

# PERSONAL FILES RELATING TO CLERGY

Guidance  
for  
Bishops and their staff

Approved by the House of Bishops on 13<sup>th</sup> March 2013



## **Personal Files relating to Clergy**

### **Guidance for bishops and their staff**

**Approved by the House of Bishops on 13<sup>th</sup> March 2013**

#### **Foreword**

Some time ago the Standing Committee of the House of Bishops concluded that a review was needed of the arrangements for holding and sharing personal information about clergy.

The House of Bishops considered the outcome of the review in December and proposals for a new guidance document. It welcomed the extensive and careful work that Church House, Lambeth and Bishopthorpe staff had put into the exercise to ensure that information was held and, as necessary, shared in a way that met the needs of the Church of England, was fair to clergy and was compliant with data protection principles.

The House authorised the Standing Committee to agree the final text of the guidance and the data sharing protocol. This it did at a meeting on 13 March.

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**

**April 2013**

## **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 previous guidance entitled '*Confidential Files on Clergy – Guidance Notes for Bishops and Bishops' Secretaries*'.
2. The guidance deals only with personal files about clergy ("clergy personal 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 DDOs 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. This guidance does not extend to these files, although again the same general principles apply.

## **Overview of relevant legal requirements**

### Data Protection

4. The Data Protection Act 1998 ("DPA") 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 is termed 'personal data' in the DPA. Processing is widely defined and includes obtaining information, holding it (whether in paper or electronic form) and sharing it with others.
5. The DPA sets out eight fundamental principles which must be observed when processing personal data. These can be summarised as follows:
  - 1) Personal information must be processed fairly and lawfully.
  - 2) It must be obtained for one or more lawful and specified purposes, and processed in a manner compatible with that purpose or those purposes.
  - 3) It must be adequate, relevant, and not excessive in relation to the purpose(s) for which it is processed.
  - 4) It must be accurate and, where necessary, kept up to date.
  - 5) It must not be kept for any longer than is necessary for the purpose(s) for which it is processed.
  - 6) It must be processed in accordance with the rights conferred by the DPA on the person who is the subject of the information ('the data subject').

- 7) Appropriate measures must be taken to protect the information from unauthorised or unlawful processing and against accidental loss, destruction or damage.
  - 8) The information must not be transferred to a country outside the European Economic Area unless that country has an adequate data protection regime.
6. The DPA also provides that certain information is to be treated as ‘sensitive personal data’ 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, union membership or criminal record (including any allegation that a criminal offence has been committed).
  7. The Information Commissioner’s website ( [www.ico.gov.uk](http://www.ico.gov.uk) ) is a useful resource which provides general and specialist guidance on many aspects of the DPA.
  8. Any data controller - defined as a person 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 required under the DPA to notify the Information Commissioner if he or she processes personal data electronically, unless the processing falls within certain exempt categories. Failure to notify is a criminal offence. The details provided are used by the Information Commissioner to maintain a public register of data controller and the categories of personal information which they process.
  9. The administration of pastoral care by a minister of religion is a non-exempt purpose and therefore clergy personal files fall within the notification requirements. The diocesan bishop, as the data controller for these files, should already have submitted a notification. Guidance on keeping the notification up to date can be found on the Information Commissioner’s website.

### Confidentiality

10. 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.
11. 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.

12. 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

13. The bishop needs to take account of the data protection principles described in paragraph 5 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 state that personal data must only be obtained for a lawful and specified purpose.
  - *Do I have the cleric's consent to hold this information on file? If not, does the DPA allow me to hold it without such consent?* 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 Information Commissioner as sensitive personal data for the purposes of the DPA, and the default position is that processing such data requires the explicit consent of the data subject.

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

14. In making this assessment the bishop should have regard to his 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 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).

#### *Do I have the cleric's consent to hold this information on file? If not, does the DPA allow me to hold it without consent?*

15. As explained in paragraph 13 above, the default position in relation to sensitive personal data is that any processing requires the explicit consent of the data subject. This should not present any problem where the information has been supplied by the individual to whom it relates, provided that he or she understands the purposes for which it will be used (as to which see the section on privacy notices later in this guidance).

