a new notice covering the new processing

94. It is therefore recommended that a privacy notice should be given to the cleric by the bishop who holds the personal file about him or her. When he or she moves to a new diocese, a fresh privacy notice should be given by the receiving bishop.

95. The purposes of the privacy notice are to ensure that clergy are properly informed about how their personal information will be used, managed etc.; the legal basis for that processing and their rights in respect of that data

96. A model privacy notice is provided in Appendix 2. However, this may need adaptation to fit the circumstances of any particular case.

Appendix 1

Retention Schedules – what is kept and for how long

The following agreed common retention periods apply to particular categories of information held in clergy personal files while those files are held under the management of the bishop.

Record type	**Retention period**
Relates to paragraph 24 A note of the reasons for processing sensitive personal data	Length of time the data to which the note is held
Relates to paragraph 26 Common Application Form	Successful application forms should be held on the file for 20 years from the date of the cleric's death
Relates to paragraph 27 Copy of birth certificate (or other appropriate evidence) required under Canon C.6 in relation to a person who is to be made a deacon	20 years from the date of the cleric's death
Relates to paragraph 27 Evidence of immigration status and permission to work in the UK (if the cleric is not a British citizen)	20 years from the date of the cleric's death or Date of cleric becoming British citizen *(which ever is soonest)*
Relates to paragraph 27 Copies of qualification certificates	20 years from the date of the cleric's death
Relates to paragraph 27 Cleric's CV since leaving school	20 years from the date of the cleric's death
Relates to paragraph 28 Copy of faculty under Canon C4.3A	20 years from the date of the cleric's death
Relates to paragraph 28 Report of the Bishop's Advisory Panel and reports from the cleric's training institution in the penultimate and final years of training	20 years from the date of the cleric's death
Relates to paragraph 29 Copies of cleric's letters of orders and (if relevant) permission under the Overseas and Other Clergy (Ordination and Ministry) Measure 1967	20 years from the date of the cleric's death
Relates to paragraph 29 Copies of any 'safe to receive' or Episcopal Reference and Clergy Current Status letters ('CCSL')	70 years from the date of the cleric's death
Relates to paragraph 29 Application papers – including	Papers relating to successful applications should be held on the file for 20 years

application form, references, copy licence, deed of institution, Statement of Particulars (where subject to Common Tenure)	from the date of the cleric's death
Relates to paragraph 30 A written record of any Ministerial Development Review	20 years from the date of the cleric's death
Relates to paragraph 31 Records of any continuing ministerial education ('CME') undertaken	20 years from the date of the cleric's death
Relates to paragraphs 33-34 Criminal Record Check certificate	6 months from the date of the recruitment decision to which they relate *Certificates can only be retained for a longer period in exceptional circumstances and where the Disclosure and Barring Service have been consulted*
Relates to paragraphs 33-34 Record of a cleric's criminal record check history (the nature of which is noted in paragraph 29)	70 years from the date of the cleric's death
Relates to paragraphs 35 and 60 Record of safeguarding allegations and concerns – including details of how these are handled, followed-up, actions taken, decisions reached and eventual outcome	70 years from the date of the cleric's death
Relates to paragraph 38 Evidence of clergy personal file being independently scrutinised under the Past Cases Review Protocol – including a note of any action resulting	70 years from the date of the cleric's death
Relates to paragraphs 39 and 60 Copies of records relating to safeguarding allegations and concerns (this refers to papers being retained in a diocese following the movement of the cleric to another diocese)	70 years from the date of the cleric's death
Relates to paragraph 37 Record of a cleric's safeguarding training – including the nature of the training, the date of the training and who provided the training	70 years from the date of the cleric's death
Relates to paragraph 41-42 Record of CDM complaints – including copies of the complaint, report on preliminary scrutiny, respondent's answer, supporting evidence, letter recording bishop's decision	70 years from the date of the cleric's death
Relates to paragraph 40	20 years from the date of the cleric's

A brief summary of an allegation of misconduct (not resulting in a formal CDM complaint)	death
Relates to paragraphs 43-44 Records of capability inquiries raised under the Capability Procedure – including a record of discussions between a cleric and a member of the bishop's senior staff, evidence of how health issues have been managed (e.g. copies of occupational health reports, note of adjustments made)	20 years from the date of the cleric's death As noted in the Capability Procedure code of practice – spent warnings should be retained on file in a sealed envelope for as long as the office holder remains in post, but should then be destroyed, unless the next post to which the office holder is appointed is designated as a probationary post, or there are other circumstances which justify retaining them
Relates to paragraph 43 Record of capability issues (where there is no formal capability inquiry)	20 years from the date of the cleric's death
Relates to paragraph 47 Record of grievances raised under the Grievance Procedure – including details of the grievance, the process followed and the outcome	20 years from the date of the cleric's death
Relates to paragraphs 48-49 Record of significant unresolved financial problems	Keep the record until financial problems have been satisfactorily resolved
Relates to paragraph 65 Personal files after a cleric's death	70 years from the date of the cleric's death

Appendix 2
(See paragraphs 77-80 of the Guidance)

Model Privacy Notice from the diocesan bishop

Using your personal information

This notice explains how the information about you which I hold in your personal file is used, managed and your rights with respect to that data.

