



CLERGY PERSONAL FILES POLICY

What does this policy cover?

1. This policy, and the instructions contained within it, is designed to assist bishops and their offices in managing personal information on behalf of the Representative Body of the Church in Wales¹ (“the RB”) about the clergy in their Dioceses, and to ensure good and consistent practice in record keeping across the six bishops’ offices. It considers the requirements of data protection legislation and the law of confidentiality and also addresses practical issues of file management and storage.
2. This policy deals only with personal files about clergy (“clergy personal files”, sometimes also referred to as “blue files” or “personnel files”). It does not specifically cover personal files relating to readers and other lay ministers, although the same general principles will apply to such files. Nor does it cover files relating to those who are exploring a vocation to ministry or who are in training but not yet ordained. The term “clergy personal file” or “personal file” will be adopted as accepted terminology in this policy.
3. Procedures relating to the personal files of Readers and other lay Ministers are now contained in the Privacy Notice for Pre-Ordination/Discernment and Lay Licensed Ministers which is Online at www.churchinwales.org.uk/privacy-notice.
4. The personal files of the bishops (including the Archbishop) are held by the Archbishop’s Registrar in the Provincial Office. The personal files for cathedral deans and other dignitaries are held in the relevant bishop’s office, along with the files for the clergy of that diocese.

Overview of relevant legislation and legal duties

Data Protection

4. The UK-GDPR applies to the processing of any information (‘personal data’) 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. Processing is widely defined and includes obtaining information, holding it (whether in paper or electronic form) and sharing it with others.
5. The UK-GDPR sets out 6 fundamental principles which must be observed when processing personal data. In summary, data must be:

¹ The Representative Body’s role as data controller is explained further at paragraph 10

- (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.
6. In comparison to previous legislation the UK-GDPR 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”.
7. 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.
8. Like its predecessor, the UK-GDPR also provides that certain information is to be treated as ‘sensitive’ (or ‘special category’ 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 or union membership. Whilst criminal records (including any allegation that a criminal offence has been committed) are not classed as “special category”, they stand as a class of their own and similar conditions will apply. Such records should be treated as “sensitive”.
9. The Information Commissioner’s website (www.ico.gov.uk) is a useful resource which provides general and specialist guidance on many aspects of the UK-GDPR.

10. The Representative Body of the Church in Wales is the 'Data Controller' in respect of the data in the personal files. An employee in the legal department at the Representative Body has been appointed as Data Protection Officer for the Representative Body. In practice most day-to-day administration of the personal files will be undertaken by the Bishops' PAs, who are employees of the Representative Body. All persons processing personal data in relation to the clergy personal files are required by the Data Controller to act in accordance with the instructions and advice contained within this policy.

Consent

11. Under previous legislation many organisations relied on consent in order to process personal data. The UK-GDPR both sets a much higher standard in relation to the obtaining and managing of consent in relation to individuals, ~~and~~ which includes managing a schedule of collection, expiry and re-collecting consent where necessary. However, the UK-GDPR also provides for many other legal bases for processing personal data (e.g. legal obligation and/or Public Task).
12. Under the UK-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.
13. The processing of the personal data contained within clergy personal files is based on the lawful basis of Public Task (UK-GDPR Article 6(1)e) and in so far as the information is "special category" (i.e. sensitive), for reasons of substantial public interest, under Article 9(2)g UK-GDPR and the substantial public interest conditions at Schedule 1 Part 2 paragraph 6(2)a Data Protection Act 2018. ("The DPA".) The reason for this choice of lawful basis is because the operational activities of running the Church in Wales are authorised by Statute Law in the form of the Welsh Church Act 1914. Also, the Constitution of the Church is created under powers provided by the Act. These data are processed by the Church under Public Task to enable the Church to be able to develop, support, administer, regulate and manage clergy through their ministry; consequently, such data processing does not fall under the lawful basis of Consent.

Confidentiality

14. 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.
15. 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.

16. 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

17. The Representative Body and those individuals acting on its behalf need to take account of the data protection principles when deciding what information should be held in any clergy personal file. The following questions should be asked in relation to any category of personal data:
 - (a) Is there a proper and lawful reason why we need to have this information? The first and second data protection principles in the UK-GDPR state that personal data must only be obtained for a lawful and specified purpose.
 - (b) Is the processing of this information on file in accordance with the lawful basis of Public Task? 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 UK-GDPR, meaning that there will be additional requirements in order to process this data.