16. Where information is supplied by a third party (i.e. a person outside the bishop's office and senior staff) without the consent of the cleric concerned having been obtained through a privacy notice or otherwise, the bishop will need to consider whether the circumstances permit him to hold it on that basis.
17. The DPA (and subordinate legislation made under it) set out a limited number of situations in which processing sensitive personal data without consent is permitted, including where the processing:
  - (a) is in the substantial public interest and is necessary for the prevention or detection of any unlawful act;
  - (b) is in the substantial public interest and is necessary for the discharge of any function which is designed to protect members of the public against dishonesty, malpractice or other seriously improper conduct, or the unfitness or incompetence of any person;
  - (c) is necessary for the exercise of any function conferred by an enactment (which includes a Measure of the Church of England); or
  - (d) is necessary in connection with any actual or prospective legal proceedings, or for the purpose of obtaining legal advice;
  - (e) relates to members or regular contacts of a not-for-profit religious organisation, provided that the data is not shared with third parties without consent.
18. The bishop should seek the advice of his registrar if he has concerns about whether he is entitled to hold a particular piece of personal information in a clergy file. It is also good practice to document any decisions taken about the processing of sensitive personal information where the individual's consent has not been obtained, 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*

19. 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. While the bishop may, if he wishes, prepare and use a standard form within his diocese to collect, and periodically update, basic biographical details about his clergy for their personal files, the practice of using such a form as a CV for the purpose of appointment is no longer recommended.
20. 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 Common Application Form<sup>1</sup>. This will help to ensure that the information

---

1

<http://www.churchofengland.org/media/1493346/common%20application%20form%20june%202012.doc>

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.

21. 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 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*

22. 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 C4.3A has been granted, a copy should be kept on the file.
23. 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 any Clergy Current Status letters ('CCSL') 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*

24. 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. Where clergy who are not on Common Tenure participate in MDR, it is good practice to keep a similar record in relation to them.
25. 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*

26. The Disclosure and Barring Service<sup>2</sup> ('DBS') has issued guidance about the record-keeping aspects of criminal record checks<sup>3</sup>. 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.
27. 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;
  - 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

---

<sup>2</sup> The Criminal Records Bureau and the Independent Safeguarding Authority merged to form the Disclosure and Barring Service with effect from 1<sup>st</sup> December 2012

<sup>3</sup> [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/143669/handling-dbs-cert.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/143669/handling-dbs-cert.pdf)

indicating where the individual's criminal record check history can be found. Any police information should be held on the personal file.

28. 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 a 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.
29. 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<sup>4</sup>.
30. Where a file has been scrutinised under the Past Cases Review Protocol<sup>5</sup>, evidence that it has been independently reviewed, together with a note of any action taken as a result, should be kept on the file.
31. A copy of any safeguarding information should be retained when the cleric moves to another diocese (see paragraph 53 below)

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

32. A record should be kept on the file of any complaint made under the CDM. 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.
33. Where a complaint is made under the CDM, copies of the complaint, the report on preliminary scrutiny, the respondent's answer (if any), any 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.
34. 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.

---

<sup>4</sup> See further *Protecting All God's Children* (4<sup>th</sup> edition) paragraphs 7.28 -7.34

<sup>5</sup> <http://www.churchofengland.org/media/36120/cpreviewprotocol.pdf>

### *Capability and health*

35. 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.
36. 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<sup>6</sup>
37. 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.
38. 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*

39. Annex 1 of the supporting advice to the Grievance Procedure Code of Practice<sup>7</sup> 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*

40. 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.
41. Serious financial embarrassment is one of the grounds on which a bishop may refuse to admit or institute a priest to a benefice<sup>8</sup>, and a question about financial matters is included in the CCSL. Any significant unresolved financial problems of which the bishop is aware should therefore be noted on a cleric's personal file.

---

<sup>6</sup>

<http://www.churchofengland.org/media/56745/10%203%2026%20capability%20supporting%20advice.pdf>

<sup>7</sup> <http://www.churchofengland.org/media/56749/grievanceprocadvice%20sa.pdf>

<sup>8</sup> Canon C10.3(a)

## **Management of clergy personal files**

### Format

42. It is for the bishop, as the data controller for the purposes of the DPA, 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.
43. For a number of years, the Bishops 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.
44. 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

45. The guiding principle here is that all personal information about clergy should, wherever possible, 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 59- 61). 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.
46. 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 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

47. The seventh data protection principle provides that appropriate measures must be taken against unlawful and unauthorised processing of personal data and against accidental loss, destruction or damage.