Your personal data – what is it?

Personal data relates to a living individual who can be identified from that data. Identification can be by the information alone or in conjunction with any other information in my possession or likely to come into such possession. The processing of personal data is governed by the General Data Protection Regulation 2016/679 (the "GDPR") and the Data Protection Act 2018, (the "DPA 2018")

Who am I?

[I*nsert name of diocesan bishop*] am the data controller (contact details below). This means I decide how your personal data is processed and for what purposes.

How do I process your personal data?

I comply with my obligations under the GDPR and DPA 2018 by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data.

I use your personal data for the following purposes: -

To exercise my legal and pastoral responsibilities as your diocesan bishop. In addition to my general oversight of your ministry, I am responsible for assessing your qualifications and suitability for any particular office or ministry within the diocese, and for making appropriate arrangements for your ministerial development (including ministerial development review).

What is the legal basis for processing your personal data?

Processing of the personal data in relation to clergy personal files is necessary for the purposes of legitimate interests in accordance with my responsibilities under the Canons, including my general responsibilities as chief pastor of the diocese and in order to be able to develop, support, administer, regulate and manage clergy through their ministry and in so far as any personal data relates to "special categories of personal data" or criminal conviction or offence data the processing is a legitimate activity in order to manage and administer internal functions in relation to membership and/or those with whom I have regular contact. It is not shared externally outside the institutional bodies that comprise the Church of England without your consent. The exception to this is the provision of Episcopal References and Clergy Current Status Letters ("CCSL")..

Episcopal References and CCSLs are processed on the basis that it is a legitimate interest as established by the Promoting a Safer Church House of Bishops Policy Statement (2017)[17]. However, in so far as the personal data contained within the Episcopal Reference and CCSL relates to "special categories of personal data" and criminal conviction and offence data, this will be processed on the basis that it is necessary for reasons of substantial public interest on the basis of UK law. The Episcopal Reference and CCSL will be disclosed both for posts within the Church of England and externally, where you have applied for a ministerial post in another diocese or a church outside the Church of England and is done so in order to protect members of the public from harm, including dishonesty, malpractice and other seriously improper conduct or safeguarding purposes as established by the Safer Recruitment: Practice Guidance (2016)[18].

Sharing your personal data

Your personal data will be treated as strictly confidential, and will be shared only when necessary with institutional bodies that comprise the Church of England for the purposes of administrative functions in connection with your role. If I wish to share your personal data outside the Church of England, then I will always seek your consent first.

How long do I keep your personal data?

I keep your personal data for no longer than reasonably necessary for the periods and purposes as set out in the attached retention table [at the following link: https://www.churchofengland.org/sites/default/files/2018-06/Personal%20Files%20Relating%20to%20Clergy%202018%20Edition.pdf[]

Your rights and your personal data

Unless subject to an exemption under the GDPR or DPA 2018, you have the following rights with respect to your personal data: -

- The right to request a copy of your personal data which the Bishop holds about you;
- The right to request that the Bishop corrects any personal data if it is found to be inaccurate or out of date;
- The right to request your personal data is erased where it is no longer necessary for the Bishop to retain such data;
- The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- The right to object to the processing of personal data, (where applicable);
- The right to lodge a complaint with the Information Commissioners Office.

[*Transfer of Data Abroad*

If the personal data is to be transferred to countries or territories outside the EU you must include details of how the data will be protected, together with details of how to obtain copies of the relevant safeguards].

[***Automated Decision Making***

[17] https://www.churchofengland.org/sites/default/files/2017-12/PromotingSaferChurchWeb.pdf
[18] https://www.churchofengland.org/sites/default/files/2017-11/safeguarding%20safer_recruitment_practice_guidance_2016.pdf

You will need to provide details of any automated decision making, together with information about the logic involved and the significance and consequences of the processing for the individual].

Further processing

If I wish to use your personal data for a new purpose, not covered by this Data Protection Notice, then I 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, I will seek your prior consent to the new processing.

Contact Details

To exercise all relevant rights, queries or complaints please contact [*insert details of the lead person for Data Protection at the Bishops office*]].

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.