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

18. The law of the Church in Wales imposes a requirement on each Bishop that s/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. For a significant amount of personal data properly held on a clergy personal file, this will be a proper and lawful reason for holding the information.

Is the processing of this information on file in accordance with the lawful basis of Public Task under the UK-GDPR? If not, is there another legal basis on which I can rely for processing this personal data?

19. As explained 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

a Lawful Basis under Article 6 of the UK-GDPR, you will also have to satisfy a processing condition contained in Article 9. The processing of this personal data must be considered necessary for the purposes of Public Task (Article 6(1)e). The provisions for processing under Article 9 UK-GDPR will also include the following matters, where appropriate: Article 9(2)a where the data subject has given explicit consent; Article 9(2)b where the Church has obligations as an employer; Article 9(2)e where the data is manifestly made public by the data subject; Article 9(2)f in relation to a legal claim; Article 9(2)g processing in pursuance of substantial public interest; Article 9(2)h processing for the purposes of preventive or occupational medicine and Article 9(2)j processing for archiving purposes in the public interest.

20. The Church in Wales has reached an agreement with the Church of England regarding data sharing (see paragraph(s) 74 and 79-81 below). Comments about the Episcopal Reference and the Clergy Current Status Letter (“CCSL”) are contained in paragraph 83 below. Data sharing with recipients outside of Wales is covered in paragraphs 74-92.
21. Where information is supplied by a third party (i.e. a person outside the provincial office, 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? Does it fall under the requirements for Public Task?
22. The vast majority of processing by the bishop will be permitted on the basis of Public Task because it is necessary to ensure that only those fit for ministry have access to ministerial posts. Nevertheless, if the bishop has concerns he/she should seek the advice of the Data Protection Officer (or legal advice from the local diocesan registrar) as to whether the Church in Wales 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

23. 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. Basic biographical details are also held on the clergy section of the ‘infonet’ database, so the hard-copy file may instead cross-reference that information.
24. 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 a standard application form. 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.

25. The Church in Wales clergy files have recently been redesigned and standardised in line with this policy. A detailed explanation and practical assistance in the management of Clergy Personal files has been provided to each Bishops office.

A cleric's personal file should include the following biographical information so far as practicable.

- (a) Name, date of birth and contact details.
- (b) If the cleric is not a British citizen, evidence of immigration status and permission to work in the UK.
- (c) 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.
- (d) Qualifications. Information (especially in relation to degree and post-graduate qualifications) should be supported by copy certificates where possible.
- (e) 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

25. 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 themselves 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 Discernment Panel and the periodic reports sent to the bishop by the cleric's training institution. If a faculty granting dispensation from an impediment to ordination has been granted, a copy should be kept on the file.

26. The following should also be kept on file:

- (a) Copies of the cleric's letters of orders.
- (b) 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.
- (c) In relation to the current appointment, copies of the application form and references (where applicable), copy licence or deed of institution or permission to officiate.
- (d) Details of Ministerial development and training

27. A record of CMD undertaken will be helpful to the bishop in assessing whether a cleric has complied with their duties under the Clergy Terms of Service Canon, and in assessing what CMD 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

28. 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:

- (a) The date of issue of a certificate;
- (b) The name of the subject;
- (c) The type of certificate requested;
- (d) The position for which the certificate was requested;
- (e) The unique reference number of the certificate;
- (f) Details of the recruitment decision taken, including a brief précis of the information provided.

29. The Representative Body undertakes DBS checks centrally and then distributes the relevant information to bishops' offices for inclusion of the relevant information on the file. Any police information should be held on the personal file. Current Church in Wales policy is for DBS Certificates to be renewed every three years, and renewal reminders are organised by the Representative Body if the cleric is not subscribed to the DBS Update service.

30. 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 bishop of another diocese when a request for an Episcopal Reference and CCSL is received. The Provincial Safeguarding Officer is responsible for providing the relevant information for inclusion on the file.