48. What is appropriate in any case will depend on the particular circumstances, but the following suggestions are offered as examples of standard good practice<sup>9</sup>:

- establishing clear rules as to which members of the bishop's staff may have access to the files (see paragraph 36 above) ;
- keeping paper files in locked, fire-proof cabinets, with access to keys limited to authorised staff;
- protecting records held on computer with permissions (at folder level) that are changed regularly;
- transmitting personal data electronically only in encrypted form;
- using recorded delivery if sending personal data through the post;
- regularly backing up electronic files.

49. The eighth data protection principle - which restricts the transfer of personal data outside the European Economic Area unless adequate safeguards are in place - is relevant to the use of 'cloud' based services for data storage, as these services do not always tell the customer where the data is actually stored. Enquiries must therefore be made before personal information is committed to one of these services.

#### Updating and retention

50. 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.

51. 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.

52. 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 Data Sharing Protocol (Appendix 1) contains details of agreed common retention periods for particular categories of personal data in clergy personal files.

---

<sup>9</sup> The ICO has issued guidance on IT security measures for small organisations and businesses:

[http://www.ico.gov.uk/for\\_organisations/guidance\\_index/data\\_protection\\_and\\_privacy\\_and\\_electronic\\_communications.aspx#security](http://www.ico.gov.uk/for_organisations/guidance_index/data_protection_and_privacy_and_electronic_communications.aspx#security)

53. It is strongly recommended that any material which relates to safeguarding concerns should be retained in the file until 50 years after the cleric's death, and material relating to CDM complaints should be retained during the lifetime of the cleric and thereafter following the guidance in paragraphs 57-58 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 safeguarding and disciplinary matters should also be retained for the same period in the diocese which dealt with the allegation or complaint, so that the bishop or his successors can provide evidence of how a particular matter was handled if they are called upon to do so.
54. It is also advisable to keep during the cleric's lifetime (and thereafter following the guidance in paragraphs 57-58 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.
55. For other categories of personal data which are not covered by the Data Sharing Protocol (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.
56. 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<sup>10</sup>. 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).
57. When a person dies, the DPA 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. After a cleric's death the personal file should be retained for 7 years before being offered to the diocesan archives, usually the County Record Office. The file remains the property of the diocese, and will be kept under whatever arrangements have been agreed with the County Record Office as regards their confidentiality, appraisal and long-term retention or disposal. It is suggested that the file should not be opened to public inspection for 30 years without the express written consent of the bishop.

---

10

[http://www.ico.gov.uk/for\\_organisations/guidance\\_index/data\\_protection\\_and\\_privacy\\_and\\_electronic\\_communications.aspx#deletion](http://www.ico.gov.uk/for_organisations/guidance_index/data_protection_and_privacy_and_electronic_communications.aspx#deletion)

58. Should the diocesan archives be unwilling to accept personal files relating to deceased clergy, such files should be retained for 20 years and then destroyed, with the important exception of any material relating to safeguarding. This material should be retained for 50 years after the date of the cleric's death, in the diocese where the file was last held (see the Data Sharing Protocol: Appendix 1)

## **Sharing information in clergy personal files**

### The bishop's office and senior staff

59. The guiding principle is that all personal information about a cleric should be held in one place – the personal file – and that no separate files (other than day to day working papers) should be kept (see paragraph 45). 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.
60. Wherever practicable, the files should be kept together in the diocesan bishop's office and under his 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 be notified to the Information Commissioner as joint data controllers in respect of the same files.
61. If these principles are followed, 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.

### The cleric

62. The DPA 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 walk into the bishop's office and demand to see their files. Under the DPA, a subject access request must be made in writing and a fee of not more than £10 may be charged.
63. Once the fee has been paid, and the bishop has received sufficient information from the applicant to enable him to comply with the request, he has 40 days in which to do so<sup>11</sup>. The information should be supplied in the form of copies unless that would involve disproportionate effort. This defence of

---

<sup>11</sup> Legislation shortening this period to 1 calendar month, and removing the power to ask for a fee, is expected to be implemented in 2015.

disproportionate effort should not, however, be invoked lightly, as the Information Commissioner is likely to scrutinise closely any reliance on it.