31. Where relevant safeguarding papers are not held by the bishop (where there is a day-to-day ongoing investigation for example) 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. The Provincial Safeguarding Officer is responsible for informing the relevant bishop's office that a safeguarding file has been opened, and that a cross-reference note should be placed on the personal file.

32. 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 and to ensure that correct cross-references can be made if the same or similar allegations arise in future.

33. A record of a cleric's safeguarding training must be retained on the personal file. This should include details of the nature of the training, the date the training was received

and who provided the training. If training data is held electronically, this should be cross-referenced on the hard-copy file.

34. Where a file has been scrutinised under a past cases review or external audit, evidence that it has been independently reviewed, together with a note of any action taken as a result, should be kept on the file.

35. A copy of any safeguarding information will be retained by the Provincial Office even where the cleric has left the Church in Wales in the central provincial safeguarding database (MyConcern).

Informal disciplinary complaints

36. 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.

Formal Complaints under the Disciplinary Procedure

37. A record should be kept on the file of all matters heard by the Disciplinary Tribunal. This should include copies of the complaint, the report of any informal investigations, the respondent's response to the complaint (if any), all supporting evidence, the report of the Preliminary Adjudicator, the judgment of the Tribunal and details of any penalty imposed. If the complaint was resolved without reference to the Tribunal, a record of all actions taken should be kept with the file. If a complaint was dismissed by the Preliminary Adjudicator, a copy of the Preliminary Adjudicator's decision should be kept on file.

38. If the bishop has passed a name to the Archbishop's Registrar to request that it be included on the Archbishop's Registrar's List, a copy of this referral should be retained on the file, together with the response of the Archbishop's Registrar to the request.

Capability and health

39. 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.

40. 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.

41. 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.

Grievance

42. A record should be kept on the personal file of grievances raised under the Church in Wales grievance procedure either by or against the cleric, including details of the grievance, the process followed and the outcome.

Finance

43. 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. A question about financial matters is included in the Episcopal Reference and CCSL and any significant unresolved financial problems of which the bishop is aware should be noted on a cleric's personal file.

Management of clergy personal files

Format

44. Unless and until such point as the Church in Wales introduces full digitised record keeping (at which point this policy will be updated) there should be a paper file for every cleric in the Church in Wales. In practice however, record-keeping is likely to involve a combination of paper-based and computer records.

45. 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. It is essential that this is done and carefully monitored to ensure that a full set of papers is provided if the cleric moves to another Diocese.

Location

46. All personal information about clergy in a diocese should be held together in one place. Those staff who contribute information to clergy personal files (for example, archdeacons and bishops' PAs) need to be clear about where the file of any cleric is kept and the arrangements for keeping it updated. Staff should not keep separate files of papers which should properly sit on the personal file, other than such day to day working papers as are required for effective discharge of (for example, an Archdeacon's) current duties. Such working papers should be transferred regularly and frequently to the main file: each diocese should have in place a policy to ensure that this happens systematically.

47. 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 staff.

48. The Provincial Safeguarding Officers, Provincial Safeguarding Manager and Director of Safeguarding must have full, unrestricted access to the files at any reasonable time. Similarly, the Data Protection Officer at the Representative Body must have full access to the files.
49. During a vacancy in a See the Archbishop acts as guardian of the spiritualities and shall give directions as to the management, storage and access arrangements for the files for the duration of the vacancy.
50. The Bishops' and Archbishop's files are under the control of the Archbishop's Registrar, who shall give directions as to the management, storage and access arrangements for the files. The Archbishop must have full access to the files of the other Bishops, and the Senior Bishop must have full access to the file of the Archbishop.
51. Upon retirement or resignation, files of the Bishops and Archbishop shall remain under the control of the Archbishop's Registrar. The Archbishop and any Diocesan Bishop in a Diocese where the retired Bishop has PTO (or a licence) shall have access to the file.
52. The files of clergy subject to a contract of employment with the Representative Body are also under the control of the Archbishop's Registrar. The Archbishop and any Diocesan Bishop in a Diocese where the cleric has PTO (or a licence) shall have access to the file.
53. During a vacancy in the Archbishopric, the Senior Bishop shall have the powers of access of the Archbishop and the next longest-serving Diocesan Bishop shall have the powers of access of the Senior Bishop.

Security

54. 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.
55. What is appropriate in any case will depend on the particular circumstances of each Bishop's office, but the following suggestions are offered as examples of standard good practice:
 - (a) establishing clear rules as to which members of the bishop's staff may have access to the files;
 - (b) keeping paper files in locked, cabinets, with access to keys limited to authorised staff;
 - (c) Ensuring that premises are properly protected with burglar and fire alarms;

- (d) protecting records held on computer with permissions managed to ensure access is restricted only to those who are entitled to access files;
- (e) transmitting personal data electronically only in encrypted form;
- (f) using secure delivery methods such as “guaranteed delivery” and “track and trace” if sending personal data through the post;
- (g) regularly backing up electronic files.

56. Only cloud-based storage solutions approved by the Head of Communications & Technology at the Representative Body should be used to store or transmit data electronically.

Updating and retention

57. The fourth data protection principle states that personal data must be accurate and, where necessary, kept up to date. 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.

58. 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 the agreed Church in Wales retention periods for particular categories of personal data in clergy personal files.

59. 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 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 in the Church in Wales for the same period; if any original documents relating to such matters are on the personal file (rather than held with the safeguarding team at the Provincial Office) these should be sent to the Provincial Safeguarding Manager for retention.

60. Material relating to disciplinary complaints (whether or not referred to the Tribunal) should be retained during the lifetime of the cleric and thereafter in accordance with the retention period policy at Appendix 1. This applies even where a 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 record of disciplinary matters must be included in the personal file sent to the new diocese. However, a copy should 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 by the diocese if necessary.

61. It is also advisable to keep during the cleric's lifetime (and thereafter in accordance with the retention period policy at Appendix 1) a record of how capability issues that have arisen have been addressed.
62. 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). 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).
63. When a person dies, the UK-GDPR ceases to apply. It is important that, when a retired cleric dies, the Representative Body are informed. Files should not be passed to third parties such as local record offices, but after the cleric's death the file should be retained for 70 years and then destroyed.
64. There may, in rare cases, material on personal files which is of important public historic record, and which therefore should be deposited with the Church in Wales records at the National Library of Wales. However, to ensure the integrity of the personal file such information should only be removed from the file immediately before the destruction date (70 years after the cleric's death). If material is deposited before that date, a full copy of the material deposited must be retained on the personal file.

Sharing information in clergy personal files

The bishop's office and senior staff

65. 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. 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.
66. The files for the whole Diocese should be kept together in the diocesan bishop's office.
67. If this Policy is followed, there should be no difficulty from a data protection perspective in a bishop sharing information from clergy personal files 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 cleric

68. The UK-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 UK-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 may make “Subject Access Requests” (SAR) 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. They are not usually entitled to see the personal data of third parties held in their files, which means file contents, which include third parties’ data, must be redacted before being presented to the cleric if an SAR is received.

69. Data controllers can no longer (ordinarily) charge for “Subject Access Requests” and will have only 1 month to respond from the receipt of the request. Data controllers are able to charge a “reasonable administrative fee”, but only for requests that are manifestly unfounded, excessive or repetitive.
70. Not all personal data should necessarily be disclosed on a subject access request. Bishops should seek advice from the Data Protection Officer on any requests received - it is vital that he is informed promptly of any Subject Access Request, given the tight time limits for compliance. Subject Access Requests relating to the Clergy Personal Files must be passed to the Data Protection Officer to record and respond and should not be answered directly by Bishops office staff.
71. 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.
72. 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.
73. The Information Commissioner has produced a useful guide for handling subject access requests.²

Third parties

74. As a general principle, other than providing an Episcopal Reference and CCSL, personal information from clergy files should not be shared with third parties outside the Church in Wales other than as set out in the following paragraphs or in compliance with a court order or other legal obligation.
75. There continue to be circumstances where sensitive (now special category) personal data can be shared outside the organisation 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.