64. 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.
65. 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.
66. The Information Commissioner has produced two useful guidance notes entitled 'Checklist for handling requests for personal information (subject access requests)' and 'Dealing with subject access requests involving other people's information'. These are available from the Information Commissioner's website<sup>12</sup>.

### Third parties

67. As a general principle, personal information from clergy files should not be shared with third parties (including other diocesan bishops) 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.
68. There are, however, circumstances where the DPA allows personal data to be shared without consent<sup>13</sup>. 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.
69. The police and other statutory authorities are usually willing to confirm that these conditions are met in relation to any information disclosed to them

---

<sup>12</sup>

[http://www.ico.gov.uk/for\\_organisations/guidance\\_index/~media/documents/library/Data\\_Protection/Practical\\_application/checklist\\_for\\_handling\\_requests\\_for\\_personal\\_information.ashx](http://www.ico.gov.uk/for_organisations/guidance_index/~media/documents/library/Data_Protection/Practical_application/checklist_for_handling_requests_for_personal_information.ashx)

[http://www.ico.gov.uk/for\\_organisations/guidance\\_index/~media/documents/library/Data\\_Protection/Detailed\\_specialist\\_guides/SAR\\_AND\\_THIRD\\_PARTY\\_INFORMATION\\_100807.ashx](http://www.ico.gov.uk/for_organisations/guidance_index/~media/documents/library/Data_Protection/Detailed_specialist_guides/SAR_AND_THIRD_PARTY_INFORMATION_100807.ashx)

<sup>13</sup> See the Data Sharing Code of Practice issued by the ICO:

[http://www.ico.gov.uk/for\\_organisations/data\\_protection/topic\\_guides/~media/documents/library/Data\\_Protection/Detailed\\_specialist\\_guides/data\\_sharing\\_code\\_of\\_practice.ashx](http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/~media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx)



which relates to concerns about safeguarding. 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.

70. 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 the Data Sharing Protocol agreed by the House of Bishops (Appendix 1).
71. Where a cleric 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 personal file should be retained by the bishop in whose diocese the cleric last served, and information from it should only be disclosed outside the Church of England with the cleric's consent.
72. 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.
73. Where a cleric is appointed as a regular chaplain to the Armed Forces or to a Royal Peculiar, the personal file will be sent to Lambeth Palace. On that person's return 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 from Lambeth, to ensure that the record of his or her ministry is complete. Armed Forces Chaplaincies are aware of the procedures governing CCSLs and Episcopal References and will comply with these when providing or requesting references.
74. 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.
75. 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.
76. 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 which other dioceses have issued a licence or PTO 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

77. The DPA states that fair processing of personal information requires the data controller to ensure, so far as practicable, that the individual is provided with the following information:
- The identity of the data controller;
  - The purposes for which the information will be processed;
  - Any further information necessary, in the specific circumstances, to enable the processing to be fair to the individual.

The Information Commissioner says that ‘*drafting a privacy notice is the obvious way to satisfy these legal requirements*’<sup>14</sup>.

78. 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.
79. The primary purpose of the privacy notice is to ensure that clergy are properly informed about how their personal information will be used, and to obtain their consent where that is needed. In particular, consent is required to transfer the personal file to another bishop if the cleric moves between dioceses. Where such consent has not been obtained, the bishop will need to disclose that fact in the CCSL which is sent to the receiving bishop before any appointment is confirmed. The cleric should be made aware that a refusal to consent may adversely affect his or her prospects of appointment in another diocese<sup>15</sup>.
80. A model privacy notice is provided in Appendix 2. However, this may need adaptation to fit the circumstances of any particular case.

---

<sup>14</sup> Privacy Notices Code of Practice, page 8

[http://www.ico.gov.uk/for\\_organisations/guidance\\_index/~media/documents/library/Data\\_Protection/Detailed\\_specialist\\_guides/PRIVACY\\_NOTICES\\_COP\\_FINAL.ashx](http://www.ico.gov.uk/for_organisations/guidance_index/~media/documents/library/Data_Protection/Detailed_specialist_guides/PRIVACY_NOTICES_COP_FINAL.ashx)

<sup>15</sup> Privacy Notices Code of Practice page 9 ‘Where people do have a choice, it must be properly explained to them’.