² <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/>

76. 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 either of the following purposes:
- a. protecting a child or adult-at-risk from neglect or physical, mental or emotional harm; or
 - b. protecting the physical, mental or emotional well-being of a child or adult-at-risk.
77. That said, in the first instance, obtaining consent ~~should~~ may still be considered. If, after having considered the position, consent cannot or should not 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. Advice from the Provincial Safeguarding Officer should be sought in such cases – it is usual practice if for requests for such information to be referred to the safeguarding team, who will liaise directly with the third party.
78. The sharing of information about clergy between diocesan bishops of the Church in Wales is treated as an operational necessity of running the Church under the lawful basis of Public Task. (See paragraph 13 above). Transfers of files between bishops offices and their staff can be achieved without additional administration or paperwork, as they fall under the data protection policies and procedures of the Representative Body. However, it should be remembered that each Ministry/Mission area within the Church are independent legal entities and Data Controllers of their own internal data protection regime. Advice should be sought from the DPO before sharing data from the Clergy personal file with a Ministry Area.
79. The sharing of information about clergy between the Church of England (including the Diocese in Europe) and the Church in Wales, is governed by a Data Sharing Protocol and agreements between the bodies that comprise the institutional Church of England and the Church in Wales. The lawful bases for this is because it is a necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; as well as being, in so far as the data is special category data, pursuant to the public interest conditions at Article 9(2)g UK-GDPR and the substantial public interest requirement at Schedule 1 Part 2 paragraph 6(2)a DPA 2018.
80. The transfer of the file between a Church of England body and the Church in Wales is considered to be necessary for the performance of a task carried out in the public interest or the exercise of official authority vested in the bishop by the Canons of the Church of England and the provisions of the Welsh Church Acts and Constitution, so under the UK-GDPR no consent will be required.

81. Where a priest or deacon moves to take up a new appointment or permission to officiate ('PTO') in another diocese in the Church in Wales, or a 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 service 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. It is vital that the file follows the cleric. It should not be made available to the receiving Bishop until after an appointment is confirmed.
82. Where a priest or deacon takes up an appointment in a diocese which is not part of the Church of England or the Church in Wales (this will include the Church of Ireland or the Scottish Episcopal Church) the clergy personal file will be retained by the bishop in whose diocese the cleric last served. Clergy personal files must not be transferred outside of the Church in Wales (except in relation to the Church of England as above). A copy of personal data from the file may be disclosed to the receiving bishop on request, as set out in more detail at paragraph 84.
83. Where a priest or deacon is being considered for an appointment or PTO in another diocese (whether in England, Wales or elsewhere, 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 performance of a task carried out in the public interest or in the exercise of official authority vested in the controller pursuant to Article 6(1)e of the UK-GDPR and in so far as the information is "special category" (i.e. sensitive) under Article 9(2)g UK-GDPR and the substantial public interest requirements at Schedule 1 Part 2 paragraph 6(2)a DPA 2018 or criminal conviction and offence data under Article 10, it is necessary for the reasons of substantial public interest on the basis of UK law³, 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 in Wales but also to posts outside the Church in Wales. The Episcopal Reference and CCSL are designed to provide sufficient information for a Bishop in the receiving diocese/church to make an informed appointment decision and start their own personal file on the cleric.
84. Where a priest or deacon takes up appointment in a diocese which is not part of the Church Wales or Church of England (including the Church of Ireland or the Scottish Episcopal Church) an Episcopal Reference and CCSL may be provided to the receiving bishop as above (if this has not already been done). As noted above, Clergy personal files must not be transferred outside of the Church in Wales except to the Church of

³ See Article 9(2)(g) and section 10(5) of the Data Protection Act 2018, Schedule 1 Part 2, paragraph 11

England. A copy of personal data from the file may be provided to the receiving bishop on request. The legal basis for disclosing this information is that it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller pursuant to Article 6(1)e of the UK-GDPR and in so far as the information is “special category” (i.e. sensitive) under Article 9(2)g UK-GDPR and the substantial public interest requirements at Schedule 1 Part 2 paragraph 6(2)a DPA 2018 or for criminal conviction and offence data under Article 10, it is necessary for the reasons of substantial public interest on the basis of UK law⁴, 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. The original file should be retained in the last diocese of the Church in Wales where the cleric ministered. A clear note should be placed on the file that the cleric has left Wales, that a copy of information in the file was provided to the relevant receiving diocese, and that enquiries must be made with relevant provinces/dioceses and the retained file updated before any ministry in Wales may resume. The Data Protection Officer should be consulted to ensure that the appropriate data, and only the appropriate data, is shared.

85. Under the Data Protection Act 2018, where a data controller 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, 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. The Representative Body’s Privacy Notice for clergy and this document comprise such policy documents.
86. The bishop must also keep a record of any processing that is done in reliance on this condition. Such record must state which condition is being relied upon; how the processing satisfies Article 6 of the UK-GDPR and whether the personal data is retained and erased in accordance with the policy document.
87. Where a cleric moves to a specialist or sector ministry (e.g. the Secretary of a Missionary Society or a prison chaplaincy) 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 issued the licence.
88. Where a cleric is appointed as a regular chaplain to the Armed Forces the personal file should be sent to Lambeth Palace as the Church of England Bishop to the Forces is based there. Armed Forces Chaplaincies are aware of the procedures governing Episcopal References and CCSLs and can be expected to comply with these when providing or requesting references.

⁴ See Article 9(2)(g) and section 10(5) of the Data Protection Act 2018, Schedule 1 Part 2, paragraph 11

89. Where a cleric is appointed to serve in a secular context, under an employment contract without a licence or PTO, the file should remain in the diocese where the cleric last served.
90. 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.
91. Where a cleric ceases to hold a PTO in any Diocese of the Church in Wales or leaves the ministry of the Church of Wales, the personal file should be retained in the diocese where he or she last served, unless they are serving in the Church of England, in which case the file should be transferred to the relevant English Diocese.
92. 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 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

93. 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 UK-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.
94. The information must be provided in a concise, transparent, intelligible and easily accessible way, using clear and plain language. In consultation with its external legal advisors, the Representative Body has prepared an issued a Privacy Notice, available at <https://www.churchinwales.org.uk/privacy-notice/>.

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 Church in Wales.

Record type	Retention period
A note of the reasons for processing sensitive personal data	Length of time the data to which the note is held
Copy of birth certificate (or other appropriate evidence demonstrating canonical age for ordination)	20 years from the date of the cleric's death
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>(whichever is soonest)</i>
Copies of qualification certificates	20 years from the date of the cleric's death
Cleric's CV since leaving school	20 years from the date of the cleric's death
Copy of faculty dispensing with ordination impediment	20 years from the date of the cleric's death
Report of the Provincial Discernment Panel and periodic reports from the cleric's training institution	20 years from the date of the cleric's death
Copies of cleric's letters of orders	20 years from the date of the cleric's death
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

Application papers for posts: application form, references, copy licence, deed of institution.	Supporting papers for successful applications should be held on the file for 20 years from the date of the cleric's death. Papers for unsuccessful applications should not be retained following the end of the relevant recruitment process
A written record of any Ministerial Review	20 years from the date of the cleric's death
Records of any continuing ministerial education ('CME') undertaken	20 years from the date of the cleric's death
DBS Certificate	Not retained on personal file. The Provincial Office processes
Record of a cleric's criminal record check history	70 years from the date of the cleric's death
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
Evidence of clergy personal file being independently scrutinised under an external review – including a note of any action resulting	70 years from the date of the cleric's death
Copies of records relating to safeguarding allegations and concerns (this refers to papers being retained in the Provincial Office safeguarding team following the movement of the cleric to diocese outside of Wales)	70 years from the date of the cleric's death
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
Record of Disciplinary Tribunal – including copies of the complaint, referral and findings of the Tribunal and preliminary and final stages, supporting evidence, letter recording sanction/penalty/action taken.	70 years from the date of the cleric's death

A brief summary of an allegation of misconduct (not resulting in a reference to the Disciplinary Tribunal)	20 years from the date of the cleric's death
Records of capability inquiries raised - including a record of discussions between a cleric and a member of the bishop's staff, evidence of how health issues have been managed (e.g. copies of occupational health reports, note of any adjustments made)	20 years from the date of the cleric's death 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
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
Record of significant unresolved financial problems	Keep the record until financial problems have been satisfactorily resolved
Personal file itself after a cleric's death	Entire file to be destroyed 70 years after the date of the cleric's death