**Appendix 1**  
**(See paragraph 70 of the Guidance)**

**Data Sharing Protocol**

**Adopted by the House of Bishops on 13<sup>th</sup> March 2013**

Purpose of the protocol

1. This protocol sets out the basis on which a diocesan bishop in the Church of England agrees to share personal information with another diocesan bishop in the Church of England about clergy who live or minister in his diocese.
2. Bishops need to share such information from time to time in order to discharge their legal and pastoral responsibilities as chief pastor of the diocese.

Circumstances in which personal information will be shared

3. Where a bishop ('the receiving bishop') submits a request at any time for personal information about a priest or deacon to another bishop ('the sending bishop') and the receiving bishop confirms in writing that the sharing of the information is in the substantial public interest and is necessary (a) for the prevention or detection of any unlawful act or (b) for the protection of the public against dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, that priest or deacon or another person, then the sending bishop will share that information with the receiving bishop. In these circumstances data protection legislation permits personal information to be shared without the individual's consent being sought.
4. Where a priest or deacon is being considered for an appointment or permission to officiate in the receiving bishop's diocese, and the sending bishop receives a request from the receiving bishop for an Episcopal Reference and Clergy Current Status Letter ('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.
5. 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 transfer to the receiving bishop the clergy personal file at 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), provided that the individual in question has given his or her consent to such transfer. If consent has been refused, the sending bishop will have advised the receiving bishop accordingly in the CCSL.
6. 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.

7. Where a priest or deacon moves to a specialist ministry in England and he or she holds a bishop's licence in connection with that ministry, the personal file will be transferred to the bishop who issues the licence. If he or she is to serve under contract without a licence, the file will remain in the diocese where the cleric last served.
8. Where a priest or deacon is appointed as a regular chaplain to the Armed Forces or to a Royal Peculiar, the personal file will be transferred to Lambeth Palace. On that person's return to diocesan ministry, a brief summary of his or her Forces posting or appointment to the Royal Peculiar in question will be added to the personal file before the file is sent to the receiving bishop from Lambeth, to ensure that the record of his or her ministry is complete.
9. When a priest or deacon retires, the personal file will remain in the diocese in which he or she last served unless and until he or she is granted PTO in another diocese.
10. Where a priest or deacon ceases to hold a PTO or leaves the ministry of the Church of England, either temporarily or permanently, the personal file will be retained in the diocese in which he or she last served.
11. Where a priest or deacon holds a licence or PTO concurrently in more than one diocese, the personal file will be held in the diocese where the greater part of his or her ministry is exercised. A note will be kept on the file as to which other dioceses have issued a licence or PTO and arrangements put in place for the appropriate staff of those dioceses to have access to the file as necessary. The other dioceses will in turn keep a record of where the personal file is held.

#### Security

12. All diocesan bishops will put in place appropriate measures to ensure that the personal information which they hold about clergy is secure. Where information is shared electronically it will be encrypted or password protected. Where it is shared in paper form it will be sent by registered or recorded delivery post.

#### Retention periods

13. 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. Where a file is deposited in a diocesan archive office after the death of the cleric to whom it relates, it will be subject to the conditions as to retention and ultimate disposal which apply to material held in that archive.

<b>Record type</b>	<b>Retention period</b>
<i>Relates to paragraph 18</i> A note of the reasons for processing sensitive personal data	Length of time the data to which the note is held
<i>Relates to paragraph 20</i> Common Application Form	Successful application forms should be held on the file for 20 years from the date of the cleric's death
<i>Relates to paragraph 21</i> 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
<i>Relates to paragraph 21</i> 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 ( <i>which ever is soonest</i> )
<i>Relates to paragraph 21</i> Copies of qualification certificates	20 years from the date of the cleric's death
<i>Relates to paragraph 21</i> Cleric's CV since leaving school	20 years from the date of the cleric's death
<i>Relates to paragraph 22</i> Copy of faculty under Canon C4.3A	20 years from the date of the cleric's death
<i>Relates to paragraph 22</i> 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
<i>Relates to paragraph 23</i> 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
<i>Relates to paragraph 23</i> Copies of any 'safe to receive' or Clergy Current Status letters ('CCSL')	50 years from the date of the cleric's death
<i>Relates to paragraph 23</i> Application papers – including application form, references, copy licence, deed of institution, Statement of Particulars (where subject to Common Tenure)	Papers relating to successful applications should be held on the file for 20 years from the date of the cleric's death
<i>Relates to paragraph 24</i> A written record of any Ministerial Development Review	20 years from the date of the cleric's death
<i>Relates to paragraph 25</i> Records of any continuing ministerial education ('CME') undertaken	20 years from the date of the cleric's death

<p><i>Relates to paragraph 27</i> Criminal Record Check certificate</p>	<p>6 months from the date of the recruitment decision to which they relate</p> <p><i>Certificates can only be retained for a longer period in exceptional circumstances and where the Disclosure and Barring Service have been consulted</i></p>
<p><i>Relates to paragraph 27</i> Record of a cleric's criminal record check history (the nature of which is noted in paragraph 27)</p>	<p>50 years from the date of the cleric's death</p>
<p><i>Relates to paragraphs 28 and 53</i> Record of safeguarding allegations and concerns – including details of how these are handled, followed-up, actions taken, decisions reached and eventual outcome</p>	<p>50 years from the date of the cleric's death</p>
<p><i>Relates to paragraph 30</i> Evidence of clergy personal file being independently scrutinised under the Past Cases Review Protocol – including a note of any action resulting</p>	<p>50 years from the date of the cleric's death</p>
<p><i>Relates to paragraph 31 and 53</i> 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)</p>	<p>50 years from the date of the cleric's death</p>
<p><i>Relates to paragraph 32, 33, 34</i> Record of CDM complaints – including copies of the complaint, report on preliminary scrutiny, respondent's answer, supporting evidence, letter recording bishop's decision</p>	<p>20 years from the date of the cleric's death</p>
<p><i>Relates to paragraph 32</i> A brief summary of an allegation of misconduct (not resulting in a formal CDM complaint)</p>	<p>20 years from the date of the cleric's death</p>
<p><i>Relates to paragraph 35, 36</i> 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)</p>	<p>20 years from the date of the cleric's death</p> <p>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</p>

<i>Relates to paragraph 35</i> Record of capability issues (where there is no formal capability inquiry)	20 years from the date of the cleric's death
<i>Relates to paragraph 39</i> 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
<i>Relates to paragraph 41</i> Record of significant unresolved financial problems	Keep the record until financial problems have been satisfactorily resolved

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

**Model Privacy Notice in the form of a letter from the diocesan bishop**

Using your personal information

This letter explains how the information about you which I hold in your personal file is used and the circumstances in which it may be shared with others.

The information in your personal file enables me 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).

The attached Data Sharing Protocol has been adopted by the House of Bishops and explains the circumstances in which I may share information about you with the bishop of another diocese in the Church of England. Otherwise, your personal information will not be shared outside my own senior and administrative staff without your consent, unless the Data Protection Act 1998 allows this to happen. In particular, your consent is needed for your personal file to be transferred to the bishop of another diocese when you are appointed to a post in that diocese. You should be aware that if you choose to refuse consent to the transfer of the file in these circumstances, I am obliged to disclose this fact in the episcopal reference that I give to any bishop who is considering you for appointment, and your prospects for appointment in another diocese may be affected as a result.

You have the right to ask for a copy of the information which I hold about you. If you would like a copy of some or all of this information, please write or send an e-mail to [y] at [address]. A charge of not more than £10 may be made.

Please sign and return the enclosed copy of this letter, indicating whether you agree that your personal file may be transferred to the bishop of another diocese in the Church of England in the circumstances described in the Data Sharing Protocol.

On copy

I agree/do not agree [*please delete as appropriate*] that my personal file may be transferred to the bishop of another diocese in the circumstances described in the Data Sharing Protocol. I understand that if I do not agree this may affect my prospects of appointment in another diocese.

Signature .....

Date .....